



## Kunnskapsinnhenting om elektroniske og internettbaserte løsninger for stemmegivning

*Utarbeidet på oppdrag for Kommunal- og distriktsdepartementet*

## Om Oslo Economics

*Oslo Economics utreder problemstillinger og gir råd til myndigheter, organisasjoner og bedrifter. Vi forstår problemstillingene som oppstår i skjæringspunktet mellom marked og politikk.*

*Vi er et samfunnsfaglig analyse- og rådgivningsmiljø med erfarne konsulenter med bakgrunn fra offentlig forvaltning og ulike forsknings- og analysemiljøer. Oslo Economics har i dag rundt 70 medarbeidere, hvorav mer enn 15 med doktorgrad. Vi tilbyr innsikt basert på fagkompetanse, sektorerfaring og et nettverk av samarbeidspartnere.*

## Om Norsk Regnesentral

*Norsk Regnesentral (NR) ble etablert i 1952 og er en privat, uavhengig stiftelse som utfører oppdragsforskning for bedrifter og det offentlige i det norske og internasjonale markedet.*

*NR er ledende i Norge innen utvalgte deler av informasjons- og kommunikasjonsteknologi. Innen IKT-området har NR innsatsområdene digital sikkerhet, digital inkludering og digital transformasjon. NRs visjon er forskningsresultater som brukes og synes.*

# Innhold

<b>Sammendrag og konklusjoner</b>	<b>5</b>
<b>1. Kunnskapsinnhentingens bakgrunn, formål og innretning</b>	<b>9</b>
1.1 Bakgrunn og formål	9
1.2 Metode og gjennomføring	9
1.3 Informasjonskilder	12
1.4 Rapportstruktur	13
<b>2. Stemmeprosessen</b>	<b>14</b>
2.1 Stegene og dimensjonene i en stemmeprosess	14
2.2 Registrering for stemmegivning	15
2.3 Velgerens identitet kontrolleres	15
2.4 Velgeren avgir sin stemme	15
2.5 Stemmene telles	16
2.6 Resultatene publiseres	16
2.7 Velgeren får bekreftet stemmen (opsjon)	17
2.8 Kryptografi i stemmesystemer	18
<b>3. Mulige løsninger for stemmegivning</b>	<b>20</b>
3.1 Kategorisering av løsninger	20
3.2 Papirbaserte systemer	20
3.3 Elektroniske systemer	23
3.4 Internettbaserte systemer	24
<b>4. Vurderingskriterier for elektroniske stemmesystemer</b>	<b>27</b>
4.1 Bakgrunn og utarbeidelse av vurderingskriteriene	27
4.2 Sikkerhet	28
4.3 Transparens og etterprøvbarehet	29
4.4 Brukervennlighet og inkludering	30
4.5 Ressursbruk	31
<b>5. Sikkerhet</b>	<b>32</b>
5.1 Hovedfunn: Sikkerhet	32
5.2 Papirbaserte systemer	33
5.3 Elektroniske systemer	34
5.4 Internettbaserte systemer	36
<b>6. Transparens og etterprøvbarehet</b>	<b>38</b>
6.1 Hovedfunn: Transparens og etterprøvbarehet	38
6.2 Papirbaserte systemer	38
6.3 Elektroniske systemer	39
6.4 Internettbaserte systemer	39

<b>7. Brukervennlighet og inkludering</b>	<b>41</b>
7.1 Hovedfunn: Brukervennlighet og inkludering	41
7.2 Papirbaserte systemer	42
7.3 Elektroniske systemer	42
7.4 Internettbaserte systemer	43
7.5 Særlig om brukervennligheten til ende-til-ende-systemer	44
<b>8. Ressursbruk</b>	<b>45</b>
8.1 Hovedfunn: Ressursbruk	45
8.2 Elektroniske systemer	45
8.3 Internettbaserte systemer	46
<b>9. Oppsummerende vurdering av risiko, gevinster og kostnader</b>	<b>48</b>
9.1 Ingen systemer er perfekte	48
9.2 Risiko ved elektronisk og internettbasert stemmegiving	48
9.3 Prinsipielle forskjeller mellom stemmesystemer	49
9.4 Kostnader for stat og kommune	50
9.5 Oppsummerende betraktninger	51
<b>10. Referanser</b>	<b>52</b>

## Sammendrag og konklusjoner

*Flere land har de seneste årene innført ulike former for elektronisk stemmegiving ved valg til folkevalgte organer. Dette innebærer både elektronisk stemmegiving i valglokale (kontrollerte omgivelser), og stemmegiving over internett andre steder enn i valglokale (ukontrollerte omgivelser). I Norge ble det under kommune- og fylkestingsvalget i 2011 og stortingsvalget i 2013 gjort forsøk med elektronisk stemmegiving over internett i utvalgte kommuner. På grunn av manglende politisk enighet ble ikke forsøkene videreført.*

*I 2017 ble det nedsatt et valglovutvalg for å foreslå ny valglov og vurdere endringer i valgordningen. Utvalget konkluderte i 2020 med at elektroniske stemmeløsninger ikke er sikre nok enda, men at det er nødvendig med videre kunnskaps- og erfaringsinnhenting om elektronisk stemmegiving. Denne utredningen, gjennomført av Oslo Economics og Norsk Regnesentral, gir et oppdatert kunnskapsgrunnlag om bruk av elektronisk stemmegiving som grunnlag for å veie muligheter, risikoer, gevinster og kostnader opp mot hverandre.*

### Rammeverk for analyse av løsninger for elektronisk stemmegiving

Det finnes tre hovedkategorier av stemmesystemer: elektroniske, internettbaserte og papirbaserte systemer. I det vi har definert som elektroniske systemer skjer stemmegivingen i valglokale på maskiner med eller uten internetttilkobling (kontrollerte omgivelser). I det vi har definert som internettbaserte systemer skjer stemmegivingen over internett andre steder enn i et valglokale (ukontrollerte omgivelser).

Formålet med utredningen er å gi et grunnlag for å veie muligheter, risikoer, gevinster og kostnader ved ulike stemmesystemer opp mot hverandre. Til dette formålet har vi utviklet et analyserammeverk som tar utgangspunkt i Europarådets anbefalinger ved innføring av elektronisk stemmegiving. Disse anbefalingene gir land som ønsker å innføre elektronisk eller internettbasert stemmegiving en minimumsstandard for å sikre at prinsippene for gjennomføring av demokratiske valg blir ivaretatt.

Europarådets anbefalinger består av 49 kriterier, gruppert i åtte kategorier. Vi har valgt ut kriteriene som er mest relevante for analysen av ulike stemmesystemer og har gjort enkelte tilpasninger. Dette har resultert i totalt 13 kriterier. Vi har sortert disse under tre hovedkategorier: *sikkerhet*, *transparens* og *etterprøvnbarhet*, og *brukervennlighet* og *inkludering*. Europarådets anbefalinger er i utgangspunktet beregnet på løsninger for elektronisk stemmegiving. I analysen har vi imidlertid inkludert en vurdering av papirbaserte løsninger, representert ved dagens norske valgssystem. Dette for å ha en referanse til vurderingen av elektroniske og internettbaserte systemer.

Det er stor variasjon mellom ulike tekniske løsninger for elektronisk stemmegiving. Når vi vurderer *sikkerhet*, *transparens* og *etterprøvnbarhet*, og *brukervennlighet* og *inkludering* ved elektroniske og internettbaserte systemer, gjør vi det imidlertid konseptuelt og ikke for bestemte tekniske løsninger. Videre har vi i disse analysene vurdert hvert stemmesystem isolert sett, og ikke sett på bruk av kombinasjoner av papirbaserte, elektroniske og/eller internettbaserte systemer i valg gjennomføringen.

Ved at det er *konseptene* elektronisk- og internettbasert stemmegiving som analyseres og ikke konkrete løsninger, er oppmerksomheten rettet mer mot de prinsipielle enn de praktiske sidene ved en eventuell innføring av elektronisk stemmegiving. Vi har imidlertid gjort en overordnet vurdering av hva som kreves av ressurser på lokalt og sentralt nivå om en skal innføre elektronisk- eller internettbaserte systemer som et *supplement* til dagens papirbaserte valg gjennomføring. Gjennomgangen viser at en delvis innføring av elektroniske systemer vil være kostbart både for kommunene og for staten. For kommunene er det særlig anskaffelsen og driften av stemmemaskinene som er kostbart. Internettbaserte løsninger kan på flere områder være ressursbesparende for kommunene, men her vil en større del av kostnadene ligge på staten. Løsningene stiller store krav til systemutvikling og sikkerhet, noe som påvirker kostnader til materiell, utstyr, systemer og bemanning.

## Analyse av hovedkategorier av stemmesystemer

Tabell A nedenfor gjengir kategoriene, kriteriene og den oppsummerende vurderingen av om de tre hovedkategoriene av stemmesystemene i stor, noen eller liten grad oppfyller kriteriene. Vurderingene tolkes som følger:

- **I stor grad:** Det er ingen vesentlige utfordringer ved stemmesystemet, og kriteriet er i stor grad oppfylt.
- **I noen grad:** Det er enkelte utfordringer ved stemmesystemet som hindrer oppfyllelse av kriteriet, men utfordringene er ikke vesentlige, eller løsningen muliggjør oppfyllelse av kriteriet på andre vis.
- **I liten grad:** Det er vesentlige og/eller uløselige utfordringer ved stemmesystemer som gjør at kriteriet i liten grad er oppfylt.

Dagens papirbaserte valgsystem i Norge kommer best ut av **sikkerhetsvurderingen**. Vi vurderer at systemet oppfyller nærsagt alle sikkerhetskriteriene til et valgsystem i stor grad. Det eneste kriteriet det norske systemet ikke fullstendig oppfyller er kriteriet som omhandler verifiserbarhet, selv om verifisering delvis er mulig i dagens valgsystem.

Elektroniske systemer kommer svakere ut i sikkerhetsvurderingen. Hovedårsaken er faren for at valgresultatet kan bli manipulert i elektroniske systemer, noe som kan ha store konsekvenser for valgfallet. Denne risikoen blir reflektert i kriteriene knyttet til valgintegritet og korrekthet. I elektroniske systemer vil det også være en større risiko for at noen får tilgang til og publiserer deler av valgresultatene på forhånd. Dette vil i tilfelle innebære et brudd på kriteriet om fravær av påvirkning.

Internettbaserte systemer kommer svakest ut i sikkerhetsvurderingen. De internettbaserte systemene har de samme risikoelementene som elektroniske systemer knyttet til manipulering og forhåndspubliserings av valgresultatet. I tillegg foregår stemmegivingen ved internettbaserte systemer i ukontrollerte omgivelser, slik at det er mer utfordrende å verifisere at de riktige personene stemmer og at valgene er hemmelige. Disse risikoelementene blir fanget opp i kriteriene om autentisering, anonymitet og motstand mot tvang. Til slutt ligger det en systemsårbarhet i det at internettbaserte systemer er sentraliserte systemer. Kun et fåtall betroede medarbeidere er involvert i stemmehåndteringen, noe som gjør systemet mer avhengig av enkeltpersoner enn dagens papirbaserte system. I dagens papirbaserte valgsystem i Norge håndteres stemmene lokalt av lokale valgmedarbeidere. Også i majoriteten av elektroniske systemer foregår opptellingen av stemmer lokalt.

Dagens papirbaserte valgsystem i Norge kommer også best ut på vurderingen av **transparens og etterprøvbarehet**. Hovedårsaken er at valgobservatører enkelt kan observere alle stegene i stemmeprosessen, og dermed kontrollere at valget er i overensstemmelse med gjeldende regler. I elektroniske og internettbaserte systemer er stegene som er lett observerbare i et papirbasert system – for eksempel tellingen og kontroll av stemmene – mer utilgjengelig for valgobservatørene; relevant informasjon vil være lagret elektronisk etter flere sikkerhetstransformasjoner, og vil bare kunne kontrolleres av valgobservatører med særlig teknisk kompetanse.

Når det gjelder vurderingen av **brukervennlighet og inkludering**, er det viktig å påpeke at *brukervennlighet* kan bety ulike ting for ulike velgergrupper. Brukervennlighet handler både om hvordan og hvorvidt velgerne klarer å ta i bruk løsningen, og dessuten hvilke muligheter løsningen gir for bruk.

Vår overordnede vurdering er at papirbaserte systemer som det norske bare i noen grad oppfyller kriteriene for brukervennlighet og inkludering. Papirbaserte systemer er fordelaktig for velgere med lav teknisk kompetanse. For velgere som er blinde eller svaksynte er løsningene vanskelig å bruke, og for enkelte i denne gruppen legger ikke løsningen til rette for selvstendig stemmegiving.

For elektroniske systemer er vår overordnede vurdering at også de bare i noen grad oppfyller kriteriene for brukervennlighet og inkludering. Fordelen ved systemene er at de åpner opp for interaktive løsninger, og muliggjør bruk av hjelpemidler for brukere med særskilte behov. Dette kan gi økt brukervennlighet gjennom en tydeliggjøring for velgere av hvilke muligheter de har i stemmegivingen, og det kan forhindre velgerne i å gjøre utilsiktede feil. Det kan også muliggjøre selvstendig stemmegiving i større grad enn papirbaserte systemer som det Norge har i dag. Ulempen ved systemene er at de vil være utfordrende å ta i bruk for personer med svake digitale ferdigheter og kan dermed forsterke et digitalt utenforskap. Det er videre usikkert om det er praktisk gjennomførbart å utforme løsninger som muliggjør selvstendig stemmegiving for alle velgere.

Vår overordnede vurdering er at internettbaserte systemer også i noen grad oppfyller kriteriet brukervennlighet, men i stor grad oppfyller kriteriet inkludering. Internettbaserte systemer deler mange egenskaper med

elektroniske stemmesystemer, men gir økt fysisk tilgjengelighet, og vil sannsynligvis gjøre selvstendig stemmegiving mulig for alle velgere.

**Tabell A: Oppsummerende vurdering av stemmesystemene\***

	Papir- baserte systemer	Elektroniske systemer	Internett- baserte systemer
<b>Sikkerhet</b>			
<b>Fravær av påvirkning</b> – ingen foreløpige resultater skal kunngjøres før stemmegivingen er avsluttet			
<b>Autentisering</b> – mulige velgere skal autentiseres slik at kun stemmeberettigede kan stemme			
<b>Anonymitet</b> – det skal ikke være mulig å finne ut hvem som har stemt på hvem			
<b>Motstand mot tvang</b> – det skal ikke være mulig å presse en velger til å stemme på bestemte måter			
<b>Valgintegritet</b> – det skal ikke være mulig å endre avgitte stemmer eller stemmeresultatet			
<b>Korrekthet</b> – stemmene må telles opp korrekt og stemmeresultatet må publiseres korrekt			
<b>Verifiserbarhet</b> – hver velger kan kontrollere at sin valgte stemme har blitt talt opp, og hvem som helst kan verifisere at alle gyldige stemmer er blitt talt opp			
<b>Tilgjengelighet</b> – stemmesystemet må være tilgjengelig i samsvar med foreskrevet stemmeperiode			
<b>Transparens og etterprøvsbarhet</b>			
<b>Transparens</b> – mulighet for kontroll, observasjon, evaluering og verifikasjon			
<b>Etterprøvsbarhet</b> – mulighet for å etterprøve integriteten til avgitte stemmer og at stemmeresultater er ivaretatt.			
<b>Brukervennlighet og inkludering</b>			
<b>Brukervennlighet</b> – stemmesystemet skal være enkelt å forstå og bruke for velgere generelt, velgere med ulik teknisk kompetanse og for velgere som stemmer fra utlandet			
<b>Inkludering av grupper med særskilte behov</b> – stemmesystemet skal være enkelt å forstå og bruke for velgere med særskilte behov, og gjøre det mulig for velgere med særskilte behov å stemme selvstendig			

\*Grønn farge indikerer at kriteriet er oppfylt «(i stor grad)», blå farge indikerer «(i noen grad)» og rød farge indikerer «(i liten grad)».

#### Oppsummert om muligheter, risikoer, gevinster og kostnader

Analysen viser at ingen av de tre hovedkategorier av stemmesystemer er bedre enn de to andre systemene på alle punkter. Dagens papirbaserte system er alene om å i stor grad tilfredsstillere kriteriene anonymitet, valgintegritet, korrekthet, transparens og etterprøvsbarhet, mens internettbaserte systemer er alene om å i stor grad tilfredsstillere kriteriet for inkludering av grupper med særskilte behov. Etter vår vurdering er ikke forskjellene mellom systemene som reflekteres i analysen primært et resultat av hvor langt den teknologiske utviklingen nå har kommet, eller hvordan systemene i dag er utformet. Trolig vil det også i fremtiden være krevende å imøtekomme kriteriet om inkludering av grupper med særskilte behov med dagens papirbaserte valgssystem, og en vil ikke kunne garantere fullt ut for sikkerheten ved bruk av elektroniske og internettbaserte systemer.

At det ikke er mulig å garantere for sikkerhet i elektroniske løsninger fører med seg en risiko for tap av tillit. Valglovutvalget påpeker at dersom sikkerheten rundt valggjennomføringen svekkes, vil det kunne få svært alvorlige konsekvenser både for valget som en sentral demokratisk ordning, for tilliten til valggjennomføringen og for valgresultatet. Svekket tillit til valggjennomføringen kan oppstå også uten et faktisk sikkerhetsbrudd. Kun en oppfatning blant deler om av befolkningen om tvil ved gyldigheten til valgresultatet vil kunne påvirke tilliten til valggjennomføringen. En mulighet for å sikre en bedre tilgjengelighet for flere, og samtidig begrense risiko for tap en tillit, er å åpne for elektronisk stemmegiving kun for utvalgte velgergrupper. Ikke fordi deres stemmer er

mindre viktige, men fordi et brudd på sikkerheten vil ha lavere økonomiske og samfunnsmessige kostnader i form av redusert tillit, jo færre stemmer det gjelder.

Det varierer hvordan et lands myndigheter, og velgerne i landet, ser på elektroniske- og internettbaserte stemmesystemer. Avveiningen mellom eventuelle gevinster knyttet til brukervennlighet og inkludering, og risikoen knyttet til sikkerhet avhenger i stor grad av landspesifikke forhold, og forhold knyttet til det eksisterende valgsystemet. I tillegg har personlige preferanser betydning. Noen kan være villig til å akseptere sikkerhetsrisikoen som ligger i bruk av elektroniske systemer i bytte mot en valggjennomføring som er bedre tilpasset velgere med særskilte behov. Andre har motsatt syn på denne avveiningen.

Oppsummert finnes en rekke muligheter for å innføre elektronisk stemmegiving, noe erfaringer fra andre land viser. Risikoen er primært knyttet til sikkerhet, mens de mulige gevinstene ligger i bedre inkludering av grupper med særskilte behov, og velgere som ikke er i Norge i perioden valg gjennomføres.



# 1. Kunnskapsinnhentingens bakgrunn, formål og innretning

*Oslo Economics og Norsk Regnesentral har på oppdrag for Kommunal- og distriktsdepartementet gjennomført en kunnskapsinnhenting om elektronisk stemmegiving. Utredningen har identifisert seks hovedkategorier av stemmesystemer, og analysert de seks systemene basert på Europarådets kriterier for innføring av elektronisk stemmegiving.*

## 1.1 Bakgrunn og formål

Norge er et demokratisk konstitusjonelt monarki og befolkningen velger representanter på lokalt, regionalt og nasjonalt nivå. Valggjennomføringen i Norge er angitt av Lov om valg til Stortinget, fylkesting og kommunestyre (valgloven). Valgloven har som formål å legge til rette for at befolkningen skal kunne velge sine representanter til kommunestyre, fylkesting og Stortinget gjennom frie, direkte og hemmelige valg.<sup>1</sup>

Valg til folkevalgte organer i Norge foregår på papir, men under kommune- og fylkestingsvalget i 2011 og stortingsvalget i 2013 ble det gjort forsøk med elektronisk stemmegiving over internett i utvalgte kommuner. Med elektronisk stemmegiving menes løsninger hvor velgere avgir stemmer digitalt. I 2014 besluttet Kommunal- og moderniseringsdepartementet at forsøk med stemmegiving over internett ikke skulle videreføres. Det var manglende politisk enighet om bruk av elektronisk stemmegiving, og for tilliten til valget kan det være uheldig med politisk uenighet knyttet til selve valggjennomføringen (Kommunal- og moderniseringsdepartementet, 2014).

Digitale løsninger, som det elektroniske valgadministrasjonssystemet (EVA), benyttes imidlertid i utstrakt grad av valgmyndighetene ved kommune-, fylkestings-, stortings- og sametingsvalg. Det har også blitt avholdt varianter av elektronisk valg i Norge i forbindelse med skolevalg, valg av universitetsledelse, og nylig i forbindelse med folkeavstemmingen om hvorvidt Innlandet fylke skulle videreføres eller deles opp i Hedmark og Oppland. Disse valgene er gjennomført uten bistand fra sentrale valgmyndigheter, men flere av de rådgivende avstemmingene har anvendt løsninger som ble utviklet i forbindelse med forsøkene i 2011 og 2013.

<sup>1</sup>Gjennomføringen av sametingsvalg er ikke angitt i valgloven, men i Lov om Sametinget og andre samiske rettsforhold, og i Forskrift om valg til Sametinget.

Flere land har de seneste årene innført ulike former for elektronisk stemmegiving ved valg til folkevalgte organer. Dette innebærer både elektronisk stemmegiving i valglokale (kontrollerte omgivelser), og stemmegiving over internett andre steder enn i valglokale (ukontrollerte omgivelser). Eksempler hvor elektroniske stemmemaskiner er tatt i bruk inkluderer nasjonale valg i Brasil og India. Internettstemmegiving har vært brukt ved offentlige valg i både Frankrike, Estland og Sveits.

I 2017 ble det nedsatt et valglovutvalg for å foreslå ny valglov og vurdere endringer i valgordningen (NOU 2020: 6). Utvalget så på og vurderte alle sider ved gjennomføring av valg, blant annet hvorvidt det bør åpnes for å stemme med elektroniske løsninger i Norge. Utvalgets konklusjon var at sikkerheten ved elektronisk stemmegiving ikke var god nok til å innføres i Norge på daværende tidspunkt. Utredningen var på offentlig høring høsten 2020, og et flertall av høringsinstansene støttet valglovutvalgets vurderinger knyttet til innføring av elektronisk stemmegiving. Likevel, utvalget og flertallet av høringsinstansene mente det er nødvendig med videre kunnskaps- og erfaringsinnhenting knyttet til elektronisk stemmegiving i takt med teknologisk utvikling og innføring av løsninger for elektronisk stemmegiving i andre land.

Denne utredningen, gjennomført av Oslo Economics og Norsk Regnesentral, skal gi et oppdatert kunnskapsgrunnlag om bruk av elektronisk stemmegiving. Formålet med utredningen er å gi et grunnlag for å veie muligheter, risikoer, gevinster og kostnader opp mot hverandre.

Utredningen omfatter både elektronisk stemmegiving i valglokale på maskiner med eller uten internetttilkobling (kontrollerte omgivelser) og stemmegiving over internett andre steder enn i valglokale (ukontrollerte omgivelser).

Løsninger for elektronisk stemmegiving i kontrollerte omgivelser omtales i utredningen som *elektroniske løsninger*, mens løsninger for elektronisk stemmegiving i ukontrollerte omgivelser omtales som *internettbaserte løsninger*.

## 1.2 Metode og gjennomføring

Kunnskapsinnhenting er gjennomført i seks steg, illustrert i Figur 1-1. Vurderingene er basert på

omfattende litteraturstudier, intervjuer med utvalgte nøkkelpersoner nasjonalt og internasjonalt, og

diskusjoner med en referansegruppe bestående av valgekspertter.

**Figur 1-1: Kunnskapsinnhentingens seks steg**

1. Utarbeide en generisk stemmeprosess og identifisere mulige variasjoner i stemmeprosessen

2. Identifisere tekniske løsninger og hovedkategorier av stemmesystemer

3. Definere kriterier for analyse av stemmesystemer

4. Analysere stemmesystemer opp mot definerte kriterier

5. Vurdere ressursbruk

6. Oppsummerende vurdering av risiko, gevinster og kostnader

### **Steg 1: Utarbeide en generisk stemmeprosess, og identifisere mulige variasjoner**

Første steg i arbeidet har vært å identifisere en måte å klassifisere stemmesystemer. Vi har gjort dette ved å definere en generisk stemmeprosess, og variasjonene som finnes på hvert steg i stemmeprosessen. Den generiske prosessen består av følgende seks steg:

1. Velgeren registreres for stemmegivning.
2. Det kontrolleres at velgeren er en del av manntallet og har stemmerett.
3. Velgeren avgir stemme til en urne.
4. Stemmene telles og sammenstilles for hvert lokale distrikt.
5. Sammenstilte resultater summeres og publiseres i valgoppgjøret.
6. Velger får bekreftet stemmen (opsjon).

På hvert steg finnes en eller flere mulige variasjoner. Vi har kalt de mulige variasjonene *dimensjoner*. Ett eksempel på en dimensjon er *Lokasjon av opptelling av stemmer*, som er knyttet til steg 4. Alternativene her er enten *lokalt* eller *sentralt*. Stemmeprosessens steg og dimensjoner gir et rammeverk for å beskrive strukturen og essensen av ulike stemmesystemer.

### **Steg 2: Identifisere tekniske løsninger og hovedkategorier stemmesystemer**

Neste steg i arbeidet har vært å identifisere mulige løsninger for stemmegivning, og sortere dem etter stemmeprosessens steg og dimensjoner.

Det finnes tre hovedkategorier av stemmesystemer: papirbaserte systemer, elektroniske systemer og internettbaserte systemer. Basert på gjennomgangen

av aktuelle løsninger har vi definert to undergrupper av hver hovedkategori: klassiske systemer og ende-til-ende-systemer.

Ende-til-ende-systemer muliggjør verifisering av *integriteten* av valgresultatet som helhet, og velgerens mulighet til å kontrollere sin egen stemme er et ledd i å oppnå dette. Valgintegritet innebærer at det ikke skal være mulig å endre avgitte stemmer eller stemmeresultatet. Mer om dette i kapittel 2.

### **Steg 3: Definere kriterier for analyse av stemmesystemer**

På tredje steg utviklet vi et analyserammeverk som tar utgangspunkt i Europarådets anbefalinger (Europarådet, 2017). Europarådets anbefalinger består av 49 kriterier, gruppert i åtte kategorier, og gir land som ønsker å innføre elektronisk eller internettbasert stemmegiving en minimumsstandard for å sikre at prinsippene for gjennomføring av demokratiske valg blir ivaretatt.

Vi har valgt ut kriteriene som er mest relevante for analysen av ulike stemmesystemer og har gjort enkelte tilpasninger. Dette har resultert i totalt 13 kriterier, sortert under de tre hovedkategoriene

- sikkerhet
- transparens og etterprøvnbarhet
- brukervennlighet og inkludering

I tillegg til kategoriene som kan utledes av Europarådets anbefalinger har vi inkludert vurdering av ressursbruk som en egen kategori.

I tillegg til kriteriene som kan utledes av Europarådets anbefalinger, er det tidligere utledet prinsipper for det norske valgsystemet spesielt. Med utgangspunkt i Grunnloven, Norges internasjonale menneskerettslige forpliktelser og prinsippene fra Venezia-kommisjonen utledet Valglovutvalget følgende prinsipper for det norske valgsystemet:

- Valget skal være fritt.
- Valget skal være hemmelig.
- Valget skal være direkte.
- Stemmeretten skal være allmenn og lik.
- Valg skal holdes med jevne mellomrom.
- Alle med stemmerett skal ha mulighet til å stemme.
- Alle med stemmerett skal kunne velges.
- Hver stemme skal ha lik vekt.
- Valgordningen skal sikre geografisk representasjon.

Våre hovedkategorier og kriterier rommer også de relevante prinsippene fra Valglovutvalgets utredning. Dette er nærmere omtalt i kapittel 4.

#### Steg 4: Analysere stemmesystemer opp mot definerte kriterier

I steg fire har vi analysert de tre hovedkategoriene av stemmesystemer opp mot våre kriterier for valg av stemmesystemer. Vi har da vurdert hvert stemmesystem isolert sett, og ikke sett på bruk av kombinasjoner av papirbaserte, elektroniske og/eller internettbaserte systemer i valg gjennomføringen.

Europarådets standarder, som kriteriene bygger på, er i utgangspunktet beregnet på løsninger for elektronisk stemmegiving. I analysen har vi imidlertid inkludert en vurdering av papirbaserte løsninger, representert ved dagens norske valgsystem. Dette for å ha en referanse til vurderingen av elektroniske og internettbaserte systemer.

Det er stor variasjon mellom ulike tekniske løsninger for elektronisk stemmegiving. Når vi vurderer *sikkerhet, transparens og etterprøvnbarhet, og brukervennlighet og inkludering* ved elektroniske og internettbaserte systemer, gjør vi det imidlertid konseptuelt og ikke for bestemte tekniske løsninger. Vi skiller mellom hvorvidt systemene oppfyller kriteriet i stor, noen eller liten grad:

- **I stor grad:** Det er ingen vesentlige utfordringer ved stemmesystemet, og kriteriet er i stor grad oppfylt.
- **I noen grad:** Det er enkelte utfordringer ved stemmesystemet som hindrer oppfyllelse av kriteriet, men utfordringene er ikke vesentlige, eller løsningen muliggjør oppfyllelse av kriteriet på andre vis.

- **I liten grad:** Det er vesentlige og/eller uløselige utfordringer ved stemmesystemer som gjør at kriteriet i liten grad er oppfylt.

Ved at det er *konseptene* elektronisk- og internettbasert stemmegiving som analyseres og ikke konkrete løsninger, er oppmerksomheten rettet mer mot de prinsipielle enn de praktiske sidene ved en eventuell innføring av elektronisk stemmegiving. For å illustrere forskjellen på det praktiske og det prinsipielle kan vi ta utgangspunkt i et internettbasert system. De praktiske/tekniske sidene ved utformingen av et system for internettstemmegiving vil påvirke om løsningen i større eller mindre grad sikrer anonymiteten til velgerne. Internettstemmegiving foregår imidlertid under ukontrollerte forhold, og vil prinsipielt være forskjellig fra stemmegiving på papir når det gjelder anonymitet: Uansett hvordan den tekniske løsningen for internettstemmegiving er utformet, så er det en større risiko for at andre enn velgeren kan følge med på hvilken stemme som avgis (Saglie & Seggaard, 2016).

#### Analyse av sikkerhet

Sikkerhet ved valg, slik det er definert i denne sammenheng, innebærer at velgerne skal kunne være trygge på at stemmene ikke manipuleres på noen måte, at valget er hemmelig, at sensitive data ikke spres, og at alle stemmer telles slik de blir avgitt.

Analysen av *sikkerhet* er gjennomført som en risikoanalyse. Utgangspunktet for risikoanalyser er at «noe kan gå galt». Vi har innledet analysen ved å identifisere mulige hendelser som kan inntreffe på hver dimensjon i stemmeprosessen, og dermed påvirke sikkerheten til ulike stemmesystemer. Vi skiller mellom tilfældige hendelser, utilsiktede hendelser og uønskede tilstander (se Vedlegg A).

Neste steg har vært å definere *omfanget* til hver dimensjonsverdi, og dermed omfanget til en hendelse når noe går galt. Omfang har tre nivåer: personnivå, lokalt nivå og sentralt nivå. Variasjonen mellom nivåene kan illustreres med to eksempler:

- Én dimensjon omhandler hvordan velgeren autentiseres. Denne dimensjonen har fire mulige verdier, vise frem legitimasjon til funksjonær, bruk av elektroniske akkrediter, bruk av biometrisk autentisering eller ingen autentisering. I dette tilfellet er alle fire verdier relatert til *personnivå*.
- En annen dimensjon er om stemmen ble gitt i et lokalt valglokale. Denne dimensjonen har to mulige verdier, enten *Ja, lokalt i valglokale*, som medfører omfang *lokalt nivå*, eller *nei*, som innebærer at stemmen er avgitt i ukontrollerte omgivelser (eksempelvis brevstemmegiving og internettstemmegiving), og betyr et omfang på *personnivå*.

Etter å ha vurdert omfang foretas en risikovurdering som omfatter konsekvens for valg gjennomføringen (hvilken betydning har hendelsen) og sannsynlighet. Disse har fem nivåer hver, som vist i risikomatrisen. Sammenlignet med standarden NIST 800-30 (Joint Task Force Transformation Initiative, 2012) er risikomatrisen justert noe for å gi mer nyansert spredning i risiko.

Omfang og risiko (sannsynlighet og konsekvens) gir til slutt en skår for hvert evalueringskriterium. Prinsippet er at for to ulike stemmesystemer med samme vurderte risiko, men med ulikt omfang, så vil stemmesystemet med kriterier med lavt omfang får bedre skår.

**Figur 1-2: Risikomatrise brukt i sikkerhetsvurderingene**

		Konsekvens				
		Svært liten	Liten	Middels	Stor	Meget stor
Sannsynlighet	Veldig høy	L	M	H	VH	VH
	Høy	L	M	H	VH	VH
	Middels	VL	L	M	H	VH
	Lav	VL	L	M	H	H
	Veldig lav	VL	VL	VL	M	H

Illustrasjon: Oslo Economics og Norsk Regnesentral

### Analyse av transparens og etterprøvnbarhet, og brukervennlighet og inkludering

Transparens og etterprøvnbarhet handler om at valgmyndighetene, velgere og uavhengige valgobservatører skal kunne observere stemmeprosessen, mens brukervennlighet og inkludering handler om at det skal være lave barrierer for å stemme, både for den gjennomsnittlige velger og for velgere med særskilte behov.

Mens vi i vurderingen av sikkerhet gjennomfører en risikoanalyse, gjør vi i analysen av transparens og etterprøvnbarhet og brukervennlighet og inkludering, en kvalitativ vurdering, uten en detaljert utredning av sannsynlighet og konsekvens. Fremgangsmåten for analysen av de to kriteriene er den samme.

### Steg 5: Vurdere ressursbruk

Til forskjell fra analysene av sikkerhet, transparens og etterprøvnbarhet og brukervennlighet og inkludering er ikke analysen av ressursbruk en analyse av stemmesystemer opp mot fastsatte kriterier. Isteden har vi tatt utgangspunkt i dagens valgordning i Norge, og vurdert hvilke implikasjoner det har å tilby elektronisk eller internettbasert stemmegiving som et supplement til dagens papirbaserte system. Forhold som er vurdert er

- materiell, utstyr og systemer
- bemanning og opplæring
- lokaler
- informasjon og veiledning

I vurderingen skiller vi mellom forutsetninger for første gangs innføring og løpende drift, og vi skiller mellom

forutsetninger og kostnader på et lokalt og nasjonalt nivå.

Med lokalt nivå menes kommunalt og fylkeskommunalt nivå. I Norge har kommunene det praktiske ansvaret for gjennomføring av både kommunestyrevalg, fylkestingsvalg, sametingsvalg og stortingsvalg. Det overordnede statlige ansvaret for valg gjennomføringen ligger hos Kommunal- og distriktsdepartementet, mens Valgdirektoratet skal bistå og støtte kommunene og fylkeskommunene i deres praktiske gjennomføring av valg.

### Steg 6: Oppsummerende vurdering av risiko, gevinster og kostnader

Formålet med kunnskapsinnhenting er å gi oppdatert kunnskap om elektronisk stemmegiving i kontrollerte og ukontrollerte omgivelser, og dermed skape et grunnlag for å veie muligheter, risikoer, gevinster og kostnader opp mot hverandre. Med utgangspunkt i analysene gjør vi i siste steg en oppsummerende vurdering av risikoer, gevinster og kostnader ved innføring av elektronisk stemmegiving.

## 1.3 Informasjonskilder

De to informasjonskildene som utredningen i hovedsak er basert på er

- dokumentstudier
- intervjuer

I tillegg har vi underveis diskutert oppdragets problemstillinger med en referansegruppe av valg-eksperter. Informasjonskildene danner grunnlaget for både oversikt og beskrivelsen av de tekniske

løsningene, landerfaringene, og vurdering av styrker og svakheter ved de ulike løsningene.

### Dokumentstudier

Dokumentstudier har vært kjernen i informasjonsinnhenting. I arbeidet har vi tatt utgangspunkt i metoden beskrevet i Hart (2001). De tre trinnene i metoden er

1. søk etter relevante artikler og rapporter ved å bruke forskjellige kombinasjoner av relevante nøkkelord
2. ekstraksjon og systematisering av informasjon fra artiklene og rapportene
3. kvalitetsvurdering av artiklene og rapportene. I det følgende vil vi gå nærmere inn på hva hver av disse trinnene innebærer

### Intervjuer

Som supplement til dokumentstudiene har vi intervjuet utvalgte aktører nasjonalt og internasjonalt. Vi har gjennomført intervjuer med

- Kristian Gjæsteen, Norges teknisk-naturvitenskapelige universitet (NTNU)
- Audun Jøsang, Universitetet i Oslo (UiO)
- Stephane Adamiste, forsker (Sveits)
- Carsten Schürmann, forsker (Danmark)
- Mihkel Solvak, forsker (Estland)
- Cato Lie, Funksjonshemmedes fellesorganisasjon
- Sverre Fuglerud og Terje André Olsen, Blindeforbundet

Intervjuene har vært gjennomført som semistrukturerte intervjuer. Det innebærer at tema og spørsmål varierer naturlig for de ulike intervjupersonene, og at spørsmål og temaer i intervjuguiden kun fungerer

veiledende – dette slik at alle relevante problemstillinger, temaområder og spørsmål blir dekket i løpet av intervjuene.

### Referansegruppe

Referansegruppen har bestått av

- Signe Bock Seggaard, forsker ved Institutt for samfunnsforskning (ISF)
- Jo Saglie, forsker ved ISF
- Dag Arne Christensen, forsker ved Norce

Vi har i prosjektperioden hatt to møter med referansegruppen, det første for å diskutere innretningen på oppdraget, og det andre for å drøfte våre foreløpige funn.

## 1.4 Rapportstruktur

Kapittel 2 beskriver den generiske stemmeprosessen som benyttes for å klassifisere stemmesystemer, mens kapittel 3 anvender stemmeprosessen til å definere og beskriver seks løsninger for stemmegivning, basert på erfaringer fra Norge og andre land.

Kapittel 4 beskriver kriteriene vi anvender i analysen av stemmesystemene, før kapitlene 5, 6 og 7 presenterer analysene av *sikkerhet, transparens og etterprøvnbarhet, og brukervennlighet og inkludering*.

Kapittel 8 drøfter hva som kreves av menneskelige og finansielle ressurser ved innføring elektronisk- og internettbaserte stemmesystemer som et supplement til dagens papirbaserte valggjennomføring, før kapittel 9 gir en oppsummerende vurdering av muligheter, risikoer, gevinster og kostnader knyttet til ulike stemmesystemer.

## 2. Stemmeprosessen

På overordnet nivå har stemmesystemer samme stemme prosess. Den begynner med en kontroll av at velgeren har stemmerett, etterfølges av at velgeren avgir sin stemme, og avsluttes med at stemmene telles og publiseres i valgoppgjøret. Det som skiller stemmesystemer fra hverandre er hvordan stegene i stemme prosessen gjennomføres. I dette kapitlet definerer vi en generisk stemme prosess, gir en inngående beskrivelse av stemme prosessens mulige variasjoner, og drøfter betydningen av kryptografi.

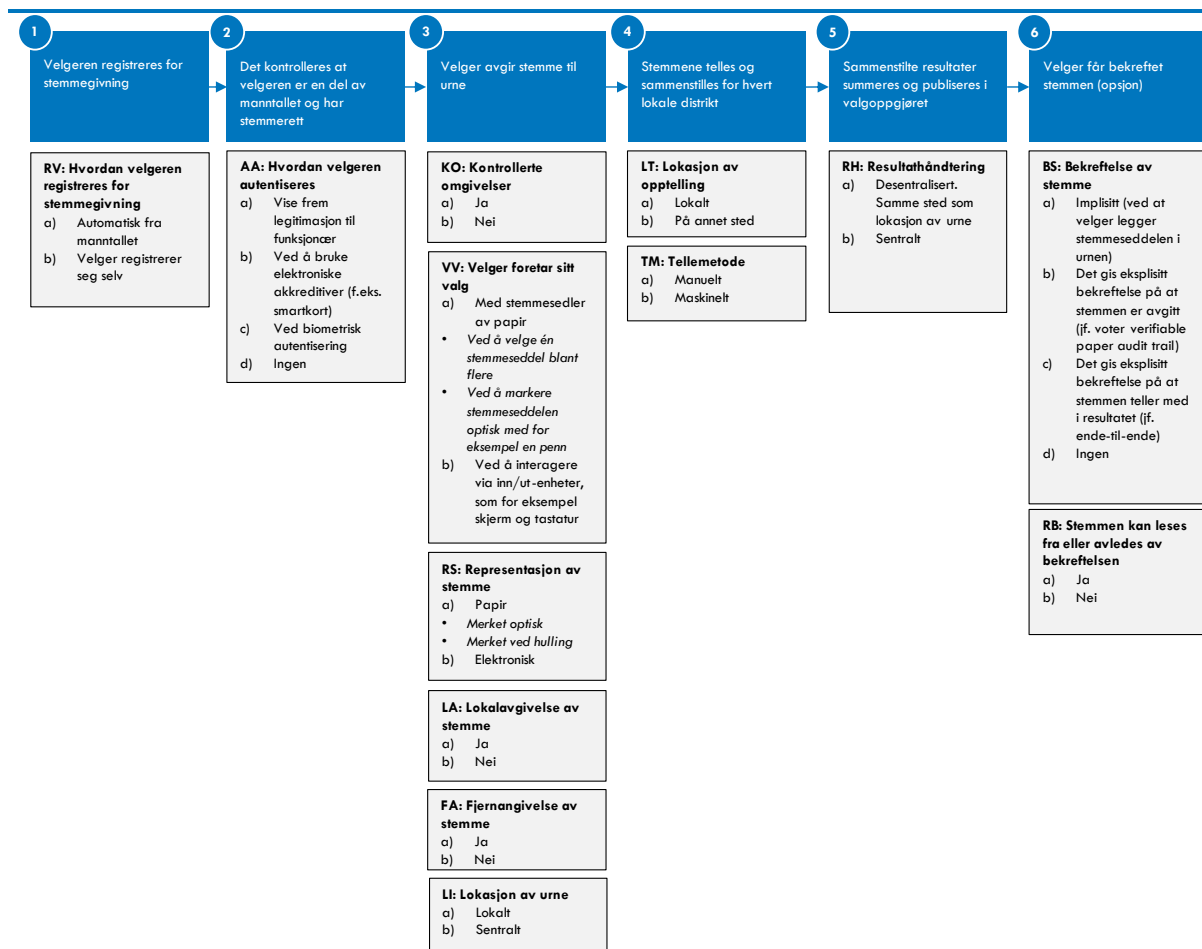
### 2.1 Stegene og dimensjonene i en stemme prosess

Vi har definert en generisk modell for en stemme prosess (Figur 2-1). Selve stemme prosessen har

seks steg, og hvert av stegene kan gjennomføres på en rekke ulike måter. Vi kaller dette *dimensjoner* i stemme prosessen. Modellen gjør at vi kan definere et hvert konkret stemmesystem som en kombinasjon av hvordan systemet svarer ut ulike dimensjoner, og dermed kan vi fange opp strukturen og essensen i ulike stemmesystem. Dette gir et grunnlag for å beskrive og analysere ulike systemer på en systematisk og sammenlignbar måte.

Vi skiller mellom sentraliserte og desentraliserte valg løsninger. Denne distinksjonen er grunnlag for flere av de nevnte dimensjonene, og har avgjørende betydning for hvordan vi vurderer et gitt valg system. Dagens norske valg system er et eksempel på en desentralisert valg løsning. Her avgir velgeren stemmen sin lokalt i et valglokale, som innebærer en desentralisert lokasjon av urne. En sentralisert valg løsning er når det finnes bare en urne for hele valget, som for et nasjonalt valg innebærer at løsningen må være internettbasert.

Figur 2-1: Stegene og dimensjonene i en stemme prosess



Illustrasjon: Oslo Economics og Norsk Regnesentral

## 2.2 Registrering for stemmegiving

### **RV: Hvordan velgeren registreres for stemmegiving**

- a) Automatisk fra manntallet (gjelder i Norge)
- b) Velger registrerer seg selv (for eksempel i USA)

**RV:** Registrering av velger for stemmegiving kan i hovedsak skje på to måter – enten automatisk fra en form for register slik som et manntall vi har i Norge per i dag, eller ved at velgeren må registrere seg selv, slik det er ved for eksempel sametingsvalg i Norge, og ved valg på lokalt, statlig og føderalt nivå i USA (USA.gov, 2022)

Manntallet som ligger til grunn for hvem som kan stemme i Norge overføres til valgadministrasjons-systemet (EVA) fra Skattedirektoratet. Manntallet har flere formål. Det skal sikre at det kun er de med stemmerett som får avgitt stemme, og dessuten at det gir oversikt over hvilken valgkrets den stemmeberettigede tilhører og dermed hvor stemmen skal avgis eller sendes til for å telles.

## 2.3 Velgerens identitet kontrolleres

### **AA: Hvordan velgeren autentiseres**

- a) Vise frem legitimasjon til valgfunksjonær
- b) Ved å bruke elektroniske akkreditiver (f.eks. smartkort, BankID)
- c) Ved biometrisk autentisering
- d) Ingen (ved brevstemmegiving)

**AA:** Autentisering av velger er en mekanisme for bevis på påstått identitet, det vi si at man er den man utgir seg for å være (Kommunal- og regionaldepartementet, 2006).

I prinsippet gjøres autentisering basert på noe velgeren *har*, *vet* eller *er*. Framvisning av legitimasjon til valgfunksjonær og bruk av elektroniske akkreditiver referer til noe velgeren har. I tillegg vil elektroniske akkreditiver ofte også benytte seg av noe velgeren *vet*, slik som et passord ved bruk av BankID. Biometrisk autentisering er et eksempel på autentisering gjennom noe velgeren *er*. Biometriske egenskaper kan være ansiktsform, fingeravtrykk, iris, stemme og lignende.

## 2.4 Velgeren avgir sin stemme

Steket der velgeren avgir sin stemme til en urne kan dekomponeres i ytterligere de tre stegene

- velgeren indikerer sitt valg
- det registreres i manntallet at velgeren har avlagt stemme
- velgeren får en kvittering på stemmen (opsjon)

### **KO: Kontrollerte omgivelser**

- a) Ja
- b) Nei

**KO:** Skillet mellom kontrollerte og ukontrollerte omgivelser er et skille mellom hvorvidt stemmegivingen skjer i valglokaler under kontroll av valgfunksjonærer, eller i ukontrollerte omgivelser utenfor valglokalene.

Hvorvidt det er kontrollerte eller ukontrollerte omgivelser har innvirkninger på en rekke sentrale aspekter som autentisering av velger, ressursbruk i kommunene, og dessuten registrering, overføring, og telling av stemmegiving.

### **VV: Hvordan velgeren foretar sitt valg**

- a) Stemmesedler av papir
  - i. Ved å velge én stemmeseddel blant flere
  - ii. Ved å markere stemmeseddelen optisk med for eksempel en penn
- b) Ved å interagere med inn/ut-enheter, som for eksempel skjerm og tastatur

**VV:** I stemmesystemer som baserer seg på stemmesedler av papir kan velgeren foreta sitt valg ved å velge én stemmeseddel blant flere, eller ved å markere optisk med for eksempel en penn.

For elektroniske løsninger kan det være bruk av pekeskjermer (touch-screen), eller ved å benytte standard datautstyr som en tradisjonell personlig datamaskin der velgeren for eksempel benytter tastatur og mus for å utføre valghandlingen.

**RS: Representasjon av stemme og urne**

- a) Papir
  - i. Merket optisk
  - ii. Merket ved hulling
- b) Elektronisk

**RS:** Representasjon av stemme omhandler i hvilket format stemmen blir avgitt. Et hensiktsmessig skille i denne sammenheng er mellom stemmer i papirformat og stemmer som er elektronisk representert. I papirformat kan stemmene enten være merket ved penn (optisk) eller at det er stemplet inn hull i gitte områder i dem.

**LA: Lokalavgivelse av stemme**

- a) Ja
- b) Nei

**LA:** Under stemmegiving i kontrollerte omgivelser vil stemmeavgivelsen være på samme sted som urnen.

**FA: Fjernavgivelse av stemme**

- c) Ja
- d) Nei

**FA:** Ved stemmegiving i ukontrollerte omgivelser vil lokasjon for å stemme være et annet sted enn urnen. Dette vil være tilfellet ved for eksempel brevstemmegivning og internettbasert stemmegivning.

**LI: Lokasjon av urne; sentralisering kontra desentralisering**

- e) Desentralisert
- f) Sentralt

**LI:** I dagens norske papirbaserte system for kommune-, fylkestings- og stortingsvalg vil stemmene enten bli avgitt eller sendt til en urne der velgeren er manntallsført. Dette innebærer at det er desentraliserte urner. Derimot, ved eksempelvis internettbaserte valg i ukontrollerte omgivelser er det mulig å ha sentraliserte urner.

## 2.5 Stemmene telles

**LT: Lokasjon av opptelling av stemmer (håndtering og transport av stemmer)**

- a) Samme sted som lokasjon av urne
- b) Et annet sted

**LT:** Lokaliseringen av opptelling av stemmer kan skje på samme sted som lokaliseringen av urnen, noe som innebærer at opptellingen skjer desentralisert. På den andre siden kan opptellingen foregå et annet sted enn hvor stemmegivingen foregikk. I slike tilfeller er det nærliggende at opptellingen skjer sentralisert på én eller få lokasjoner.

**TM: Tellemetode**

- a) Manuelt
- b) Maskinelt

**TM:** Opptelling av stemmer kan enten skje manuelt eller maskinelt. Manuell telling innebærer at valgfunksjonærer manuelt vurderer gyldigheten til stemmesedlene, før de teller dem.

Maskinell telling er gjerne en optisk leser som leser trykte og skrevne tegn, eventuelt strekkoder, fra papir og omsetter disse dataene til bitmønstre. I Norge benyttes EVA skanning av kommuner og fylkeskommuner som ønsker å lese stemmesedler maskinelt.

Elektroniske stemmesystemer vil muliggjøre elektronisk telling. Gitt at datamaskinene er programmert på riktig måte vil mulighetene for manuelle feil i opptellingen nærmest forsvinne.

## 2.6 Resultatene publiseres

**RH: Resultathåndtering**

- a) Desentralisert
- b) Sentralt

**RH:** Hvis lokasjon av opptelling av stemmer skjer desentralisert må resultatet formidles til et sentralt hold. Vi omtaler denne prosessen som desentralisert resultathåndtering. Tilfeller der det ikke er nødvendig med denne formidlingen fra lokalt til sentralt hold, omtaler vi som sentralisert resultathåndtering.



## 2.7 Velgeren får bekreftet stemmen (opsjon)

### BS: Bekreftelse av stemme

- a) Implisitt (ved at velger legger stemmeseddelen i urnen)
- b) Det gis eksplisitt bekreftelse på at stemmen er avgitt (jf. voter verifiable paper audit trail)
- c) Det gis eksplisitt bekreftelse på at stemmen teller med i resultatet (jf. ende-til-ende)
- d) Ingen

**BS:** Ved papirbaserte systemer som det norske systemet gis det ingen form for eksplisitt bekreftelse av at stemmen er avgitt eller talt i valgresultatet. Men, selv om det ikke er en eksplisitt bekreftelse gis det ved mange papirbaserte systemer en form for implisitt bekreftelse på at stemmen er avgitt ved at velgeren ser at stemmeseddelen blir lagt i urnen eller avgir den selv.

En metode for å gi verifikasjon for at stemmen er avgitt omtales i litteraturen som voter-verified paper audit trail (VVPAT). VVPAT er en metode for å gi bekreftelse for at stemmen er talt med i elektroniske, stemmeseddelfrie systemer.<sup>2</sup> I VVPAT er det en utskrift av en kvittering til velgeren som gir velgeren en bekreftelse på hva vedkommende har stemt. Denne kvitteringen gir imidlertid *ikke* velgeren en bekreftelse på at den avgitte stemmen er med i valgresultatet. For å oppnå dette kan det brukes en type system som kalles «end-to-end auditable» eller «end-to-end verifiable».

Bekreftelse til velgere på at stemmen er talt er verdifullt i form av at det kan sikre integriteten til valgresultatet. Valgintegritet innebærer at det ikke skal være mulig å endre avgitte stemmer eller stemmeresultatet. Hovedhensikten med ende-til-ende verifisering er å sikre integriteten av valgresultatet som helhet, og velgerens mulighet til å kontrollere sin egen stemme er et ledd i å oppnå dette. Det er tilstrekkelig at en liten andel av velgerne sjekker sin stemme, for at man skal være tilstrekkelig sikker på integriteten til systemet i sin helhet (Benaloh et al., 2014).

Ende-til-ende verifikasjon omfatter to prinsipielle komponenter:

<sup>2</sup> VVPAT er ikke mulig for internettbaserte systemer, ettersom det er avhengig av dedikerte maskiner med en

- Hver velger kan kontrollere at sin valgte stemme har blitt talt opp.
- Hvem som helst kan verifisere at alle gyldige stemmer er blitt talt opp.

Dette er i tråd med Benaloh et al. (2014), og de to prinsippene kan oppnås i tre faser:

1. Avgitt slik intendert - velgerens vilje skal fritt komme til uttrykk
  - Velgere gjør sine valg, og ved tidspunkt for avgivelse kan de få overbevisende bekreftelse på at deres krypterte stemme reflekterer deres valg.
2. Inkludert slik avgitt
  - Velgere kan sjekke at deres krypterte stemmer har blitt korrekt inkludert. Dette kan gjøres ved at velgere finner sin krypterte stemme på en offentlig liste over krypterte avlagte stemmer.
3. Talt slik inkludert
  - Enhver kan sjekke at alle publiserte krypterte stemmer er inkludert i tellingen, uten å vite hvordan noen spesifikke personer har stemt.

Felles for ulike løsninger av dette systemet er at optellingen skjer med en kryptografisk stemme-protokoll, selv om stemmen er avgitt på papir (se avsnitt 2.8 for mer om kryptografi).

Ulike ende-til-ende-løsninger har ulike måter å utføre oppgaver på. I det følgende beskriver vi hvordan et ende-til-ende-system kan se ut.

Ved stemmegiving får velgeren en kryptografisk maskert kopi av sin avlagte stemme. Dette skal gi en bekreftelse på at stemmen er avgitt slik intendert. Det er ønskelig med en kryptografisk maskert kopi av stemmen istedenfor en menneskelesbar kvittering, ettersom en menneskelesbar kvittering kan fungere som et bevis for gitt stemmegiving ovenfor en eventuell tvangsutøver eller ved salg av stemme. Det er derimot en utfordring å overbevise velger om at den maskerte kopien faktisk reflekterer intendert valg.

Det finnes ulike tekniske løsninger for å forsikre velgeren om at stemmen er avgitt slik intendert. En ofte brukt løsning er å tillate velgerne å produsere så mange krypterte stemmegivninger de vil, men hvor velgeren avgir kun én stemme. Dette innebærer at velgeren markerer sitt valg, før den elektroniske løsningen (maskinen) lager en kryptert versjon av stemmegivingen uten å avgi den. I stedet for å avgi stemmen, vil løsningen spørre velgeren hvorvidt den ønsker å avgi stemmen eller å «utfordre» den. Hvis velgeren stoler på at den maskerte kopien av stemmen reflekterer intendert valg kan velgeren velge

papirstrimmel som kan kontrolleres etter stemmegiving er avsluttet.

å avgi stemmen med den krypterte versjon av stemmen. I tilfelle velgeren ikke stoler på maskinen, kan velgeren utfordre den. I så tilfelle vil løsningen gi data som lar velgeren eller utenforstående sjekke at den maskerte kopien faktisk genererer intendert stemmegiving. Dette kan eksempelvis bli gjort ved å bruke en offentlig krypteringsnøkkel. Den sentrale egenskapen ved denne metoden er at maskinen binder seg til en gitt kryptering av stemmen før velgeren avgjør hvorvidt den stemmen skal avgis. Velgeren kan gjennomføre denne prosessen helt til hen stoler på at løsningen avgir stemme slik intendert (Benaloh et al., 2014).

Når stemmeperioden er over publiserer systemet alle de maskerte kopiene av stemmene på en elektronisk oppslagstavle, som kan være en nettside. Publisering gjør at velgeren kan se at stemmen er inkludert, og ikke endret – den er slik den ble avgitt.

I det siste steget vil alle publiserte kryptografiske stemmegivinger gå igjennom kryptografiske protokoller og danne valgresultatet. Her kan enhver sjekke at alle publiserte krypterte stemmegivinger er inkludert i tellingen, uten å vite hvordan noen spesifikke personer har stemt.

**RB: Stemmen kan leses fra eller avledes av bekreftelsen**

- a) Ja
- b) Nei

**RB:** Dette omhandler hvordan en eventuell bekreftelse på stemmen er representert overfor brukeren, noe som har stor betydning for systemets motstandsdyktighet mot press og tvang. Bekreftelsen kan representeres på to prinsipielt forskjellige måter. Den ene er at brukeren kan lese sitt valg direkte fra bekreftelsen eller indirekte utlede dette, for eksempel ved å slå opp på et tilsendt kodeark. Den andre er at brukeren bare kan sjekke at sin stemmeseddel er kommet med i resultat, men uten at det røpes hvilket valg som ble gjort.

## 2.8 Kryptografi i stemmesystemer

Sikkerhet er grunnleggende for alle elektroniske og internettbaserte stemmesystemer, og det er et sentralt premiss at det legges til grunn et sett med veldefinerte sikkerhetskrav ved utforming av slike systemer. Sentralt i IKT-baserte sikkerhetsløsninger er kryptografiske metoder.

<sup>3</sup> Anonymitet er et sikkerhetskrav for elektroniske og internettbaserte systemer. Vi presenterer bakgrunn og innhold i dette kravet i kapittel 4.

Kryptografiske metoder er matematiske metoder som brukes for å «sikre» informasjon, men har ingenting å gjøre med programvaresikkerhet og sårbarheter i dataprogrammer og datasystemer.

Kryptografiske metoder gjelder for data som både sendes over nettverk (i transport) og er lagret.

De vanligste sikkerhetsegenskapene ved kryptering er

- konfidensialitetsbeskyttelse – beskyttelse mot at informasjon blir kjent for uvedkommende
- integritetsbeskyttelse – beskyttelse mot manipulasjon av systemet eller endring av data
- autentisitetsbeskyttelse – sikring av opphavet til informasjonen

De mest grunnleggende typer kryptografiske metoder er kryptering og dekryptering for å sikre konfidensialitetsbeskyttelse, og dessuten kryptografiske signaturer (signering og signaturverifikasjon) for å sikre integritetsbeskyttelse og verifiserbarhet i form av dataautentisering.

Kryptering foregår ved forvansking av en tekst (eller et bitmønster) til en uforståelig såkalt chifftertekst som bare kan dekrypteres ved hjelp av en krypteringsnøkkel. Krypteringsnøkkel er et spesielt bitmønster som brukes som inndata til program kryptering og dekryptering.

Kryptografiske signaturer har den egenskapen at de knytter sammen en person eller annen entitet (vha. denne personens offentlige nøkkel eller digitale sertifikat) mot signerte data og den aktuelle signaturen. Ved å verifisere de signerte dataene opp mot signaturen og personens offentlige nøkkel så kan man fastslå om vedkommende har signert. Digitale signaturer gir samtidig integritetsbeskyttelse i form av en integritetskontroll, for om dataene i etterkant skulle endres, enten på grunn av tilsiktet angrep eller ved utilsiktet feil ved dataoverføringen, så vil verifikasjonen feile.

### 2.8.1 Anonymitetsprotokoller

Et grunnleggende problem ved kommunikasjon i data-nettverk fra et personvernperspektiv er at all slik kommunikasjon vil kunne være sporbar. Et sentralt forhold ved stemmesystemer er at stemmen må avgis på en anonym måte<sup>3</sup>, slik at den ikke kan knyttes opp mot en bestemt velger. Dette er med andre ord det omvendte av dataautentisering nevnt over.

Såkalte mix nets er anonymitetsprotokoller som forutsetter en kjede med flere såkalte proxyservere, og bruk av offentlig nøkkelkryptering. En proxyserver

er en betrodd datamaskin, som i så måte ikke skal kontrolleres av interessenter, det vil si at de må kontrolleres av betrodde og uavhengige parter. Hver avsender krypterer sin melding for hver proxyserver (ved å bruke hver proxyserver sin offentlige nøkkel), slik at den endelige kryptmeldingen består av like mange krypteringer, lag på lag som en løk (meldingslengden er den samme). Hver avsender sender kryptoteksten sin til den første proxyserveren. Hver proxyserver venter til den har mottatt et tilstrekkelig antall kryptotekster, dekrypterer (og slik skreller av et krypteringslag), og sender kryptotekstene videre i tilfeldig rekkefølge til neste proxyserver. På denne måten vil det ikke være mulig for de påfølgende proxyservere eller den endelige mottakeren å knytte meldinger mot den opprinnelige avsenderen, med mindre alle proxyservere unntatt én er kompromitterte eller kollaborerer. Med kompromittert mener vi at en betrodd entitet (datamaskin eller part) ikke er lenger nøytral og uavhengig, men blir brukt av andre parter hvis formål innebærer at et eller flere sikkerhetskrav blir brutt.

### 2.8.2 Forutsetninger ved bruk av kryptografiske stemmeprotokoller

Bruken av kryptografi i et stemmesystem er tverrgående over stegene i en stemmeprosess og dimensjonene. Kryptografiske metoder kan benyttes i elektroniske og internettbaserte stemmesystemer for å sikre de viktigste sikkerhetskravene. Det er uklart hvor mange elektroniske og internettbaserte stemmesystemer som faktisk bruker kryptografiske stemmeprotokoller, men kryptering og kryptografisk signering av stemmer er vanlig. Dette gir ingen anonymitet i seg selv, men forutsetter at det finnes betrodde parter (valgmedarbeidere) som behandler de krypterte stemmene konfidensielt.

Nødvendigheten av betrodde parter er et grunnleggende premiss for alle kryptoløsninger. I et sentralisert system kan dette være en stor svakhet

siden bare én uærlig enkeltperson kan være nok til å kompromittere sentrale deler eller hele systemet. Det samme er tilfelle ved en alvorlig hendelse eller et angrep. I et desentralisert system hvor en hendelse bare rammer lokalt vil konsekvensene derimot bli mye mindre.

Et annet grunnleggende premiss ved alle kryptoløsninger er at nøkkelhåndtering må være sikker. Dette forutsetter at det tas i bruk maskinvarekomponenter som er sikre (som gjør det umulig å gjenskape eller å kompromittere kryptonøkler), lagres sikkert for å hindre kompromittering (grunnet en trusselaktør eller at de på annet vis kommer på avveie), og kryptooperasjoner utføres sikkert.

### 2.8.3 Særlig om bruk av blokkjedeteknologi

Elektroniske og internettbaserte løsninger benytter seg av blokkjedeteknologi<sup>4</sup>. Blokkjedeteknologi gjør det mulig å vedlikeholde en desentralisert transaksjonslogg som kan oppdateres og verifiseres av alle parter og som ikke kan forfalskes av noen part. Man kan dermed skape konsensus om en historikk, selv om ingen part har kontroll over hele systemet. Det er disse egenskapene som ligger til grunn for kryptovalutaer som for eksempel Bitcoin, og de har også gjort at blokkjedeteknologi er blitt sett på som en lovende mekanisme for å gjennomføre elektroniske valg, ved at en blokkjede brukes som elektronisk stemmeurne. En grundigere analyse viser imidlertid at bruken av blokkjedeteknologi til dette formålet kan skape flere problemer enn den løser (Park et al., 2021). Det er vanskelig å drive blokkjeder, de introduserer ekstra kompleksitet i løsningen, oppdateringer av programvaren krever mer tid og innsats, og de er vanskelige å implementere korrekt. På den annen side løser de ikke problemer relatert til hemmelighet, verifiserbarhet, eller manipulasjon av utstyret brukt til stemmegiving.

<sup>4</sup> Et eksempel på dette er løsningen Vocdoni, presentert i delkapittel 3.3

### 3. Mulige løsninger for stemmegiving

Det finnes tre hovedkategorier av stemmesystemer: papirbaserte, elektroniske og internettbaserte, men innenfor disse kategoriene finnes betydelige variasjoner. I dette kapitlet anvender vi dimensjonene i en stemmeprosess til å definere seks løsninger for stemmegiving, og vi gir en beskrivelse av de seks løsningene basert på erfaringer fra Norge og andre land.

#### 3.1 Kategorisering av løsninger

Dimensjonene i en stemmeprosess, presentert i kapittel 2, gir grunnlag for å systematisere systemer eller teknologier i tre hovedkategorier med

stemmesystemer – papirbaserte systemer, elektroniske systemer og internettbaserte systemer. Vi deler videre hver av disse tre hovedkategoriene inn etter to underkategorier – klassiske eller ende-til-ende-systemer.

Innenfor kategoriene kan det være individuelle variasjoner, og det kan også finnes hybrider mellom kategoriene, men de har fellestrekk som gjør at vi anser det egnet å gruppere dem sammen. Tabell 3-1 viser hvordan ulike systemer eller teknologier gjennomfører de ulike dimensjonene, slik beskrevet i kapittel 2. Bokstavene a, b, c eller d refererer til hvordan dimensjonene svares ut. Eksempelvis, bokstaven a, under RV referer til «Automatisk fra manntallet». I det videre gir en beskrivelse av hver kategori, supplert med konkrete eksempler på systemer og teknologier.

Tabell 3-1: Kategorisering av mulige løsninger for stemmegiving

Klasse	System eller teknologi	Land	RV	AA	KO	VV	RS	LA	FA	LI	LT	TM	RH	BS	RB
Klassisk papirbasert	Det norske systemet - valgting	NO	a	a	a	a	a	a	b	a	a(b)	(a)b	a	a	-
	Det norske systemet - forhåndsstemmer	NO	a	a	a	a	a	a	b	a	b	(a)b	a	a	-
	Det norske systemet - brevstemmer	NO	a	d	b	a	a	b	a	b	b	(a)b	a	a	-
Ende-til-ende papirbasert	Scantegrity II	US			a	a	a	a		a	b	b	b	c	b
	PunchScan				a	a	a	a		a	b	b	b	c	b
	Prêt à voter				a	a	a	a		a	b	b	b	c	b
	ThreeBallot				a	a	a	a		a	b	b	b	c	b
	Scratch and Vote				a	a	a	a		a	b	b	b	c	b
Klassisk elektronisk	Det norske forsøket i 2003	NO	a	a	a	b	b	a	b	a	a	b	a	d	-
	NEDAP ES3B	NL		a	a	b	b	a	b	a	a	b	a	d	-
	Diebold AccuVote-TS	US	b	a	a	b	b	a	b	a	a	b	a	d	-
Ende-til-ende elektronisk	ElectionGuard			a	a	(a)b	b	a	b	a		b	b	c	b
	Votebook			a	a	b	b	a	b	a	b	b	b	c	b
	STAR-Vote	US	b	a	a	b	b	a	b	a		b	b	c	b
	vVote	AU			a	b	b	a	b	a		b	b	c	b
Klassisk internettbasert	Det norske forsøket i 2011 og 2013	NO	a	b	b	b	b	b	a	b	b	b	b	b	a
	Det estiske systemet	EE		b	b	b	b	b	a	b	b	b	b	b	a
Ende-til-ende internettbasert	Helios			b	b	b	b	b	a	b	b	b	b	c	b
	Belenios	FR		b	b	b	b	b	a	b	b	b	b	c	b
	Swiss Post	CH		b	b	b	b	b	a	b	b	b	b	c	b
	Vocdoni			b	b	b	b	b	a			b	b	c	b

Kilde: Oslo Economics og Norsk Regnesentral. Note: Strek indikerer at det er et irrelevant felt, mens et blankt felt indikerer at det er ukjent.

#### 3.2 Papirbaserte systemer

Papirbaserte systemer er en utbredt og velprøvd stemmemåte. De fleste sammenlignbare land til Norge benytter seg av papirbaserte systemer. Alle disse systemene er varianter av klassiske papirbaserte systemer. Det er ingen land som benytter seg av ende-til-ende papirbaserte systemer ved nasjonale, lovgivende valg.

##### 3.2.1 Klassiske papirbaserte systemer

Ved klassiske papirbaserte systemer skjer stemmegivingen som regel under kontrollerte forhold, men

den kan lett tilpasses til bruk i ukontrollerte forhold gjennom brevstemmegiving. Systemene kjennetegnes ved at velgeren gjør sitt valg med stemmesedler av papir, og legger stemmeseddelen i en urne. Velgeren får en implisitt bekreftelse på avgitt stemme ved at stemmen legges i urnen, men får ingen form for bekreftelse utover dette på at stemmen er inkludert i optellingen eller talt slik avgitt. Stemmene kan telles opp manuelt, maskinelt eller ved bruk av begge deler.

**Dagens norske valgsystem** er et klassisk papirbasert system. I det norske systemet registreres velgerne automatisk. Dette står i motsetning til for eksempel

valg gjennomføring i USA og sametingsvalget i Norge, der det kreves at velgeren registrer seg for stemmegiving. I Norge sendes det ut valgkort til alle, men det er ikke nødvendig å ha med valgkortet for å stemme.

Når det gjelder selve stemmegivningen er denne i utgangspunktet basert på stemmesedler som legges i en urne under kontrollerte forhold. Dette kan skje enten på **valgdagen** eller ved **forhåndsstemmegivning** i stemmelokale. Det er også mulig med stemmegiving hjemme for personer som ikke kan forhåndsstemme på vanlig måte som følge av sykdom eller uførhet. Dette kalles som ambulerende stemmegivning. For stemmer avgitt i et stemmelokale i forhåndsstemmeperioden må stemmesedlene fraktes og oppbevares frem til de blir talt. Opptellingen av forhåndsstemmer kan starte dagen før valgdagen (Valgmedarbeiderportalen, 2022).

Når en velger som ønsker å stemme i forhåndsstemmeperioden er manntallsført i en annen kommune legges ikke stemmen i en urne. Stemmeseddelen blir lagt i en stemmeseddelkonvolutt, som i sin tur legges i omslagskonvolutt sammen med identifikasjon av velgeren. Denne sendes så i en forsendelseskonvolutt til kommunen der velgeren er manntallsført. Stemmeseddelkonvolutter kan også bli tatt i bruk på selve valgdagen. Dette kan være i kommuner som ikke har elektronisk manntall, stemmegivninger i særskilt omslag slik som når stemmemottakeren ikke finner velger i manntallet eller allerede er krysset av, eller som beredskapsrutine, det vil si ved strømbrydd eller kommunikasjonsbrydd mot manntallet.

Ellers er det også for velgere bosatt i utlandet mulig å bruke **brevstemmegivning**. Til dette brukes samme system av konvolutter, men utføres da kun av velgeren selv under ikke-kontrollerte forhold, og dermed uten autentisering. Disse alternativene, inklusiv fremgangsmåtene, er definert gjennom valgloven ((*Lov om valg til Stortinget, fylkesting og kommunestyre (valgloven)*, 2022) og gjeldende regelverk ((*Forskrift om valg til Stortinget, fylkesting og kommunestyre (valgforskriften)*, 2022). Alternativene støttes av det elektroniske valgadministrasjonssystemet som kommunene og fylkeskommunene benytter, som kalles for EVA. Det er et støtteverktøy kommunene bruker i de ulike fasene av valg gjennomføringen.

Alle kommuner og fylkeskommuner benytter EVA i valg gjennomføringen, men bruken av EVA er ikke lovfestet, og det er derfor ikke obligatorisk for kommunene og fylkeskommunene å benytte systemet. Det er heller ikke obligatorisk for kommunene å benytte seg av hjelpemidlene som Valgdirektoratet tilbyr. Dette innebærer at kommunene og fylkeskommunene kan velge å benytte alternative systemer for å gjennomføre valg. Det er imidlertid ingen kommuner eller fylkeskommuner som har valgt å ikke

benytte EVA (NOU 2020: 6). EVA Admin er hovedapplikasjon for valg gjennomføring. Den inneholder informasjon om manntallsførte velgere og benyttes til å registrere stemmegivninger på velgeren. EVA Skanning blir benyttet av kommuner og fylkeskommuner som ønsker å lese dagens papirbaserte stemmesedler maskinelt framfor å telle manuelt.

Ved stemmegivning i valglokale, enten på valgdagen eller i forhåndsstemmeperioden, må velgeren legitimere seg for valgfunksjonær. Det er ingen formelle krav til legitimasjonen utover navn, fødselsdato og bilde. Dette skiller seg fra forhåndsstemmegivning med brevpost der velgeren ikke legitimerer seg. Dette alternativet er kun tillatt ved stemmegivning fra utlandet og samlet sett utgjør brevstemmene en svært liten andel av stemmene.

På valgdagen og ved forhåndsstemmegivning i velgerens egen kommune, er det stemmesedler for alle partiene som deltar i valget i stemmeavsluttet. Velgeren tar en stemmeseddel for det aktuelle partiet som velgeren ønsker å gi sin stemme til. Velgeren kan eventuelt gi personstemmer ved å endre på stemmeseddelen. Deretter tar velgeren stemmeseddelen med ut fra avsluttet og gir den til stemmemottakeren som stempler seddelen før velgeren legger den i urnen. Det krysses av at velgeren har avgitt sin stemme.

For velgere med synsnedsettelse er det laget en generell stemmeseddel med punktskrift. På den generelle stemmeseddelen er partiene listet opp alfabetisk. Det er risset opp en rute foran partiets navn hvor velgeren setter et kryss. Det følger med en veiledning i punktskrift og storskrift. På denne type seddel er det ikke mulig å endre kandidatene på enkeltpartiers lister (Norges Blindforbund, 2021). Det er heller ikke alle kommuner som tar i bruk den generelle stemmeseddelen (Saglie et al., 2022). Det er ikke krav om at generelle stemmesedler skal brukes i valgforskriften. Forskriften sier at «Blinde og svaksynte velgere skal kunne avgi stemme uten å måtte be om hjelp», Valgforskriftens § 26.

Når stemmeseddelen legges i urnen eller i stemmeseddelkonvolutten får velgeren en implisitt kvittering, i form av at velgeren får muntlig forklart hva som skjer. Velgeren får imidlertid ikke noen form for bekreftelse på at stemmen faktisk er talt opp, og at den teller med i det endelige valgresultatet.

Når det brukes stemmeseddel- og omslagskonvolutt sjekker valgfunksjonæren som til slutt skal åpne konvoluttene opplysningene på omslagskonvolutten mot manntallet og krysser av for at velgeren har stemt. Deretter åpner valgfunksjonæren stemmeseddelkonvolutten og tar ut stemmeseddelen. Åpningen av de to konvoluttene må skje slik at valgfunksjonærene ikke kan vite hva velgeren har stemt.

Kommunene teller opp forhåndsstemmer og stemmer avgitt på valgdagen hver for seg. Alle stemmesedler skal telles minimum to ganger i kommunen. Ved fylkestingsvalg og stortingsvalg kontrollteller fylkeskommunene også stemmesedlene. I opptellingsfasen brukes EVA til å godkjenne tellinger, forkaste stemmesedler, rapportere resultater til media og holde oversikt over opptellingsprosessen i kommunen. Når kommunene teller manuelt, fører de tallene fra opptelling manuelt inn i EVA. Ved maskinell opptelling kommer resultatene inn i systemet gjennom EVA-skanning. Den første opptellingen av stemmesedlene kalles foreløpig telling og skal gjøres manuelt av alle kommuner. Kommunene kan velge om de vil foreta den endelige tellingen manuelt eller ved hjelp av skannere (NOU 2020: 6). Det finnes en veileder for sikkerhetstiltak ved bruk av EVA-skanning, men det er ellers ingen spesielle sikkerhetskrav til maskinene som brukes til optisk avlesning og EVA-skanning (Valgdirektoratet, 2021).

### 3.2.2 Ende-til-ende papirbaserte systemer

Ende-til-ende papirbaserte systemer ligner i utgangspunktet på klassiske papirbaserte systemer, men de er basert på kryptografiske stemmeprotokoller. Dette gjør at velgeren kan få en bekreftelse på at stemmen teller med i resultatet (ende-til-ende verifiserbarhet). Velgeren verifiserer at stemmen er talt med i resultatet gjennom offentlig publisert informasjon.

Det er ikke kjent at ende-til-ende papirbaserte systemer er blitt brukt i stor skala, men systemet Scantegrity II har blitt testet i liten skala (Carback et al., 2010). Det norske valgsystemet er eksempelvis for komplekst til å kunne bruke ende-til-ende papirbaserte systemer. Ende-til-ende papirbaserte systemer er av praktiske forhold ved teknologien begrenset til å sette ett kryss på én felles stemmeseddel. Det er dermed ingen slike systemer som kan brukes til et valg der det avgis både en stemme til et parti og en modifisert rangering av kandidater innen partiet, som for eksempel i det norske systemet.

Når det gjelder implementeringen av ende-til-ende papirbaserte systemer så vil det i stor grad være tilsvarende betraktninger som for klassiske papirbaserte systemer. Autentisering, og dessuten transport og lagring av stemmer kan løses med varierende grad av kvalitet og sikkerhetsnivå.

Eksempler på ende-til-ende papirbaserte systemer omfatter Scantegrity II, PunchScan, Prêt à Voter, ThreeBallot og Scratch and Vote. Felles for disse stemmesystemene er at de er kryptografiske stemmesystem basert på papirstemmesedler, men at de telles opp elektronisk.

**Scantegrity II** (Chaum et al., 2008) er som nevnt et system som har blitt testet i liten skala. Systemet ble

foreslått i 2008 av David Chaum, Peter Ryan, Ronald Rivest og flere andre forskere. Scantegrity II er kompatibelt med eksisterende klassiske papirbaserte stemmesystemer der velgeren gjør sitt valg ved å merke en stemmeseddel optisk, og det kan brukes til å utvide slike systemer med ende-til-ende verifiserbarhet. Dette krever ikke modifikasjon av utstyr for optisk skanning som brukes ved klassiske papirbaserte valg, men det krever bruk av andre typer stemmesedler enn dem som brukes ved slike valg.

Etter autentisering og autorisering får velgeren utlevert en stemmeseddel med et unikt nummer og dessuten en spesialpenn. Velgeren gjør deretter sitt valg ved å bruke pennen til å merke en «boble» ved siden av det aktuelle alternativet. Dette fremkaller en kode skrevet med usynlig blekk i boblen, og denne koden kan kopieres over til en kvitteringsdel som rives av og som også inneholder det unike nummeret. Etter at stemmegivningen er over, publiseres verifikasjonskoden for hvert unike nummer, og velgeren kan verifisere at denne stemmer overens med koden som ble notert på kvitteringsdelen.

Scantegrity II ble testet ved lokalvalget i Tacoma Park i Maryland i 2009. Byen har 11 000 registrerte velgere, og 1 728 av disse stemte med Scantegrity II (Carback et al., 2010). Det ble i denne sammenhengen også testet en tilpasning for fjernavgivelse av stemmer, kalt Remotegrity.

Systemet **PunchScan** er gitt ut som åpen kildekode, og ble utviklet ved University of Ottawa basert på et opprinnelig forslag av David Chaum i 2005.

Systemet bruker stemmesedler bestående av to ark som henger sammen. På det underste laget står det bokstaver i tilfeldig rekkefølge. På det øverste laget står kandidatene forbundet med bokstaver, begge i tilfeldig rekkefølge. I tillegg har stemmeseddelen huller som er plassert slik at bokstavene på det underste arket vises gjennom hullene. Begge lagene er forsynt med det samme, unike ID-nummeret.

Velgeren bruker en farget tusj til å merke det valgte alternativet, slik at tusjen dekker både det øverste og det nederste arket. Når arkene skilles, inneholder ingen av dem nok informasjon til at utenforstående kan finne ut hva stemmen var. Velgeren velger ett av disse arkene og legger det i valgurnen eller skanner det. I tellesystemet finnes det informasjon som kobler hvert ID-nummer til en ordning av kandidater og bokstaver på hvert ark, og dermed kan det regnes ut hva stemmen var. Alle stemmesedler blir publisert offentlig, for eksempel i en avis eller på en nettside, slik at velgeren kan verifisere valget sitt, men utenforstående kan ikke finne ut hva vedkommende har stemt.

**Prêt à Voter** (Ryan et al., 2009), **ThreeBallot** (Rivest, 2006), **Scratch and Vote** (Adida & Rivest, 2006) er

alle eksempler på ende-til-ende papirbaserte systemer som ble utviklet på 2000-tallet. Systemene har sine særegne karakteristika i utforming, men svarer ut dimensjonene i stegene i stemmeprosessen på lik måte.

### 3.3 Elektroniske systemer

I elektroniske systemer skjer stemmegivingen fortsatt i kontrollerte omgivelser, men urne og stemmesedler er skiftet ut med henholdsvis et elektronisk lager og en elektronisk representasjon av stemmene. For velgeren innebærer dette systemet i praksis stemmegivning i valglokaler med ordinære eller spesialtilpassede datamaskiner. I litteraturen er denne typen system kjent som Direct-Recording Electronic (DRE).

#### 3.3.1 Klassiske elektroniske systemer

I klassiske elektroniske systemer gjør velgeren sitt valg ved å interagere med inn-/ut-enheter på en datamaskin. Etter at stemmen er avlagt, lokaliseres den i et lokalt plassert elektronisk lager. Dette kan enten være kryptert eller i klartekst. Den videre overføringen til opptellingssystemet kan også være enten kryptert eller i klartekst.

Autentisering i elektroniske systemer har likhetstrekk med autentisering i papirbaserte systemer, i og med at begge systemene omhandler kontrollerte omgivelser. I elektroniske systemer kan autentisering gjennomføres med varierende kvalitet og sikkerhetsnivå. Autorisasjon til å stemme kan gjøres ved at velgeren får utlevert enten en engangskode eller et smartkort som brukes til å aktivere stemmemaskinen.

Stemmemaskiner har egenskapen at de i stor grad kan tilpasses til eller brukes med hjelpemidler som velgere med funksjonsnedsettelse innehar. Spesielt synshemmede har et ønske om å bruke hjelpemidler og tilpassede løsninger som kan forbedre stemmegivningsprosessen (NOU 2020: 6).

Det norske forsøket i 2003, og dessuten bruk av stemmemaskiner i en rekke land, er eksempler på klassiske elektroniske systemer.

**Det norske forsøket i 2003** var et forsøk med elektronisk stemmegivning ved kommunestyre- og fylkestingsvalget i kommunene Oppdal, Bykle og Larvik og ved lokalstyrevalget i Longyearbyen (Christensen et al., 2004). Forsøkene omfattet til sammen rundt 11 000 stemmeberettigede som kunne velge elektronisk stemmegivning. Den tekniske løsningen, som ble levert av firmaet ErgoEphorma, var datamaskiner med pekeskjerm og utstyr for lesing av smartkort. Evalueringen av forsøket var først og fremst en evaluering av brukervennligheten og den generelle gjennomføringen, der spesielt velgernes reaksjon stod i sentrum. Den tekniske løsningen ble ikke evaluert.

Evalueringen konkluderte med god brukervennlighet, men at løsningen kunne tilpasses bedre til funksjonshemmedes behov. Dette gjaldt særlig synshemmede.

Løsningen fungerte slik at velgerne fikk utdelt et smartkort ved avkrysningen i mantallet og brukte dette til å identifisere seg på stemmemaskinen. Etter at stemmegivningen var avsluttet, ble stemmene overført fra stemmemaskinene over internett til en sentral server, der de ble talt opp.

Det finnes en rekke stemmemaskiner som er tatt i bruk i ulike land. De deler mange av de samme egenskapene, og vi fremhever noen eksempler på anvendte løsninger og erfaringer ved bruk.

**NEDAP/Groenendaal ES3B** (Gonggrijp & Hengeveld, 2007) er et eksempel på et elektronisk system. Maskinen har vært brukt til elektronisk stemmegivning i Nederland. NEDAP produserer maskinen, mens Groenendaal produserer programvaren som kjøres i maskinen. Velgeren interagerer med maskinen for å avgi sin stemme, som lagres i en minnemodul. Da løsningen ble anvendt i Nederland foregikk opptellingene av stemmene i hvert valgdistrikt ved at resultatene fra maskinene ble summert og lagt sammen med manuelle stemmer.

Nederland brukte elektroniske stemmemaskiner i flere valg frem til 2008. Maskinene var plassert i stemmelokaler, det vil si i kontrollerte omgivelser. Flere hendelser førte til at bruken av maskinene etter hvert ble avvirket. Blant annet lagde maskinene lyder som gjorde at det var mulig for de andre som sto i valglokalet å identifisere hva velgeren hadde stemt på. I tillegg var det utfordringer ved at velgerne ikke forstod om de hadde avgitt stemme eller ikke. Det førte blant annet til at en valgmedarbeider i et stemmelokale gikk inn etter at velgeren trodde de hadde stemt, og endret valgene deres. En aktivistgruppe skaffet en av stemmemaskinene, og viste at den var sårbar for enkel manipulasjon (Loeber, 2008).

Et annet land som har benyttet seg av elektroniske stemmemaskiner er USA. **Diebold AccuVote-TS** (Feldman et al., 2006) er den stemmemaskinen som er mest utbredt i USA med mer enn 33 000 maskiner i drift. Når en velger skal bruke en stemmemaskin i USA, blir maskinen aktivert av en valgmedarbeider for å sikre at hver velger bare stemmer én gang. Etter at velgeren har stemt blir stemmedataen lagret på en minnekomponent, slik at den kan bli kopiert ut av stemmesystemet.

Andre land med erfaring med stemmemaskiner inkluderer land som India, Brasil og Frankrike.

I India har bruk av stemmemaskiner vært omtalt som et vellykket system. Maskinene bidro i stor grad til å

gjøre administrasjonen, gjennomføringen og opp-tellingen av valg mer effektiv og pålitelig, spesielt sett i sammenheng med de store massene som avlegger stemme ved nasjonale valg (over 600 millioner). Fra oppstarten på 1980-tallet og utover på 2000-tallet var det også stor tillit til systemets sikkerhet. Det ble senere rettet et mer kritisk blikk på sikkerheten til systemet og mangler ved offisielle tekniske evalueringer av systemet (Wolchok et al., 2010).

Brasil startet med elektronisk stemmegivning i 1996 og var det første landet med helelektronisk valg i 2000. Som følge av dette beskrives landet gjerne som en pionér i denne sammenheng. Tilsvarende som for India, ble implementeringen i 2000 i flere fora ansett som en suksess, mens det i nyere tid har vært rettet kritikk mot systemets sikkerhetsmekanismer og andre forhold knyttet til transparens og etterprøvnbarhet. Ytterligere kritiserer deler av litteraturen stemmesystemet i form av at det ikke har hatt den ønskede effekten på valgdeltakelse og tillit til det politiske systemet, til tross for store investeringer (Aranha & van de Graaf, 2018).

Frankrike har brukt elektroniske stemmemaskiner siden tidlig 2000-tall. Det er kun i bruk i 60 kommuner, og tilgjengelig for 2 prosent av stemmeberettigede. Det ble rettet omfattende kritikk mot stemmemaskinene under valget i 2007. Kritikken dreide seg om sikkerhet generelt, men også til spesifikke forhold som transparens, sertifisering og etterprøvnbarheten til maskinene. Kritikken medførte at franske myndigheter fryste innføring av stemmemaskiner i kommuner som ikke allerede hadde tatt de i bruk, og situasjonen har stått uforandret siden (Enguehard & Noûs, 2020).

### 3.3.2 Ende-til-ende elektroniske systemer

Ende-til-ende elektroniske systemer har store likhetstrekk med elektroniske systemer, men de er basert på kryptografiske stemmeprotokoller, noe som gjør at velgeren kan få en bekreftelse på at stemmen teller med i resultatet. Det er stor grad av overlappende betraktninger for ende-til-ende elektroniske systemer som for klassiske elektroniske systemer når det gjelder implementering.

Ende-til-ende-systemer flytter i praksis alt ansvar for valgintegriteten til selve opptellingen av stemmene. Hvis man skulle konstruere et svært enkelt ende-til-ende-system for en forenklet versjon av det norske valget, kunne man publisere en tabell der hver rad er et fødselsnummer og hver kolonne er et politisk parti. Stemmene legges inn som kryss i tabellen, og vi kan dermed telle opp hvor mange stemmer hvert parti har fått. Valgintegriteten er beskyttet ved at hver velger kan verifisere at sin egen stemme er korrekt og at alle kan verifisere at kryssene er korrekt talt opp. Hvordan stemmene formidles til denne tabellen spiller ingen rolle for valgintegriteten, slik at man trenger ikke å ha

tillit til hvordan dette skjer. Dette systemet gir altså svært god valgintegritet, men ingen anonymitet. Det komplette ende-til-ende-systemer i praksis gjør, er å beholde disse egenskapene som gir valgintegritet, men samtidig bruke forskjellige kryptografiske metoder for å anonymisere stemmene. Dermed oppnår man både høy valgintegritet og anonymitet.

Vi kjenner ikke til at ende-til-ende elektroniske systemer er blitt brukt i stor skala, men ulike systemer har blitt testet i mindre skalaer, deriblant valg på regionalt nivå i land.

Eksempler på ende-til-ende elektroniske systemer inkluderer ElectionGuard, Votebook, STAR-Vote og vVote.

**ElectionGuard** (Election Guard, 2022) er en programvareutviklingspakke utgitt som åpen kildekode, som kan brukes til å lage papirløse kryptografiske stemmesystemer. Systemet ble utviklet av Microsoft i samarbeid med Galois i 2019.

**Votebook** (Kirby et al., 2016) er et papirløst kryptografisk stemmesystem beregnet på bruk i kontrollerte omgivelser. I motsetning til de andre eksemplene, er Votebook basert på blokkjedeteknologi. Blokkjedeteknologi gjør det mulig å vedlikeholde en distribuert transaksjonslogg som kan oppdateres og verifiseres av alle parter og som ikke kan forfalskes av noen part. Det er disse egenskapene som ligger til grunn for kryptovalutaer som for eksempel Bitcoin.

Det siste eksempelet, **STAR-Vote** (Bell et al., 2013), er et elektronisk kryptografisk stemmesystem beregnet på bruk i kontrollerte omgivelser. Systemet ble utviklet i 2013 under ledelse av Travis County i Texas.

Ett særtrekk ved STAR-Vote er at selv om velgeren interagerer med en maskin med inn-/ut-enheter og stemmen registreres elektronisk, blir det skrevet ut en stemmeseddel, som velgeren da avgir ved å skanne den ved en dertil egnet stasjon. Den elektroniske stemmen blir ikke gyldig før stemmeseddelen er skannet. Eventuelt kan velgeren ugyldiggjøre stemmen og bruke den som en teststemme for å kontrollere systemet.

**vVote** (Burton et al., 2016; Eldridge, 2018) er et elektronisk kryptografisk stemmesystem beregnet på bruk i kontrollerte omgivelser. Det er utformet som en elektronisk versjon av det papirbaserte systemet Prêt à Voter og ble brukt ved delstatsvalget i Victoria i Australia i 2014. Systemet har også tilpasninger som gjør at det kan brukes av blinde og svaksynte.

## 3.4 Internettbaserte systemer

Internettbaserte systemer er i denne sammenheng elektronisk stemmegivning under ukontrollerte forhold.



Det kan beskrives som det elektroniske motstykket av brevstemmegiving i papirbaserte systemer.

### 3.4.1 Klassiske internettbaserte systemer

Ved et internettbasert system stemmer velgeren under ukontrollerte forhold, via nettleser på personlig datamaskin eller gjennom en app på mobiltelefonen. Stemmene legges inn i et sentralt elektronisk lager, og telles opp maskinelt.

Velgeren autentiseres med elektroniske akkreditiver. Autentisering av velger og overføring av stemme til urnen kan gjøres med varierende kvalitet og sikkerhetsnivå. Etter at stemmen er avgitt kan den legges inn i urnen enten kryptert eller i klartekst. Den videre overføringen til opptellingssystemet kan også være enten kryptert eller ukryptert.

Tilsvarende som for elektroniske systemer kan internettbaserte systemer tilpasses, eller brukes med hjelpemidler for velgere med funksjonsnedsettelse.

**Det norske forsøket i 2011 og 2013** var forsøk med internettbasert stemmegiving i et kommune- og fylkesvalg og i et stortingsvalg (Segaard et al., 2014). Forsøkene omfattet til sammen rundt 168 000 og 250 000 stemmeberettigede som kunne velge internettbasert stemmegiving. Systemet ble kun brukt til forhåndsstemmeperioden. Velgerne kunne avgis flere stemmer via internett og den sist avgitte stemmen ble tellende i valgoppgjøret. Velgerne kunne også stemme papirbasert, i forhåndsstemmeperioden eller på valgdagen, og det var da papirstemmen som ville telle.

Systemet ble utviklet av det spanske selskapet ScytI, bortsett fra tjenesten som håndterer manntallet, som ble utviklet av Ergo.

For å stemme via Internett måtte stemmegiver bruke en nettleser og åpne nettsiden "valg.stat.no" Deretter autentiserte velgeren seg med MinID eller et godkjent smartkort. I forsøket i 2013 var også BankID et av autentiseringsalternativene. Velgeren fikk deretter tilsendt en kvittering på SMS. Kvitteringen inneholdt verifikasjonskoder, et tall som kunne brukes til å sjekke hvilke parti velgeren har stemt på, og at stemmen ble mottatt. Alle velgere i kommunene med elektronisk valg som supplement til den ordinære stemmemåten fikk et valgkort med koder. Disse kodene og tallene var unike for hver enkelt velger og på denne måten kunne velgeren bruke informasjonen i SMS-en til å dekode eller sammenlikne koden med kodene på valgkortet.

Bruk av koder for autentisering og verifisering er fortsatt aktuelle løsninger for bruk i elektroniske stemmesystem. Sveits er et land som har gjort omfattende forsøk med elektronisk stemmegiving. Flere ulike stemmesystemer har vært i bruk samtidig.

Siden 2005 har 15 kantonene i Sveits tilbudt internettstemmegiving til deler av sine velgermasser, og totalt 300 forsøk har blitt gjennomført (Swiss Federal Chancellery, 2022). Spesielt systemene i kantonene Genève og Neuchâtel har vedvart over tid og er i dag kjent som Genève-systemet og Swiss post-systemet (Applegate et al., 2020). Etter lovendringer som sikrer mer innsyn i kildekoden til de ulike systemene, ble Swiss Post systemets kode gjort tilgjengelig i 2019. Dette avdekket flere sikkerhetshull, og førte til debatt rundt internettstemmegiving og sikkerhet i Sveits. Per 2022 planlegger enkelte kantonene å gjeninnføre en redesignet versjon av Swiss Post-systemet. I den nye versjonen står utsendelser av koder til velgere sentralt med tanke på både autentiserings- og verifiseringsformål. Vi beskriver denne nye versjonen mer inngående i neste delkapittel, ettersom det kan beskrives som et ende-til-ende-system.

**Det estiske systemet** er basert på elektroniske stemmer som avgis under ukontrollerte forhold (Springall et al., 2014). Velgeren laster ned en app til sin personlige datamaskin og bruker denne til å avgis stemmen. For autentisering belager systemet seg primært på Estlands nasjonale ID-kort, som er et smartkort som er i stand til å utføre kryptografiske operasjoner og brukes til å autentisere og autorisere velgeren. Alternativt finnes det også et system som kalles Mobile-ID, som er basert på mobiltelefon og SIM-kort, men dette er mye mindre brukt.

Protokollen ligner på bruken av stemmeseddel-konvolutt og omslagskonvolutt. Stemmen krypteres og signeres elektronisk av velgeren. Deretter sendes dette over en sikker forbindelse (TLS) til sentrale maskiner. Velgeren får returnert en unik ID som refererer til den krypterte stemmen. Ved å sende inn denne ID-en, kan velgeren få returnert den krypterte stemmen og dermed kontrollere at den krypterte stemmen er blitt registrert som avgitt. Det er mulig å stemme flere ganger, og det er kun den siste stemmen som teller. Velgeren får altså en kvittering på at stemmen er avgitt, men kan ikke verifisere at den teller med i resultatet.

De krypterte stemmene lagres sammen med velgerens identitet på sentrale maskiner, og når stemmegivningen er avsluttet sjekkes velgerens elektroniske signatur på hver stemme. Deretter skrives alle de krypterte stemmene uten identifiserende informasjon på en DVD, som fraktes til en tellemaskin på et offentlig sted. Her blir stemmene dekkryptert og talt opp, og valgoppgjøret skrives ut.

### 3.4.2 Ende-til-ende internettbaserte systemer

Ende-til-ende internettbaserte systemer kjennetegnes av mange av de samme særtrekkene som klassiske internettbaserte systemer, men de er basert på kryptografiske stemmeprotokoller, noe som gjør at

velgeren kan få en bekreftelse på at stemmen teller med i resultatet.

**Belenios**, et internettbasert, kryptografisk stemmesystem, er blitt brukt ved valg til lovgivende forsamling i Frankrike i juni 2022. I Belenios får velgeren tilsendt akkreditiver gjennom elektronisk post. Disse brukes til å gjennomføre stemmegivningen i en nettleser, og velgeren får en kvitteringskode som kan sjekkes mot publiserte elektroniske stemmesedler. Velgeren kan avgis sin stemme flere ganger, slik at det bare er den siste som teller.

Belenios er basert på systemet **Helios** (Adida, 2008). Helios er et internettbasert, kryptografisk stemmesystem som er utgitt som åpen kildekode. Systemet ble foreslått av Ben Adida ved Harvard University i 2008.

Internettstemmegiving har vært et omtalt tema i Frankrike, spesielt de siste ti årene. I 2012 fikk franskmenn bosatt i utlandet for første gang lov til å stemme elektronisk over internett ved nasjonale valg. Dette var riktignok kun for parlamentsvalg og ikke presidentvalg. Elektronisk stemmegiving var et supplement til å bruke papirstemmesedler, men velgerne fikk kun lov til å stemme én gang. I 2017 ble muligheten for internettstemmegiving for personer bosatt i utlandet suspendert etter bekymringer om sikkerheten i systemet og faren for hackerangrep og manipulasjon av valget (NOU 2020: 6). I 2020 reintroduserte Frankrike internettstemmegiving for velgere bosatt i utlandet, men kun for visse deler av valgsystemet.

I arbeidet med å forbedre **Swiss Post**-stemmesystemet, som enkelte kantonene i Sveits planlegger å benytte, er det ønske om å sikre ende-til-ende verifisering. Systemet fungerer slik at hver velger på forhånd får tilsendt et ark med koder som brukes til å gjennomføre stemmegivningen i en nettleser. En stemmegivning inneholder typisk flere spørsmål som er oppe til votering. Stemmegivningen skjer i to faser: først gjør velgeren et valg med koder for å svare på alle spørsmålene, og deretter brukes en spesiell kode for å gjøre valgene endelige. Til slutt får velgeren tilsendt en kvitteringskode som skal stemme overens med en kode som er trykket på kodearket. I motsetning til flere andre stemmesystemer i samme kategori, er en avgitt stemme endelig og kan ikke endres senere.

Foreløpige funn fra undersøkelser av løsningen viser at systemene som er foreslått kommer til kort på enkelte områder, inkludert dokumentasjon, sikkerhetsarkitektur og implementasjon av sikkerhetsprotokollen, men at de tekniske utfordringene fremstår som mulige å håndtere (Ford, 2022). De uavhengige undersøkelsene påpeker også at løsningene vil fremstå uperfekte når de måles opp imot et teoretisk ideal, mens at systemet i stor grad oppnår sine spesifiserte målsetninger basert på hvilke trusler som systemet er ment å skulle motstå.

Et annet ende-til-ende internettbasert stemmesystem er Vocdoni (Aragon, u.å.), et internettbasert, kryptografisk stemmesystem basert på blokkjedeteknologien Ethereum.

## 4. Vurderingskriterier for elektroniske stemmesystemer

*Europarådet har etablert kriterier for innføring av elektronisk stemmegiving. Disse gir land som ønsker å innføre elektronisk stemmegiving en minimumsstandard for å sikre at prinsippene for gjennomføring av demokratiske valg blir ivaretatt. Dette kapitlet gir en beskrivelse av hvordan vi har tilpasset og supplert Europarådets kriterier til bruk i analysen av ulike elektroniske og internettbaserte løsninger for stemmegiving i Norge.*

### 4.1 Bakgrunn og utarbeidelse av vurderingskriteriene

Norsk lov forutsettes å være i samsvar med internasjonal rett. Prinsipper for demokratiske valg gjenspeiles i en rekke internasjonale forpliktelser. På valgområdet er det forpliktelser gjennom samarbeidet i Europarådet som er av størst betydning (Kommunal- og regionaldepartementet, 2006).

Europarådet ble opprettet i 1949 og har 46 medlemsland, deriblant Norge (Store Norske Leksikon, 2022). Den viktigste oppgaven for Europarådet i dag er å verne om menneskerettigheter, demokrati og rettsstatsprinsippet. Samarbeidet i Europarådet har resultert i et nettverk av internasjonale avtaler og konvensjoner, deriblant den europeiske menneskerettighetskonvensjonen og «Kodeks for god valgpraksis». Europarådets kriterier for innføring av elektronisk stemmegiving, som danner fundamentet for vurderingskriteriene, kan utledes fra nevnte konvensjon og kodeks.

#### 4.1.1 Den europeiske menneskerettighetskonvensjonen

Det er en forutsetning for å bli medlem av Europarådet at landet ratifiserer den europeiske menneskerettighetskonvensjonen. Den europeiske menneskerettighetskonvensjonen fra 1950 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 ikke bare til forpliktelsen om å 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 stemmegiving sikres. I tillegg skal stemmegivingen foregå 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 dermed muligheter for skjønnsutøvelse når betingelsene for universell stemmerett og valgsystemet fastsettes. Slike begrensninger og vilkår må imidlertid tjene legitime formål (Kommunal- og regionaldepartementet, 2006).

#### 4.1.2 Kodeks for god valgpraksis

Kodeks for god valgpraksis fra 2002 gir retningslinjer for gjennomføring av valg i medlemsstatene i Europarådet. Kodeksen er fastsatt av Venezia-kommisjonen, som er opprettet av Europarådet. Venezia-kommisjonen er den europeiske kommisjonen for demokrati gjennom lovgiving.

Kodeks for god valgpraksis definerer «European electoral heritage» gjennom to aspekter. Det første kan beskrives som konstitusjonelle prinsipper som er felles for europeiske valg – retten til alminnelige, like, frie, hemmelige og direkte valg. I Europa kommer dette til uttrykk gjennom den europeiske menneskerettighetskonvensjonen art. 3. Det andre aspektet omhandler grunnleggende forhold som må være på plass slik som rettsikkerhet, respekt for fundamentale rettigheter, og dessuten stabilitet i valglovgivingen.

#### 4.1.3 Europarådets anbefaling for elektronisk stemmegiving

I 2004 utga Europarådet en anbefaling med kriterier for innføring av elektronisk stemmegiving. Anbefalingen er ikke juridisk bindende, men gir generelle juridiske, tekniske og operasjonelle retningslinjer for elektronisk og internettbasert stemmegiving. Anbefalingen bygger på *Kodeks for god valgpraksis* fra 2002, og adresserer tematikk som er ansett som relevant for elektronisk og internettbasert stemmegiving spesielt. Hensikten med retningslinjene er å gi land som ønsker å innføre elektroniske valg minimumsstandarder å ta utgangspunkt i. Dette for å bidra til å sikre at prinsippene for gjennomføring av demokratiske valg blir ivaretatt. Europarådet poengterer imidlertid at selv om anbefalingen følges, så gir de ingen garanti for den demokratiske kvaliteten til elektroniske valg. Nasjonal lovgiving kan trenge ytterligere krav, og et elektronisk valg må bli vurdert helhetlig og i detalj, ut fra kontekst. Likevel vil etterfølgelse av anbefalingene være et viktig steg i

retning av å sikre demokratisk kvalitet i valg gjennomføring.

Da anbefalingene fra Europarådet kom i 2004, var det få europeiske land som hadde erfaring med elektronisk stemmegiving. Følgelig var anbefalingene i større grad basert på teoretiske prinsipper enn på praktisk erfaring. I 2017 kom en oppdatert versjon som utvidet definisjonen av elektroniske valg til å også omfatte maskinell opptelling av stemmer (Europarådet, 2017).

Den oppdaterte versjonen har tatt hensyn til utviklingen på feltet de siste par tiårene. Nye, strengere anbefalinger om risikohåndtering er tatt inn, og tematikk knyttet til autentiseringsmekanismer, verifiserbarhet, etterprøvnbarhet og åpenhet er i større grad dekket i den oppdaterte versjonen. Dette kommer blant annet som følge av at denne type vurderinger har blitt mer relevante etter framveksten av internettbaserte løsninger.

Europarådet anbefaler at elektroniske og internettbaserte valgsystemer innføres gradvis, med en mulighetsstudie og grundig testing før det anvendes ved valg.

Anbefalingene omfatter totalt 49 kriterier<sup>5</sup> som Europarådet grupperer i åtte kategorier (våre oversettelser i parentes):

- Universal suffrage (universell stemmerett)
- Equal suffrage (lik stemmerett)
- Free suffrage (fri stemmerett)
- Secret suffrage (hemmelig avstemming)
- Regulatory and organisational requirements (regulatoriske og organisatoriske krav)
- Transparency and observation (transparens og observasjon)
- Accountability (ansvar)
- Reliability and security of the system (pålidelighet og sikkerhet ved systemet)

#### 4.1.4 Utarbeidelse av vurderingskriterier

Blant de 49 kriteriene har vi definert et mindre utvalg kriterier som vi anser er relevante for analysen av stemmesystemene. Vi har utelatt kriterier som omhandler andre forhold enn egenskaper ved systemene, slik som anbefalinger knyttet til gjennomføring av elektroniske og internettbaserte valg generelt. Vi har gruppert kriteriene under færre, men bredere kategorier. De tre kategoriene er<sup>6</sup>

- sikkerhet

<sup>5</sup> Europarådet omtaler det som «standards» sin anbefaling, mens vi omtaler det som «kriterier» i denne rapporten.

<sup>6</sup> Kriterier i Europarådets anbefaling som omhandler universell, lik og fri stemmerett, og dessuten hemmelig avstemming inngår i analysene, selv om de ikke direkte kan avleses fra kategoriseringen. Prinsippene om universell, lik,

- transparens og etterprøvnbarhet
- brukervennlighet og inkludering

I tillegg har vi inkludert en kategori som går på *ressursbruk*. Forhold knyttet til ressursbruk kan ikke utledes direkte fra Europarådets anbefalinger. Kunnskap om ressursbruk er imidlertid viktig for å kunne vurdere muligheter, risikoer, gevinster og kostnader ved elektronisk stemmegiving, og er derfor inkludert i kunnskapsinnhentingen.

Europarådets anbefalinger er beregnet på løsninger for elektronisk stemmegiving. Men som redegjort for innledningsvis vil vi i vår analyse også vurdere papirbaserte løsninger. Dette gjør vi for å ha en referanse å vurdere elektroniske og internettbaserte løsninger opp imot.

## 4.2 Sikkerhet

Sikkerhet ved valg innebærer at velgerne skal være trygge på at stemmene ikke manipuleres på noen måte, at valget er hemmelig, at sensitive data ikke spres, og at alle stemmer telles slik de blir avgitt (NOU 2020: 6). Kategorien *sikkerhet* er ment å fange opp at tilsiktede eller utilsiktede hendelser kan ramme hele eller deler av stemmeprosessen eller valgtutfallet. Tilsiktede hendelser kan ha sitt utspring hos enkeltpersoner, grupper eller fremmede makter som ønsker få innsyn i velgeres valg, påvirke eller så tvil om valgtutfallet. Utilsiktede hendelser kan skyldes uhell, som igjen avhenger av hvilken løsning som anvendes. Kategorien *sikkerhet* består av følgende kriterier:

fri stemmerett og hemmelig avstemming er innlemmet i kategoriene sikkerhet, transparens og etterprøvnbarhet, og brukervennlighet og inkludering. Som tidligere nevnt, er utarbeidelsen av kriterier for analysen, og kategoriseringen av disse, utformet med hensikt om å være tjenlig for analyseformål.

**Fravær av påvirkning** – ingen foreløpige resultater skal kunngjøres før stemmegivingen er avsluttet

**Autentisering** – mulige velgere skal autentiseres slik at kun stemmeberettigede kan stemme

**Anonymitet** – det skal ikke være mulig å finne ut hvem som har stemt på hvem

**Motstand mot tvang** – det skal ikke være mulig å presse en velger til å stemme på bestemte måter

**Lik stemmerett** – det skal kun være mulig å avgi maksimalt en stemme (eller samme antall stemmer) per velger

**Valgintegritet** – det skal ikke være mulig å endre avgitte stemmer eller stemmeresultatet

**Korrekthet** – stemmene må telles opp korrekt og stemmeresultatet må publiseres korrekt

#### Verifiserbarhet

- Hver velger kan kontrollere at sin valgte stemme har blitt talt opp
- Hvem som helst kan verifisere at alle gyldige stemmer er blitt talt opp

**Tilgjengelighet** – Stemmesystemet må være tilgjengelig i samsvar med foreskrevne stemmeperiode

Kriteriene danner grunnlaget for den sikkerhetsmessige utformingen av stemmesystemer, og de nevnte kriteriene gjelder også for kryptografiske stemme-protokoller.<sup>7</sup> En vesentlig forskjell mellom e-stemmesystem og papirbaserte metoder er at riktig bruk av kryptografi i e-stemmesystemer direkte kan realisere enkelte sikkerhetskrav som ellers vil være under menneskelig og/eller maskinell kontroll, som eksempelvis anonymitet og integritetsbeskyttelse. Andre kriterier er av en funksjonell og systemorientert art, som for eksempel tilgjengelighet (stemmesystemet må være tilgjengelig i samsvar med foreskrevne stemmeperiode) og stemmeberettighet (autentisering). Disse kravene kan ikke oppnås eller sikres ved kryptografi.

Kriteriet anonymitet innebærer at det ikke skal være mulig å finne ut hvem som har stemt på hvem, og er relevant både under og etter stemmegiving. For analyseformål er anonymitet under stemmegiving (hemmelig stemmegiving) avgrenset til vurdering om anonymitet for den allmenne velger. Forhold knyttet til hemmelig stemmegiving for velgere med særskilte

behov dekkes av *brukervennlighet og inkludering* (se kapittel 4.4).

Kriteriet anonymitet er videre knyttet til kjøp og salg av stemmer. Verdien av kjøp og salg av stemmer er begrenset når det ikke er mulig å finne ut hva en person har stemt (Saglie & Seggaard, 2016).

Vi velger å sette opp «Lik stemmerett» som et eget kriterium ettersom det er sentralt valgprinsipp. Derimot vil vi ikke vurdere løsningene etter dette kriteriet. Alle datasystemer kan være utsatt for sårbarheter som muliggjør angrep. Det er derfor tenkelig at en angriper lykkes med å modifisere programkoden på en slik måte at enkeltstemmer slettes, erstattes eller fordobles. Dette medfører integritetsbrudd, som vi dekker i kriteriet «valgintegritet».

Som beskrevet i kapittel 2, er bekreftelse til velgere på at stemmen er talt verdifullt, da det kan sikre integriteten til valgresultatet. Dette illustrerer avhengigheten mellom to av sikkerhetskriteriene, valgintegritet og verifiserbarhet. Denne avhengigheten gir videre opphav til et perspektiv på hvordan man skal sikre e-stemmesystem: «verifiser valgresultatet, ikke stemmesystemet» (Ryan et al., 2009).

Det kan i noen tilfeller være ønskelig at e-stemmesystem har funksjonalitet for å motvirke faren for at velgere kan bli utsatt for tvang (engelsk: coercion). Et eksempel på funksjonalitet som kan bidra til å motvirke tvang er å gi de stemmeberettigede mulighet til å stemme flere ganger. Valgordningen kan, hvis dette er mulig, bestemme at det er siste avgitte stemme som teller, eller at stemmen på valgdagen telles, og ikke den elektronisk avgitte stemmen.

## 4.3 Transparens og etterprøvbarehet

Transparens og etterprøvbarehet er sentrale forhold i valg gjennomføringen. Generelt vil tilrettelegging for valgobservasjon bidra til å øke transparensen og tilliten til valget. Transparens vil i tillegg være nødvendig for etterprøvbareheten til et system, som til slutt er avgjørende for å sikre integriteten til avgitte stemmer.

Valg av stemmesystem, enten papirbasert eller elektronisk, har implikasjoner for hvordan det tilrettelegges for transparens og etterprøvbarehet, men også for hva det innebærer å ha transparente og etterprøvbare systemer.

For denne kategorien *transparens og etterprøvbarehet* har vi følgende kriterier:

<sup>7</sup> Kryptografiske stemmeprotokoller er nærmere beskrevet i delkapittel 2.8.

**Transparens:** Stemmesystemet og delkomponenter i stemmesystemet skal være åpent for kontroll, observasjon, evaluering og verifikasjon, iht. tekniske- og sikkerhetsmessige krav til stemmesystemet.

**Etterprøvnbarhet:** Det skal være mulig å etterprøve at integriteten til avgitte stemmer og stemmeresultater er ivaretatt. Det skal være mulig å etterprøve telling av stemmer, for eksempel ved hjelp av observatører.

Transparens er nært knyttet til både tillit og sikkerhet i valggjennomføringen (NOU 2020: 6). For tilliten til valggjennomføringen antas det å være av betydning at velgerne forstår, eller har mulighet til å forstå, valgprosessen. Det kan ha en egenverdi at de avgjørende prosessene kan observeres og kontrolleres uten behov for spesialkompetanse (NOU 2020: 6). Enkelte argumenterer imidlertid for at grad av forståelighet for hvordan valgprosesser gjennomføres i noen tilfeller kan gå på bekostning av sikkerheten til systemet (Rogers, 2021). Dersom deler av valggjennomføringen krever kompliserte tekniske løsninger og behov for kryptering og sikkerhetsklareringer, vil det føre til mindre åpenhet og til at folk flest ikke kan beskrive hvordan valggjennomføringen skjer. På den andre siden er det nødvendig med et tilfredsstillende sikkerhetsnivå for å oppnå tillit til valggjennomføring. I så tilfelle vil sikkerhetstiltakene måtte kombineres med transparens rundt løsningens virkemåte. Dette illustrerer avhengighetene mellom transparens og etterprøvnbarhet i valggjennomføringen.

Vår utforming av vurderingskriteriene for transparens og etterprøvnbarhet legger vekt på hvordan elektroniske stemmesystemer muliggjør transparens og etterprøvnbarhet.

For elektroniske stemmesystemer kan transparens innebære dokumentasjon av programvaren og de kryptografiske stemmeprotokoller som benyttes. Dette er nødvendig for å sikre systemets etterprøvnbarhet. Etterprøvnbarhet og gode kontrollrutiner sørger for ansvarlighet, og er en kilde til at valgresultatene oppfattes som troverdige. Dagens ordinære, papirbaserte valgordning i Norge kan bare etterprøve valgresultatet ved at papirstemmer kan telles på nytt.<sup>8</sup> Etterprøvnbarhet ved elektronisk stemmegiving er i større grad relatert til verifiserbarhet. Det skal være mulig å verifisere eller etterprøve at operasjonene foretatt i den elektroniske løsningen er korrekte og at resultatene er nøyaktige.

<sup>8</sup> Dette er gitt at stemmene oppbevares trygt over nødvendig tidsperiode.

## 4.4 Brukervennlighet og inkludering

Kategorien *brukervennlighet* og *inkludering* er knyttet til bruk, forståelse og enkel tilgang til stemmeløsningen, så vel som inkludering av mennesker med en funksjonsnedsettelse som medfører behov for tilrettelagt stemmegiving. Vi omtaler denne gruppen som velgere med *særskilte behov*.

Europarådets anbefalinger vektlegger at det elektroniske stemmesystemet skal være brukervennlig. For velgerne skal det være lett å forstå hvordan en deltar i valget og hvordan en avgir stemme. Vi har lagt til grunn følgende kriterier:

**Brukervennlighet:** Stemmesystemet skal være enkelt å forstå og bruke

- for velgere generelt
- for velgere med ulik teknisk kompetanse
- for velgere som stemmer fra utlandet

### Inkludering

- Stemmesystemet skal være enkelt å forstå og bruke for velgere med særskilte behov.
- Stemmesystemet skal gjøre det mulig for velgere med særskilte behov å stemme selvstendig.

I kriteriet *brukervennlighet* er oppmerksomheten rettet mot velgere generelt, velgere med ulik teknisk kompetanse og velgere som stemmer fra utlandet. Brukervennlighet omhandler både hvordan og hvorvidt velgerne klarer å ta i bruk løsningen, og dessuten hvilke muligheter løsningen gir for bruk. Eksempelvis kan elektroniske og internettbaserte løsninger tillate interaktivitet underveis i stemmeprosessen, noe som ikke er mulig på samme måte for papirbaserte løsninger. Interaktivitet viser i denne sammenheng til interaksjonen eller samspelet mellom velgeren og datasystemet i stemmegivingen. For eksempel kan datasystemet gi en respons til en velger om at velgeren ikke har avgitt stemme korrekt før stemmen sendes.

Et annet aspekt som bidrar til brukervennlighet er fysisk tilgjengelighet, det vil si hvilke tider og fra hvilke lokasjoner det er mulig å avgi stemme.

Kriteriet *inkludering* har to aspekter. Det første handler om hvorvidt løsningen er brukervennlig og forståelig å bruke for velgere med særskilte behov. Relevante momenter er hvordan ulike løsninger kan tilrettelegge for bruk av hjelpemidler som gir økt brukervennlighet. Det aspektet er forholdet til

selvstendig stemmegiving. Dette tar for seg hvorvidt stemmesystemet kan utformes slik at blinde og svaksynte velgere kan stemme uten assistanse. Se ellers omtalen av *anonymitet* i kapittel 4.2.

## 4.5 Ressursbruk

Ressursbruk handler om hva som kreves av menneskelige og finansielle ressurser på statlig og kommunalt nivå ved innføring og drift av elektronisk- eller internettbasert stemmegiving som et supplement til ordinær papirbasert valg gjennomføring.

Oppmerksomheten er rettet mot ressursbruk i den praktiske valg gjennomføringen. Kriteriene omfatter ikke arbeid knyttet til eventuelle nødvendige endringer i lovverket, og vurderer heller ikke hvordan innføring av elektronisk- eller internettbasert stemmegiving påvirker velgeres ressursbruk når de skal avgi stemme.

### **Ressursbruk på lokalt og nasjonalt nivå er**

- materiell, utstyr og systemer
- bemanning og opplæring
- lokaler
- informasjon og veiledning

Materiell, utstyr og systemer handler om hva stat og kommune må utvikle, anskaffe, implementere og drifte av program- og maskinvare knyttet til elektronisk- og internettbaserte stemmesystemer.

Bemanning og opplæring handler om hvordan staten og kommunens behov for bemanning endrer seg. Er eksempelvis kommunen nødt til å sysselsette flere valgmedarbeidere, eller kan de klare seg med færre? Og er det behov for en annen type kompetanse og/eller opplæring?

Lokaler handler om hvorvidt kommunene må gjøre tilpasninger i lokalene de bruker til valg, og om staten som følge av innføringen av elektronisk og/eller internettbasert valg er nødt til å etablere nye sentrale elektroniske lagre.

Informasjon og veiledning handler om hvorvidt stat og kommune må drive et mer aktivt informasjonsarbeid ut mot velgerne, og om kommunene vil ha behov for økt grad av veiledning i valg gjennomføringen.

## 5. Sikkerhet

*Sikkerhet handler om at velgerne skal kunne være trygge på at stemmene ikke manipuleres, at valget er hemmelig, at sensitive data ikke spres, og at alle stemmer telles slik de blir avgitt. Vi vurderer at et papirbasert system i større grad ivaretar krav til sikkerhet enn elektronisk- og internettbaserte systemer. I dette kapitlet gir vi en nærmere beskrivelse av våre vurderinger.*

### 5.1 Hovedfunn: Sikkerhet

Figur 5-1 oppsummerer hvordan vi har vurdert de ulike kriteriene knyttet til kategorien *sikkerhet*.

Som redegjort for i kapittel 1 har vi gjort en risikoanalyse og vurdert i hvilken grad valgsystemene oppfyller de respektive kriteriene, beskrevet i kapittel 4. Grad av oppfyllelse er gjengitt på en tredelt skala:

- **I stor grad:** Det er ingen vesentlige utfordringer ved stemmesystemet, og kriteriet er i stor grad oppfylt.
- **I noen grad:** Det er enkelte utfordringer ved stemmesystemet som hindrer oppfyllelse av kriteriet, men utfordringene er ikke vesentlige, eller løsningen muliggjør oppfyllelse av kriteriet på andre vis.
- **I liten grad:** Det er vesentlige og/eller uløselige utfordringer ved stemmesystemet som gjør at kriteriet i liten grad er oppfylt.

Det er i utgangspunktet flere typer papirbaserte systemer og ulike varianter av elektroniske og internettbaserte systemer. I analysen har vi for papirbaserte systemer tatt utgangspunkt i det norske systemet, og den delen av valget der stemmer avgis i valglokaler på valgdagen. For elektroniske og internettbaserte systemer er det konseptene vi analyserer. Vi går ikke nærmere inn på forhold knyttet til design og implementering av konkrete løsninger, eksempelvis betydningen kryptografi (se kapittel 2.8). Det er utfordrende å si noe om hvordan kryptografiske metoder vil påvirke systemer på generelt grunnlag. Dette kommer av at bruken kryptografiske metoder er nært knyttet til implementeringen av den spesifikke løsningen som skal

innføres. Det kan være svært subtile aspekter ved mange steg i stemmeprosessen, som kan virke inn på det faktiske resultatet.

Dagens papirbaserte valgsystem i Norge er systemet som kommer best ut av sikkerhetsvurderingen. Vi vurderer at systemet oppfyller nærsagt alle sikkerhetskriteriene til et valgsystem i stor grad. Det eneste kriteriet det norske systemet ikke fullstendig oppfyller er kriteriet som omhandler *verifiserbarhet*, selv om verifisering delvis er mulig i dagens valgsystem.

Elektroniske systemer kommer svakere ut i vurderingen av kategorien *sikkerhet*. Hovedårsaken er faren for at valgresultatet kan bli manipulert i elektroniske systemer, noe som kan ha store konsekvenser for valgfallet. Denne risikoen blir reflektert i kriteriene knyttet til valgintegritet og korrekthet. I elektroniske systemer vil det også være en større risiko for at noen får tilgang til og publiserer deler av valgresultatene på forhånd. Dette vil innebære et brudd på kriteriet om fravær av påvirkning.

Internettbaserte systemer kommer svakest ut i vurderingen av kategorien *sikkerhet*. De internettbaserte systemene har de samme risikoelementene som elektroniske systemer knyttet til manipulering og forhåndspubliserings av valgresultatet. I tillegg foregår stemmegiving ved internettbaserte systemer i ukontrollerte omgivelser, slik at det er mer utfordrende å verifisere at de riktige personene stemmer og at valgene er hemmelige. Disse risikoelementene blir fanget opp i kriteriene om autentisering, anonymitet og motstand mot tvang.

Et tilleggsmoment til vurderingen av sikkerheten til elektroniske og internettbaserte systemer, som ikke kan utledes av kriteriene direkte, er sårbarheten som ligger i sentraliserte systemer. I ende-til-ende elektroniske systemer er stemmehåndteringen sentralisert, mens i internettbaserte systemer er alt sentralisert. Ved sentraliserte systemer er vesentlig færre valgfunksjonærer involvert, disse systemene krever og forutsetter at de få involverte medarbeiderne er fullt betrodd.

I det følgende beskriver vi nærmere hvordan hvert av valgsystemene gjør det opp mot hvert av sikkerhetskriteriene beskrevet i kapittel 4.



Figur 5-1: Vurdering av stemmesystemer opp mot sikkerhetskriteriene

	Papirbaserte systemer	Elektroniske systemer	Internettbaserte systemer
Fravær av påvirkning	I stor grad	I stor grad	I noen grad
Autentisering	I stor grad	I stor grad	I liten grad
Anonymitet	I stor grad	I noen grad	I liten grad
Motstand mot tvang	I stor grad	I stor grad	I liten grad
Valgintegritet	I stor grad	I noen grad	I liten grad
Korrekthet	I stor grad	I noen grad	I liten grad
Verifiserbarhet	I noen grad	I stor grad	I stor grad
Tilgjengelighet	I stor grad	I stor grad	I noen grad

**Oppfyller kriteriet**

- I stor grad
- I noen grad
- I liten grad

Illustrasjon: Oslo Economics og Norsk Regnesentral

## 5.2 Papirbaserte systemer

### 5.2.1 Fravær av påvirkning

Kriteriet omhandler at velgerne ikke skal ha noe informasjon om valgresultatet når de stemmer. I det norske systemet blir dette kriteriet overholdt ved å ha klare retningslinjer for når opptellingen av stemmer skal begynne, noe som (implisitt) legger føringer på når resultatene kan bli offentliggjort. Kriteriet kan imidlertid bli brutt hvis medier får tilgang til tidlig opptalte stemmer, og publiserer disse før sperrefristen. Vår vurdering er likevel at det norske systemet med stor grad oppfylder kriteriet om fravær av påvirkning.

### 5.2.2 Autentisering

Kriteriet autentisering handler om at det ikke skal være mulig å utgi seg for å være noen andre i stemmeprosessen. I det norske systemet autentiserer velgeren seg ved å vise legitimasjon til en valgfunksjonær, som valgfunksjonæren deretter kontrollerer opp mot manntallet. Kriteriet kan brytes hvis noen bruker andres legitimasjon. Det har imidlertid vært få rapporterte tilfeller av dette i dagens valgsystem. Ved at stemmegivingen foregår i kontrollerte omgivelser er det vanskelig å klare å utgi seg for å være noen andre enn den man er. Vår vurdering er derfor at det norske systemet i stor grad oppfylder kriteriet autentisering.

### 5.2.3 Anonymitet

Kriteriet anonymitet omhandler at det ikke skal være mulig å finne ut hvem som har stemt på hvem, og er relevant både under og etter stemmegivning. Anonymitet under stemmegiving kan for eksempel bli kompromittert om noen observerer stemmegivningen, mens anonymitet etter stemmegiving omhandler at ingen skal kunne knytte en spesifikk stemme til en velger. Som redegjort for i kapittel 4 handler dette kriteriet om anonymitet for den allmenne velger. Forhold knyttet til hemmelig stemmegiving for velgere med særskilte behov favnes under *brukervennlighet* og *inkludering* i kapittel 7.

I det norske systemet vil anonymiteten sikres ved at velgeren bestemmer seg for stemmeseddelen i et skjult avlukke, og bretter den sammen, som holder den skjult fra avlukke til urnen. Når stemmeseddelen først er lagt i urnen og blandet med øvrige stemmer er det ikke mulig å knytte den tilbake til en velger. Kriteriet vil for eksempel kunne bli brutt hvis velgere eller valgfunksjonærer ser inne i stemmeavlukket når noen velger det de skal stemme på. Det har vært få rapporterte problemer med dette i forbindelse med valg gjennomføringen i dagens system. Vår vurdering er at det norske systemet i stor grad oppfylder kriteriet anonymitet.

### 5.2.4 Motstand mot tvang

Kriteriet motstand mot tvang handler om at det skal være vanskelig å presse en velger til å stemme på et bestemt parti eller en bestemt kandidat. Det vil i

utgangspunktet være vanskelig å utsette velgerne for tvang i det norske systemet. Grunnen er at stemmegivningen foregår i kontrollerte omgivelser, der valgfunksjonærer sørger for at velgere er alene i avlukket når de avgir sin stemme.<sup>9</sup> En som forsøker å utøve tvang kan ikke vite hva velgeren stemmer; dermed vil velgeren kunne foreta sitt valg uten å frykte konsekvenser fra tredjeparten. Vår vurdering er derfor at det norske systemet i stor grad oppfyller kriteriet motstand mot tvang.

### 5.2.5 Valgintegritet

Kriteriet valgintegritet handler om at det velgeren har stemt på teller med i det faktiske valgresultat. I det norske systemet, og andre papirbaserte systemer, kan dette sikkerhetskriteriet brytes hvis det systematisk byttes ut eller forkastes stemmer fra noen utvalgte partier. Vi er ikke kjent med rapporterte tilfeller av dette i Norge, og velgere har stor tillit til at deres stemmer håndteres på en sikker måte (Bock Seggaard, et al., 2014). Vår vurdering er derfor at det norske systemet i stor grad oppfyller kriteriet valgintegritet.

### 5.2.6 Korrekthet

Kriteriet korrekthet handler om at stemmene skal bli talt opp og rapportert på en riktig måte.

I dagens norske system foregår opptellingen av stemmer i to runder.<sup>10</sup> Systematisk juks vil derfor kreve samarbeid mellom flere valgfunksjonærer. Vi er ikke kjent med rapporterte tilfeller om dette i Norge. I tilfelle det skulle foregå enkeltfeil vil også det ha lav betydning for det endelige valgutfallet. Riktignok, ved stortingsvalget i 2021 ble 4 517 stemmegivninger forkastet (*Innst. 1 S (2021-2022), 2021*). Manglende stempel på stemmeseddelen er den forkastelsesgrunnen som forekommer oftest, og ofte skyldes dette at stemmegiver benytter en separat stemmeseddel som «omslag» til sin egentlige stemme, typisk for å skjule hva man har stemt på. I slike tilfeller blir kun den ytterste stemmeseddelen, omslaget, påført stempel. Den reelle stemmen blir da forkastet (*Innst. 1 S (2021-2022), 2021*). Dette kan unngås ved elektroniske eller internettbaserte systemer, som omtalt lenger nede. Det kan også skje at stemmesedler blir forlagt eller at de ikke blir sendt til stedet der stemmene telles. Oppdages dette må valgstyret vurdere om valget kan godkjennes. Gitt historikken og de sikkerhetssystemer som er på plass er det vår vurdering at det norske systemet i stor grad oppfyller kriteriet korrekthet.

<sup>9</sup> Det er viktig å huske at analysen tar for seg stemmegivning som foregår i et valglokale. Andre vurderinger vil gjelde for stemmegivning som foregår via brev.

### 5.2.7 Verifiserbarhet

Kriteriet verifiserbarhet handler om at velgeren skal få en bekreftelse på at stemmen er avgitt, at den teller med i det endelige valgresultat, og at alle gyldige stemmer er talt med i det endelige valgresultatet.

Det norske systemet oppfyller delvis kriteriet om verifiserbarhet fordi velgeren (implisitt) kan verifisere at stemmen blir avgitt når de legger den i urnen. Imidlertid kan velgeren ikke verifisere at stemmen er talt med i det endelige valgresultat, eller om alle gyldige stemmer er talt med i det endelige resultat. Vår vurdering er derfor at det norske systemet bare i noen grad oppfyller kriteriet verifiserbarhet.

### 5.2.8 Tilgjengelighet

Kriteriet tilgjengelighet omhandler at stemmesystemet må være tilgjengelig i samsvar med foreskrevet stemmeperiode. I papirbaserte systemer så er det et begrenset risikobilde for tilgjengelighetsbrudd. Tilgjengelighetsbrudd i denne sammenheng vil være knyttet til fysiske forhold ved valglokalet. Dette kan eksempelvis være strømbrydd eller brann. Vår vurdering er at det norske systemet med valgtid i stor grad oppfyller kriteriet tilgjengelighet.

## 5.3 Elektroniske systemer

### 5.3.1 Fravær av påvirkning

Kriteriet handler om at velgerne ikke skal ha noe informasjon om valgresultat når de stemmer. Med elektroniske systemer er det lav risiko for at deler av valgresultatet blir publisert før stemmegivningen er avsluttet. Grunnen er at de som eventuelt ønsker å publisere resultatene på forhånd må få tilgang til stemmemaskinene, og hente resultatene ut fra disse; det vil være vanskelig å få til i praksis, og vi kjenner ikke til noen hendelser fra land som har tatt i bruk elektroniske systemer hvor noe slikt har skjedd. Vår vurdering er derfor at elektroniske systemer i stor grad oppfyller kriteriet konfidensialitet.

### 5.3.2 Autentisering

Kriteriet autentisering handler om at det ikke skal være mulig å utgi seg for å være noen andre i stemmeprosessen. Også elektroniske systemer brukes i kontrollerte omgivelser, hvor en valgfunksjonær kontrollerer velgerens legitimasjon ved ankomst til valglokalet. Vi kjenner ikke til elektroniske stemmesystemer med en integrert autentiseringsløsning, selv om dette kan være mulig. Velgernes autentisering er med andre ord lik som for dagens norske papirbaserte system, og sannsynligheten for at en

<sup>10</sup> Tellemåtene i de to rundene er også uavhengige fra hverandre – én maskinell og en manuell opptelling.

person klarer å utgi seg for å være en annen er lav da det vil kreve falsk bruk av legitimasjon. Vår vurdering er derfor at elektroniske systemer i stor grad oppfyller kriteriet autentisering.

### 5.3.3 Anonymitet

Kriteriet anonymitet handler om at velgerens stemme skal forbli skjult for alle andre gjennom stemmeprosessen. Langt på vei gjelder de samme vurderingene her som for papirbaserte systemer; det er mulig å se for seg noen hendelser, for eksempel at noen ser hva andre stemmer i valglokalet, hvor velgerens anonymitet i så fall blir brutt. Men sannsynligheten for disse hendelsene er lav.

Imidlertid er det noen andre hendelser som også er relevante når en vurderer anonymiteten i elektroniske systemer. Den viktigste av disse er at noen kobler sammen velgerens identitet og stemme etter at stemmer har blitt avgitt. Dette sikkerhetsbruddet er mulig i et elektronisk system fordi det eksisterer en elektronisk kobling mellom velgeren og hva velgeren har stemt på. Hvis noen får tilgang til stemmemaskinene som har blitt brukt, vil det i teorien være mulig å identifisere hvem som har stemt på hva. Hvor vanskelig det er vil avhenge av forutsetningene som ligger til grunn for systemet. Avgitte stemmer vil være beskyttet med en eller annen form for kryptering, men siden kryptonøkklene er fremskaffet av en tiltrodd part som er tilknyttet gjennomføringen av valget, avhenger anonymitetsbeskyttelsen i særlig grad av den tiltrodde parten og hvordan nøkkelhåndteringen gjøres.

Det er viktig å understreke at sannsynligheten for sikkerhetsbrudd av denne typen er relativt liten da det blant annet vil kreve at noen får fysisk tilgang til stemmemaskinene. Imidlertid er dette en tilleggsrisiko ved elektroniske systemer som ikke er til stede for papirbaserte systemer. Vår vurdering er derfor at elektroniske systemer i noen grad oppfyller kriteriet anonymitet.

### 5.3.4 Motstand mot tvang

Kriteriet motstand mot tvang handler om at det skal være vanskelig å presse en velger til å stemme på et bestemt parti eller en bestemt kandidat. Det følger av kriteriet ovenfor at det vil være god beskyttelse av velgere mot press i et elektronisk system. Grunnen er at god sikring av anonymitet gjør det vanskelig for tredjeparter å vite hva en person stemmer på, og de kan dermed ikke utøve faktisk press på personer. Anonymiteten sikres i stor grad fordi stemmegivingen foregår i kontrollerte omgivelser, der valgfunksjonærer sørger for at velgere er alene i valglokalet når de avgir stemmen.

Samlet sett vurderer vi at elektroniske systemer i stor grad oppfyller kriteriet motstand mot tvang.

### 5.3.5 Valgintegritet

Kriteriet valgintegritet handler om at velgerens stemme teller med i det faktiske valgresultat.

Valgintegriteten kan bli brutt på flere måter i et elektronisk system. Den mest nærliggende måten vil være at noen endrer programvaren i maskinen i forkant av valget. Et illustrerende eksempel på dette kom frem i forbindelse med en sikkerhetsanalyse (Feldman, et al., 2006) av Diebold Accuvote-TS, som er mye brukt ved valg i USA. Analysen av maskinen konkluderte med at alle som har fysisk tilgang til maskinen lett kan installere en kode som endrer stemmer. Dette er heller ikke et enestående tilfelle. En analyse av stemmemaskinen Nedap ES3B (Gonggrijp & Hengeveld, 2007), som er blitt brukt ved valg i Nederland, Tyskland, Frankrike og Irland, viste at denne var tilsvarende lett for angripere å skaffe seg kontroll over. Disse eksemplene illustrerer sårbarhet for integriteten i elektroniske stemmesystemer. Det medfører også høy sårbarhet for internt hemmelighold uansett om det er et klassisk system eller et ende-til-ende-system.

Det er krevende å anslå sannsynligheten for at risikomomentene beskrevet ovenfor faktisk inntreffer. I tilfelle det skulle skje vil konsekvensene for valgfallet sannsynligvis bli noe større enn ved brudd på valgintegriteten i dagens norske system. Årsaken er at det vil påvirke alle stemmene fra en stemmemaskin og ikke bare enkeltstemmer. En faktor som bidrar til å begrense de potensielle konsekvensene er at opptellingen av stemmene til majoriteten av de elektroniske systemene foregår lokalt. Vår vurdering er derfor samlet sett at elektroniske systemer i noen grad oppfyller kriteriet valgintegritet.

### 5.3.6 Korrekthet

Kriteriet korrekthet handler om at stemmene skal bli talt opp og rapportert på en riktig måte. I elektroniske systemer vil i utgangspunktet opptellingen av stemmer foregå via en automatisk prosess: Når velgeren avgir stemmen vil den lagres i et lokalt elektronisk lager, og når stemmegivingen avsluttes, vil den bli talt opp. Måten selve opptellingen foregår på vil variere fra system til system, men i majoriteten av tilfellene skjer opptellingen lokalt.

Den mest nærliggende måten en feil kan skje på vil være et sikkerhetsbrudd likt det som ble skissert i vurderingen av valgintegritet; noen får tilgang til programvaren i tellemaskinen, og legger inn endringer slik at opptellingen blir feil.

Automatiseringen av opptellingsprosessen kan bidra til å minske sannsynligheten for feilkilder ved manuell håndtering, men betraktninger knyttet til omfang og risiko for feil veier tungt i våre vurderinger. Vår vurdering av sannsynligheten for at kriteriet blir brutt,

og konsekvensene av dette, er lik som vår vurdering av valgintegriteten i avsnittet ovenfor. Altså oppfyller elektroniske systemer kriteriet korrekthet i noen grad.

### 5.3.7 Verifiserbarhet

Kriteriet verifiserbarhet handler om at velgeren skal få en bekreftelse på at stemmen er avgitt, at den teller med i det endelige valgresultat, og at alle gyldige stemmer er talt med i det endelige valgresultat. Det er i utgangspunktet enklere å ha en ende-til-ende-løsning, med full verifiserbarhet, når en bruker elektroniske systemer, sammenlignet med papirbaserte systemer. Grunnen er at ende-til-ende løsninger forutsetter at man har et stemmealternativ for hver mulig kombinasjon som en kan stemme på. I det norske valgsystemet, hvor det blant annet er mulig å gi personstemmer, er det veldig mange mulige kombinasjoner av stemmealternativer. Det vil aldri være mulig å ha en stemmeseddel for hver av disse kombinasjonene i et papirbasert valg, men det er mulig når stemmesedlene er elektroniske som i et elektronisk system. Vår vurdering er derfor at elektroniske systemer i stor grad oppfyller kriteriet verifiserbarhet.

### 5.3.8 Tilgjengelighet

Kriteriet tilgjengelighet omhandler at stemmesystemet må være tilgjengelig i samsvar med foreskrevet stemmeperiode. Ettersom elektroniske systemer, i likhet med papirbaserte systemer, er i kontrollerte omgivelser, deler elektroniske systemer det samme risikobildet med tanke på fysisk tilgjengelighet med papirbaserte systemer.

Når det gjelder den elektroniske sårbarheten så foregår stemmegivingen på stemmemaskiner, noe som kan øke sårbarheten. Forutsatt at maskinene ikke er tilkoblet internett, vurderer vi imidlertid at det ikke vil være en betydelig økning i risiko sammenlignet med papirbaserte systemer, og at kriteriet i stor grad er oppfylt.

## 5.4 Internettbaserte systemer

### 5.4.1 Fravær av påvirkning

Kriteriet handler om at velgerne ikke skal ha noe informasjon om valgresultat når de stemmer.

Med internettbaserte systemer er det en risiko for at valgresultatet publiseres før stemmegivingen er avsluttet. Det kan skje hvis innbrytere får tilgang til de delene av systemet hvor de allerede avgitte stemmene ligger lagret. Denne risikoen er ikke til stede i et papirbasert system som det norske. Her ligger ikke stemmene lagret på et sentralt sted. På grunn av denne risikoen er vår vurdering at et internettbasert

system i noen grad oppfyller kriteriet fravær av påvirkning.

### 5.4.2 Autentisering

Kriteriet autentisering handler om at det ikke skal være mulig å utgi seg for å være andre i stemmeprosessen. Internettbaserte systemer skiller seg fra de to andre systemene ved at stemmegivingen foregår i ukontrollerte omgivelser. Dette har følger for hvordan en velger legitimerer seg. I et internettbasert system vil velgeren legitimere seg ved å bruke elektroniske akkreditiver, for eksempel gjennom BankID eller koder. Andre kan få tilgang til akkreditivene, utgi seg for å være velgeren, og dermed bryte kriteriet for autentisering. Akkreditiver som benytter seg av to-faktorautentisering<sup>11</sup> eller biometrisk autentisering kan være sikrere, men vår vurdering er likevel den at internettbaserte systemer i liten grad oppfyller kriteriet autentisering.

### 5.4.3 Anonymitet

Kriteriet anonymitet handler om at velgerens stemme skal forbli skjult for alle andre gjennom stemmeprosessen. Anonymiteten til velgeren kan bli utfordret på flere måter i et internettbasert system. Først og fremst er det en risiko for at en eller flere andre er sammen med velgeren når stemmen avgis, og dermed kan observere hva det stemmes på. På samme måte som for elektroniske systemer er det også en mulighet for at noen kobler velgeren og hva velgeren har stemt på i etterkant av at stemmen er avgitt; dette sikkerhetsproblemet er mulig i et internettbasert system fordi det eksisterer en elektronisk kobling mellom velgeren og stemmen.

Hvis noen bryter seg inn i et internettbasert system, vil det i teorien være mulig å identifisere hvem som har stemt på hva, og det vil ikke nødvendigvis bli oppdaget. Denne typen angrep kan gjennomføres ved å manipulere programvaren i de delene av systemet der velgerens identitet kan knyttes til stemmen. Dette gjelder både på klienten, som typisk er enten en nettleser eller en dedikert app, og det kan gjennomføres ved et leverandørkjedeangrep, for eksempel ved å legge inn en trojansk hest i et bibliotek som brukes av programvaren. Dette er en risiko som ikke er til stede for papirbaserte systemer.

Vår vurdering er derfor at internettbaserte systemer i liten grad oppfyller kriteriet anonymitet.

### 5.4.4 Motstand mot tvang

Kriteriet motstand mot tvang handler om at det skal være vanskelig å presse en velger til å stemme på et bestemt parti eller en bestemt kandidat. Fordi det er mulig å observere velgeren når de avgir sin stemme,

<sup>11</sup> Bruk av to-faktorautentisering kan gjøre det mer krevende for enkelte velgergrupper å stemme.

er det i utgangspunktet en risiko for at velgere kan bli utsatt for tvang ved bruk av internettbaserte systemer.

En faktor som kan redusere denne risikoen er å utforme systemet slik at velgeren kan endre stemmen inntil fristen for stemmegivningen går ut.<sup>12</sup> Dette endrer likevel ikke det overordnede bildet siden de som ønsker å tvinge velgere til å stemme på et parti eller en kandidat kan følge med helt opptil fristen. Vår vurdering er derfor at et internettbasert system i liten grad oppfyller kriteriet motstand mot tvang.

#### 5.4.5 Valgintegritet

Kriteriet valgintegritet handler det om at velgerens stemme teller med i det faktiske valgresultatet. I et internettbasert system kan dette kriteriet bli brutt ved at noen får tilgang til systemet, og endrer det slik at partiet eller kandidaten en velger har stemt på, ikke kommer med i valgopptellingen.

Integritetsbruddet kan skje enten gjennom operativsystemet eller direkte gjennom applikasjonen. Forskjellige operativsystemer kan ha varierende tilgangskontrollpolicyer for å begrense hva applikasjoner kan gjøre med systemet, som for eksempel hva slags applikasjoner som kan installeres og hvilke rettigheter de kan ha. Det skilles her mellom skjønnsmessig tilgangskontroll, der brukeren selv gjør beslutninger etter eget skjønn, og obligatorisk tilgangskontroll, der rettighetene styres etter absolutte regler. Sistnevnte gir i prinsippet mindre spillerom for å korrumpere systemet og er implementert for eksempel i Android 5 eller nyere. Når det gjelder overføringen av en applikasjon fra en «app store» til en lokal enhet ville det være svært vanskelig å korrumpere en applikasjon i dette leddet, ettersom alle slike applikasjonskilder bruker digital signering.

En alternativ angrepsmetode er å korrumpere selve applikasjonen i utviklingen. Dette er ikke bare en teoretisk mulighet. Moderne applikasjoner er basert på et stort antall biblioteker<sup>13</sup> som stammer fra mange forskjellige kilder, og det finnes konkrete eksempler på både biblioteker som bevisst har blitt korrumpert og biblioteker som har hatt alvorlige svakheter som har blitt oppdaget først etter lang tid. Hvis en angriper har kontroll over et bibliotek som brukes av en stemmeapplikasjon, kan vedkommende legge inn en trojansk hest gjennom dette biblioteket uten at det oppdages og sikre seg kontroll over stemmeapplikasjonen. Denne typen angrep kan også brukes mot nettlesere og muliggjør det som kalles et «man-in-the-browser»-angrep, der angriperen kan manipulere informasjonen som går gjennom nettleseren.

<sup>12</sup> Det ble tilrettelagt for en slik mulighet under forsøksvalget med internettstemmegiving i 2013 (Saglie & Segaaard, 2016)

Det er i utgangspunktet krevende å vurdere sannsynligheten for at disse sikkerhetsbruddene finner sted. I tilfelle det skulle skje vil likevel konsekvensene for valgfallet kunne være svært store; det vil potensielt kunne være lett skalerbart og påvirke alle stemmer levert via internett. Vår vurdering er derfor at internettbaserte systemer i liten grad tilfredsstiller kriteriet valgintegritet.

#### 5.4.6 Korrekthet

Kriteriet korrekthet handler om at stemmene skal bli talt opp og rapportert på en riktig måte. I internettbaserte systemer vil i utgangspunktet opptellingen av stemmer foregå via en automatisk prosess. Den mest nærliggende måten en feil kan skje på vil være et sikkerhetsbrudd likt det som ble skissert når vi vurderte valgintegriteten; noen bryter seg inn i systemet og endrer det slik at opptellingen blir feil.

Tilsvarende som for elektroniske systemer kan automatiseringen av opptellingsprosessen bidra til å minske sannsynligheten for feilkilder ved manuell håndtering, men betraktninger knyttet til omfang og risiko for feil veier tungt i våre vurderinger. Vår vurdering av sannsynligheten for at kriteriet blir brutt, og konsekvensene av dette, er derfor lik som vår vurdering av valgintegriteten i avsnittet ovenfor. Vi vurderer at internettbaserte systemer i liten grad oppfyller kriteriet korrekthet.

#### 5.4.7 Verifiserbarhet

Kriteriet verifiserbarhet handler om at velgeren skal få en bekreftelse på at stemmen er avgitt, at den teller med i det endelige valgresultat, og at alle gyldige stemmer er talt med i det endelige valgresultat. Det er i utgangspunktet enklere å ha en ende-til-ende-løsning, med full verifiserbarhet, når en bruker internettbaserte systemer, sammenlignet med papirbaserte systemer. Begrunnelsen her er den samme som den vi ga for elektroniske systemer. Vår vurdering er derfor at internettbaserte systemer i stor grad oppfyller kriteriet verifiserbarhet.

#### 5.4.8 Tilgjengelighet

Kriteriet tilgjengelighet omhandler at stemmesystemet må være tilgjengelig i samsvar med foreskrevet stemmeperiode. Internettssystemer er sentraliserte og muliggjør dermed at visse hendelser kan forårsake tilgjengelighetsbrudd som kan ramme stemmegivingen for hele valget.

Vi vurderer at internettbaserte systemer i noen grad oppfyller kriteriet verifiserbarhet.

<sup>13</sup> Et bibliotek er en samling av delprogrammer for å oppnå et bestemt formål, slik at felles funksjonalitet kan samles på ett sted og deretter gjenbrukes i flere programmer.

## 6. Transparens og etterprøvbarehet

*Transparens og etterprøvbarehet handler om at det skal være mulig å føre tilsyn med hele stemmeprosessen, slik at det kan sikres at valget er gjennomført korrekt. Et papirbasert system som det norske kommer godt ut på disse kriteriene, mens både elektroniske og internettbaserte systemer kommer mindre godt ut. I dette kapitlet gir vi en nærmere begrunnelse for våre vurderinger.*

### 6.1 Hovedfunn: Transparens og etterprøvbarehet

Figur 6-1 oppsummerer hvordan vi har vurdert kriteriene knyttet til kategoriene transparens og etterprøvbarehet. Som redegjort for i kapittel 1 vurderer vi om kriteriene er oppfylt på følgende tredelte skala:

- **I stor grad:** Det er ingen vesentlige utfordringer ved stemmesystemet, og kriteriet er i stor grad oppfylt.
- **I noen grad:** Det er enkelte utfordringer ved stemmesystemet som hindrer oppfyllelse av kriteriet, men utfordringene er ikke vesentlige, eller løsningen muliggjør oppfyllelse av kriteriet på andre vis.
- **I liten grad:** Det er vesentlige og/eller uløselige utfordringer ved stemmesystemer som gjør at kriteriet i liten grad er oppfylt.

Det er i utgangspunktet flere typer papirbaserte systemer og ulike varianter av elektroniske og internettbaserte systemer. I analysen har vi for papirbaserte systemer tatt utgangspunkt i det norske systemet, og den delen av valget der stemmer avgis i valglokaler på valgdagen. For elektroniske og internettbaserte systemer er det konseptene vi analyserer. Vi går ikke nærmere inn på forhold knyttet til design og implementering av konkrete løsninger

Dagens papirbaserte valgsystem i Norge er brukt som referanse, og det er dette systemet som kommer best ut av vurderingen. Hovedårsaken er at valgobservatører enkelt kan observere alle stegene i stemmeprosessen, og dermed kontrollere at valget er i overensstemmelse med gjeldende regler.

I elektroniske og internettbaserte systemer er stegene som er lett observerbare i et papirbasert system, for eksempel tellingen og kontroll av stemmene, mer utilgjengelig for valgobservatørene. Relevant informasjon vil være lagret elektronisk etter flere sikkerhetstransformasjoner, og vil bare kunne kontrolleres av valgobservatører med særlig teknisk kompetanse.

I det følgende beskriver vi nærmere hvordan hvert av valgsystemene gjør det opp mot hvert av sikkerhets-kriteriene beskrevet i kapittel 4.

**Figur 6-1: Vurdering av stemmesystemer opp mot kriterier for transparens og etterprøvbarehet**

	Papirbaserte systemer	Elektroniske systemer	Internettbaserte systemer	Oppfyller kriteriet
Etterprøvbarehet	Grønn	Rød	Rød	Grønn: I stor grad Blå: I noen grad Rød: I liten grad
Transparens	Grønn	Rød	Rød	

Illustrasjon: Oslo Economics og Norsk Regnesentral

### 6.2 Papirbaserte systemer

#### 6.2.1 Transparens

Kriteriet transparens handler om at valgobservatører skal kunne observere de ulike stadiene i stemmeprosessen, for å kontrollere at prosessen er i tråd med kriteriene for valg gjennomføring. I et papirbasert system som det norske systemet er det mulig for valgobservatører å observere alle stegene i

stemmeprosessen, herunder stegene frem til velgeren legger stemmen i urnen og opptelling av stemmene i etterkant. Vår vurdering er derfor at dagens norske system i stor grad oppfyller kriteriet transparens.

#### 6.2.2 Etterprøvbarehet

Etterprøvbarehet handler om at det skal være enkelt for valgobservatører å kontrollere at integriteten til stemmene blir ivaretatt og at stemmeopptellingen går riktig for seg. Siden papirbaserte systemer som det

norske systemet kommer godt ut på kriteriet transparens, følger det at det også gjør det godt når det kommer til etterprøvnbarhet. Vår vurdering er derfor at det norske systemet i stor grad oppfyller kriteriet etterprøvnbarhet.

## 6.3 Elektroniske systemer

### 6.3.1 Transparens

Kriteriet transparens handler om at valgobservatører skal kunne observere de ulike stadiene i stemme-prosessen, for å kontrollere at prosessen er i tråd med kriteriene for valggjennomføring. Elektroniske systemer, for eksempel i Brasil, har fått kritikk for manglende transparens i systemet. Kritikken mot løsningen i Brasil omhandler at velgerne har svært begrensede muligheter til å kunne vite hvorvidt stemmene deres er inkludert og talt korrekt. Kritikken omhandler også om at det er logistiske utfordringer ved testing av systemet. Det er umulig å bevise at testet programvare korresponderer med installert programvare i maskinene, og at maskinene som brukes i valget fungerer slik som de som har blitt testet. I tillegg gir en stor og kompleks kodebase begrensede muligheter for sikkerhetstesting (Aranha & van de Graaf, 2018).

Elektroniske systemer er mindre transparente enn papirbaserte. Grunnen er at informasjonen om stemmegivingen er representert i bitmønstre i forskjellige former for elektronisk minne. I tillegg er informasjonen typisk transformert med forskjellige kryptografiske mekanismer og pakket inn i flere lag av komplekse protokoller. Den eneste måten å gjøre informasjonen tilgjengelig på og forståelig for mennesker, er å tolke den med et program og vise den frem på en ut-enhet, som for eksempel en skjerm eller en utskrift. Muligheten til å observere det som skjer i systemet er altså kritisk avhengig av programmet som gjør denne tolkningen, noe som skaper et nytt ledd av usikkerhet. Vår vurdering er derfor at elektroniske systemer i liten grad oppfyller kriteriet transparens.

### 6.3.2 Etterprøvnbarhet

Etterprøvnbarhet handler om at det skal være enkelt for valgobservatører å kontrollere at integriteten til stemmene blir ivaretatt og at stemmeopptellingen foregår på en skikkelig måte.

Å etterprøve det som skjer i et papirbasert system er enkelt, ettersom vanlige stemmesedler i prinsippet kan håndteres, tolkes, forstås og telles av praktisk talt hvem som helst. Som forklart ovenfor er det vanskeligere å etterprøve et elektronisk system. Man er avhengig av programmer for å tolke resultatene, og et grunnleggende usikkerhetsmoment er i hvilken grad man kan stole på programmene. For eksempel,

når en velger avgir sin stemme med en vanlig elektronisk stemmemaskin, vil maskinen vise frem valget på en skjerm. Hvis maskinen er manipulert eller har en feil, ville skjermen vise det korrekte valget til velgeren mens et annet valg faktisk blir registrert i minnet. I klassiske elektroniske og internettbaserte systemer eksisterer dette usikkerhetsmomentet i prinsippet på alle punkter der det er ønskelig å etterprøve prosessen. Det eksisterer derimot ikke i papirbaserte systemer, siden tolking av informasjonen ikke er nødvendig.

Enkelte elektroniske ende-til-ende systemer vil kreve mindre etterprøving enn andre stemmesystemer. Kort oppsummert er grunnen til det at resultatene fra stemmegivingen blir publisert offentlig slik at velgere selv kan etterprøve resultatene; hvis en liten del av velgermassen gjør det, vil det være tilstrekkelig for å etterprøve systemet. Det er imidlertid lite trolig at et slikt ende-til-ende elektronisk system vil bli innført. Årsaken er at det vil være svært krevende for velgerne å bruke det, noe vi kommer tilbake til i kapittel 7.5. Vår vurdering er derfor at elektroniske systemer i liten grad oppfyller kriteriet etterprøvnbarhet.

## 6.4 Internettbaserte systemer

### 6.4.1 Transparens

Kriteriet transparens handler om at valgobservatører skal kunne observere de ulike stadiene i stemme-prosessen, for å kontrollere at prosessen er i tråd med kriteriene for valggjennomføring. Internettbaserte systemer, som for eksempel i Estland, har fått kritikk for manglende transparens (Springall et al., 2014). Estiske myndigheter har imidlertid introdusert tiltak for å imøtekomme kritikken. De har åpnet for muligheten til observasjon av valgmedarbeidere, og de har publisert deler av kildekoden som løsningen benytter. I tillegg er det krav om en uavhengig ekspertvurdering av resultatet (Ehin et al., 2022).

I internettbaserte systemer er mye av informasjonen på samme måte som i de elektroniske, i bitmønstre i forskjellige former for elektronisk minne. I tillegg er informasjonen typisk transformert med forskjellige kryptografiske mekanismer og pakket inn i flere lag av komplekse protokoller. For å kunne observere og kontrollere opptellingen i et internettbasert system, vil valgobservatører trenge tekniske kunnskaper og ferdigheter på et høyt nivå. Færre vil altså kunne bli valgobservatører, og valgobservatørenes jobb vil bli mer krevende med et internettbasert system. Samlet sett er vår vurdering at internettbaserte systemer i liten grad oppfyller kriteriet transparens.

#### 6.4.2 Etterprøvnbarhet

Etterprøvnbarhet handler om at det skal være enkelt for valgobservatører å kontrollere at integriteten til stemmene blir ivaretatt og at stemmeopptellingen foregår på en skikkelig måte.

På samme måte som elektroniske systemer, er internettbaserte systemer lite etterprøvbare fordi de er lite transparente. Vår vurdering er derfor at internettbaserte systemer i liten grad oppfyller kriteriet etterprøvnbarhet.



## 7. Brukervennlighet og inkludering

*Brukervennlighet og inkludering handler om at stemmeløsningen skal være enkel å forstå og bruke, og dessuten muliggjøre selvstendig stemmegiving. Alle løsningene har fordeler og ulemper, men vi vurderer at elektroniske og internettbaserte systemer i større grad oppfyller kriteriene, fordi de i større grad muliggjør selvstendig stemmegiving for velgere med særskilte behov. I dette kapitlet gir vi en mer inngående beskrivelse av våre vurderinger.*

### 7.1 Hovedfunn: Brukervennlighet og inkludering

Figur 7-1 oppsummerer hvordan vi har vurdert kriteriene *brukervennlighet* og *inkludering*. Som redegjort for i kapittel 1 vurderer vi om kriteriene er oppfylt for de tre hovedkategoriene av stemmesystemer etter følgende tredelte skala:

- **I stor grad:** Det er ingen vesentlige utfordringer ved stemmesystemet, og kriteriet er i stor grad oppfylt.
- **I noen grad:** Det er enkelte utfordringer ved stemmesystemet som hindrer oppfyllelse av kriteriet, men utfordringene er ikke vesentlige, eller løsningen muliggjør oppfyllelse av kriteriet på andre vis.
- **I liten grad:** Det er vesentlige og/eller uløselige utfordringer ved stemmesystemer som gjør at kriteriet i liten grad er oppfylt.

Det er i utgangspunktet flere typer papirbaserte systemer og ulike varianter av elektroniske og internettbaserte systemer. I analysen har vi for papirbaserte systemer tatt utgangspunkt i det norske systemet, og den delen av valget der stemmer avgis i valglokaler på valgdagen. For elektroniske og internettbaserte systemer er det konseptene vi analyserer. Vi går ikke nærmere inn på forhold

knyttet til design og implementering av konkrete løsninger.

Vår overordnede vurdering er at papirbasert systemer som det norske i noen grad oppfyller kriteriene for *brukervennlighet* og *inkludering*. Papirbaserte systemer er fordelaktig for velgere med lav teknisk kompetanse. For velgere som er blinde eller svaksynte er løsningene vanskelig å bruke, og for enkelte i denne gruppen legger ikke løsningen til rette selvstendig stemmegiving. Det Figur 7-1 ikke synliggjør er at brukervennlighet kan bety ulike ting for ulike velgergrupper.

For elektroniske systemer er vår overordnede vurdering at de i noen grad oppfyller kriteriet brukervennlighet og inkludering. Fordelen ved systemene er at de åpner opp for interaktive løsninger, og muliggjør bruk av hjelpemidler for brukere med særskilte behov. Dette kan gi økt brukervennlighet gjennom en tydeliggjøring for velgere av hvilke muligheter de har i stemmegivingen, og det kan forhindre velgerne i å gjøre utilsiktede feil. Det kan videre muliggjøre selvstendig stemmegiving i større grad enn papirbaserte systemer som det Norge har i dag. Når vi likevel ikke gir skåren i *stor grad* skyldes dette at systemene kan være utfordrende å ta i bruk for personer med digitalt utenforskap.<sup>14</sup> Det er videre usikkert om det er praktisk mulig å utforme løsninger som faktisk muliggjør selvstendig stemmegiving for alle velgere.

Til slutt er vår overordnede vurdering er at internettbaserte systemer også i noen grad oppfyller kriteriet brukervennlighet, men i stor grad oppfyller kriteriet inkludering. Internettbaserte systemer deler mange egenskaper med elektroniske stemmesystemer, men gir økt fysisk tilgjengelighet, og vil sannsynligvis gjøre selvstendig stemmegiving til en mulighet for blinde og svaksynte.

I det følgende beskriver vi nærmere hvordan hvert av valgsystemene gjør det opp mot hvert av kriteriene.

<sup>14</sup> Digitalt utenforskap innebærer manglende tilgang til eller mulighet til å bruke digitale tjenester som er nødvendige for å få innfridd sine rettigheter (Digdir, u.å.)

**Figur 7-1: Vurdering av stemmesystemer opp mot kriterier for brukervennlighet og inkludering**

	Papirbaserte systemer	Elektroniske systemer	Internettbaserte systemer	Oppfyller kriteriet
Brukervennlighet				
Inkludering				

I stor grad

I noen grad

I liten grad

Illustrasjon: Oslo Economics og Norsk Regnesentral

## 7.2 Papirbaserte systemer

### 7.2.1 Brukervennlighet

Kriteriet brukervennlighet handler om at stemmesystemet skal være enkelt å forstå og bruke for velgerne. Når det kommer til selve stemmegivningen i stemmelokalet, kommer det norske systemet relativt godt ut av det med tanke på brukervennlighet. Systemet er veletablert og velgermassen kjenner godt til hvordan det fungerer. Det er positivt for enkelte velgergrupper at det ikke kreves noen teknisk kompetanse å bruke det.

En spørreundersøkelse fra høsten 2020 med rundt 3 000 respondenter viser at rundt tre prosent av befolkningen i alderen 16 år og oppover ikke bruker internett eller digitale verktøy som smarttelefon, datamaskin og nettbrett og elleve prosent har svake grunnleggende digitale ferdigheter (Bjønness, et al., 2021). For denne gruppen kan det være uoverkommelige digitale hindringer med elektroniske og internettbaserte løsninger, men gruppen er vant med det ordinære, papirbaserte norske systemet.

Papirbaserte systemer har også svakheter. For det første er de ikke interaktive; systemet kan ikke automatisk kontrollere at velgeren har avgitt stemmen på en riktig måte. For det andre er det norske systemet mindre brukervennlig i form av tilgjengelighet for velgere generelt, sammenlignet med internettbaserte løsninger. Dette omhandler skillet mellom kontrollerte og ukontrollerte forhold, der kontrollerte forhold krever at velgeren kommer til et valglokale for å avgi stemme. For velgere som stemmer fra utlandet blir dette enda tydeligere ettersom deres fysiske tilgjengelighet til stemmelokaler er mer begrenset.<sup>15</sup> Dagens papirbaserte system i Norge bidrar til økt fysisk tilgjengelighet gjennom å tilby forhåndsstemmegiving og ambulerende stemmegiving i spesielle tilfeller. Det blir uansett mindre brukervennlig enn å stemme hjemme, men forskjellen mellom stemmegiving i valglokalet og stemmegiving hjemme blir mindre når forhåndsstemmegivningsmulighetene er gode.

<sup>15</sup> Merk, i analysen tar vi utgangspunkt i den delen av valget der stemmer avgis i valglokalet.

Vår vurdering er at papirbaserte systemer i noen grad oppfyller kriteriet brukervennlighet.

### 7.2.2 Inkludering

Kriteriet inkludering handler om brukervennligheten til stemmesystemer for grupper med særskilte behov, eksempelvis personer med en funksjonsnedsettelse eller reduserte kognitive evner, og dessuten hvordan systemet muliggjør selvstendig stemmegiving.

Det sentrale når det gjelder papirbaserte systemer er manglende mulighet til å ta i bruk digitale hjelpemidler. I det norske papirbaserte systemet anvendes generelle stemmesedler med punktskrift og noe større skrift enn andre stemmesedler. Dette bidrar til at blinde og svaksynte i mange tilfeller kan stemme selvstendig, noe som er avgjørende for hemmelig stemmegiving. Det er imidlertid ikke alle blinde og svaksynte som leser punktskrift, og ikke alle kommuner legger til rette for bruk av generelle stemmesedler (Saglie et al., 2022). Generelle stemmesedler gir heller ikke mulighet til å avgi personstemmer eller renummerere selvstendig.

Videre vil enkelte gruppers særskilte behov være knyttet til det å komme seg til valglokalet; da vil heller ikke et papirbasert system, som forutsetter stemmegiving i et stemmelokale, være gunstig. Vår vurdering er derfor at papirbaserte systemer i noen grad oppfyller kriteriet inkludering.

## 7.3 Elektroniske systemer

### 7.3.1 Brukervennlighet

Kriteriet brukervennlighet handler om at stemmesystemet skal være enkelt å forstå og bruke for velgerne. En fordel med elektroniske systemer er at de er interaktive. På denne måten kan velgere automatisk få beskjed hvis de gjør noe feil i stemmeprosessen. Dette kan bidra til å forhindre at stemmer blir forkastet ved feil utfyllelse, noe som skjer i et visst omfang ved papirbaserte systemer. Ved stortingsvalget i 2021 ble 4 517 stemmegivinger forkastet. Som beskrevet i delkapittel 5.2.6 blir flere stemmesedler forkastet fordi velgere bruker

stemmesedler som omslag for sin egentlige stemme. Dette problemet vil en ikke ha i elektroniske systemer.

Det kan imidlertid være problematisk for grupper med lavere teknisk kompetanse å ta i bruk elektroniske stemmesystemer, og siden stemmegivningen foregår i valglokaler kan reisevei være en barriere for enkelte velgere.

Samlet sett er det for elektroniske systemer en balansegang mellom utfordringer med bruk hos velgere med lav teknisk kompetanse, og fordeler som følge av interaktive løsninger. Vår vurdering er derfor at elektroniske systemer i noen grad oppfyller kriteriet brukervennlighet.

### 7.3.2 Inkludering

Kriteriet inkludering handler om brukervennligheten til stemmesystemer for grupper med særskilte behov, og dessuten hvordan systemet muliggjør selvstendig stemmegiving. Det er to ting som er særlig relevant for vurderingen av brukervennligheten av elektroniske systemer for grupper med særskilte behov.

For det første kan elektroniske systemer være interaktive og tilrettelegge for hjelpemidler. Dette kan gjøre løsningen mer brukervennlig og forståelig å bruke enn papirbaserte systemer, noe forsøk på området har vist (van Eijk et al., 2019). Spesielt synshemmede har et ønske om å bruke hjelpemidler og tilpassede løsninger som kan forbedre stemmegivningsprosessen (NOU 2020: 6).

Det er imidlertid usikkert i hvilken grad elektroniske løsninger faktisk vil legge til rette for selvstendig stemmegiving. En gruppe som kan oppnå selvstendig stemmegiving ved innføring av elektroniske løsninger er velgere som benytter generelle stemmesedler, men som ønsker å gi personstemmer, noe generelle stemmesedler ikke åpner for. En annen gruppe er svaksynte eller blinde som ikke bruker punktskrift, men som bruker hjelpemidler som elektroniske løsninger kan tilrettelegge for. Utfordringen er å utvikle elektroniske løsninger som tillater dette. Blinde og svaksynte kan være avhengig av PC-er med spesialtilpasset programvare og hjelpemidler de er kjent med for å kunne stemme på denne måten. Det vil være utfordrende å sette opp og tilrettelegge for alle variasjoner av nødvendige hjelpemidler i kontrollerte omgivelser.

For det andre vil elektroniske systemer i valglokaler også innebære en reisevei for velgere, som vil gå særlig ut over noen grupper med særskilte behov.

Samlet sett vurderer vi at elektronisk stemmegiving i noen grad oppfyller kriteriet inkludering. Det er imidlertid verdt å understreke at elektroniske systemer

kan utformes på måter som bidrar til bedre brukervennlighet for personer med særskilte behov i visse tilfeller sammenlignet med papirbasert stemmegiving.

## 7.4 Internettbaserte systemer

### 7.4.1 Brukervennlighet

Kriteriet brukervennlighet handler om at stemmesystemet skal være enkelt å forstå og bruke for velgerne. På samme måte som elektroniske systemer kan internettbaserte systemer gjøres interaktive, med de fordelene det medfører for velgere. En annen fordel med internettbaserte systemer er at de fjerner eventuelle barrierer knyttet til reisevei, noe som spesielt vil være gunstig for velgere i rurale strøk med lang reisevei eller velgere i utlandet som må reise til en ambassade. Studier har vist at enkelhet i stemmemåte er en viktig grunn for velgere som velger å stemme over internett (Segaard et al., 2014). I Estland har det over tid blitt en større andel av velgerne som benytter seg av den internettbaserte stemmeløsningen, istedenfor papirbasert alternativ (Ehin et al., 2022).

Segaard et. al (2014) beskriver at det kommer til uttrykk i medier og blant folk at internettvalg bidrar til å øke valgdeltakelsen, men at forskningslitteratur i liten grad kan støtte opp om dette. De undersøkte hvordan valgdeltakelsen ble påvirket av muligheten til å stemme over internett ved forsøksvalget i 2013. I tråd med tidligere forskningsresultat fant de ikke at forsøket med stemmegiving over internett førte til økt valgdeltakelse.

Utfordringen for brukervennligheten til internettbaserte systemer er tilgjengeligheten til velgere med svakere teknisk kompetanse. Disse utfordringene har en også ved elektroniske systemer, men utfordringene er trolig større ved internettbaserte systemer. Årsaken er at det er vanskeligere å tilby veiledning når velgerne ikke stemmer i et valglokale.

Alt dette tatt i betraktning, er vår vurdering at internettbaserte systemer i noen grad oppfyller kriteriet brukervennlighet.

### 7.4.2 Inkludering

Kriteriet inkludering handler om brukervennligheten til stemmesystemer for grupper med særskilte behov, og dessuten hvordan systemet muliggjør selvstendig stemmegiving. Som forklart tidligere, er sentrale forhold hvorvidt stemmeløsningen tillater interaktive løsninger, tilrettelegging for bruk av hjelpemidler og om det er lave reisebarrierer.

Vurderingen av inkludering ved internettbaserte systemer er i stor grad den samme som for elektroniske systemer, men noe bedre. Som beskrevet under vurderingen av inkludering i elektroniske systemer, kan blinde og svaksynte være avhengig av

PC med spesialtilpasset programvare de er kjent med. Internettbaserte systemer kan sannsynligvis utformes slik at bruk av spesialiserte hjelpemidler kan anvendes i stemmegivningen, og dermed muliggjøre selvstendig stemmegiving for denne gruppen.

Det har generelt vært begrenset med forskning på funksjonshemmede og grupper med særskilte behovs bruk av internettbaserte løsninger (Fuglerud & Røssvoll, 2012), men vår samlede vurdering er at internettbaserte systemer i stor grad oppfyller kriteriet inkludering.

## 7.5 Særlig om brukervennligheten til ende-til-ende-systemer

I enkelte av vurderingene ovenfor har vi skissert ende-til-ende elektroniske og internettbaserte systemer som et alternativ til klassiske systemer. Bruk av ende-til-ende-systemer, enten i elektronisk eller internettbaserte systemer, er nært knyttet til brukervennligheten til systemet. Integritetsgarantien som slike systemer gir, forutsetter at den enkelte velger tar ansvaret med å kontrollere at stemmen er korrekt registrert og å utfordre systemet ved å avgi kontrollstemmesedler. I praksis har det vist seg at velgerne har problemer med å forstå hensikten og å

bruke systemene i praksis. Forsøk med tre forskjellige ende-til-ende-systemer (Helios, Prêt à Voter og Scantegrity II) viste at velgerne fant dem «eksepsjonelt vanskelige» å bruke i praksis, enten de bruker stemmesedler av papir eller ikke, med bare 58 prosent av stemmene vellykket avgitt (Acemyan et al., 2014). En annen undersøkelse viste at avhengig av hvilken verifikasjonsmetode som ble brukt, klarte henholdsvis 61,3 prosent og 81,3 prosent av førstegangsvelgere å verifisere at stemmen deres var korrekt avgitt selv om alle var overbevist om at den var det (Marky et al., 2018).

En annen studie gjort med det elektroniske ende-til-ende-systemet vVote konkluderte med at det var veldig lett å bruke (Burton et al., 2016). Med et så stort sprik i resultater er det grunn til å se nærmere på metodene som er brukt. En nærliggende forklaring er at mens alle studiene registrerte hvor lett velgerne syntes systemet var å bruke, var det kun de først nevnte som faktisk målte hvor mange stemmer som ble vellykket avgitt. Det er altså grunn til å tro at sistnevnte studie har betydelig metodesvakhet.

Alt tatt i betraktning, er det stor grunn til å stille spørsmål ved brukervennligheten til ende-til-ende-systemer.

## 8. Ressursbruk

Ressursbruk omhandler hva som kreves av menneskelige og finansielle ressurser ved innføring og drift av elektronisk- og internettbaserte stemmesystemer som et supplement til dagens papirbaserte valg gjennomføring. For kommunene vil sannsynligvis innføringen av elektroniske stemmesystemer være mest ressurskrevende, mens for staten vil det trolig være noe mer ressurskrevende å få på plass et system for internettbasert stemmegiving. I dette kapitlet gir vi en nærmere beskrivelse av hva som påvirker ressursbruken.

### 8.1 Hovedfunn: Ressursbruk

I vurderingen av sikkerhet, transparens og etterprøvnbarhet, og brukervennlighet og inkludering har vi vurdert forhold knyttet til papirbaserte, elektroniske og internettbaserte systemer isolert sett. Men dersom e-valg skal tas i bruk, vil det trolig være som et supplement til dagens papirbaserte valg gjennomføring. Figur 8-1, som oppsummerer våre

**Figur 8-1: Vurdering av ressursbruk opp mot dagens papirbaserte valg gjennomføring**

	Lokalt nivå		Sentralt nivå		Vurdering
	Elektroniske systemer	Internettbaserte systemer	Elektroniske systemer	Internettbaserte systemer	
Materiell, utstyr og systemer	Orange	Grønn	Orange	Orange	Grønn
Bemannning	Blå	Grønn	Blå	Orange	Blå
Lokaler	Blå	Grønn	Ikke relevant	Ikke relevant	Blå
Informasjon og veiledning	Blå	Blå	Blå	Orange	Orange

Illustrasjon: Oslo Economics og Norsk Regnesentral

### 8.2 Elektroniske systemer

Vi forutsetter at finansiering av utvikling av løsninger for elektronisk stemmegiving skjer på nasjonalt nivå. Dette er også anbefalt i kunnskapsinnhenting om elektronisk stemmegiving fra 2006 (Kommunal- og regionaldepartementet, 2006). Begrunnelsen baserer seg på at det er stordriftsfordeler ved å utvikle løsninger sentralt.

vurderinger knyttet til ressursbruk, viser derfor våre vurderinger av hva det vil kreve av ressurser, på lokalt og sentralt nivå, ved å innføre elektronisk- eller internettbaserte systemer som et supplement til dagens papirbaserte valg gjennomføring.

På kort sikt vil det naturligvis være vesentlig mer ressurskrevende å drifte et papirbasert og et elektronisk valg system samtidig enn bare et papirbasert system. Kostnadene vil kunne reduseres på sikt, men det er mer sannsynlig at en delvis innføring av e-valg også på sikt vil være mer ressurskrevende enn å fortsette kun med dagens papirbaserte system.

En delvis innføring av elektroniske systemer vil være ressurskrevende, både for kommunene og for staten. For kommunene er det særlig anskaffelsen og driften av stemmemaskinene som er kostbart.

Internettbaserte løsninger kan på flere områder tenkes å være ressursbesparende for kommunene. Her vil en større del av kostnaden ligge på staten. Løsningene stiller store krav til systemutvikling og sikkerhet, noe som påvirker både kostnader til *Materiell, utstyr og systemer*, og dessuten *Bemannning*.

#### 8.2.1 Ressursbruk på lokalt nivå

For kommunene vil en innføring av elektroniske systemer som supplement til dagens papirbaserte valg gjennomføring være ressurskrevende. Selv om det er rimelig å anta at staten vil dekke kostnadene med utvikling av systemene, er det kommunene som må anskaffe og drifte stemmemaskinene. Det er et forholdsvis stort spekter av ulike typer stemmemaskiner. Ulike løsninger av elektroniske systemer spenner fra ordinære datamaskiner til avanserte stemmemaskiner. Følgelig varierer anskaffelses-kostnadene i stor grad. Stemmemaskiner anvendt i

India kan ha en pris på rundt 2 000 kroner, mens maskiner benyttet i USA kan ha en prislapp på flere titalls tusen kroner (Wolchok et al., 2010).

I tillegg til kostnader ved systemene, er det sannsynlig at det må gjøres ytterligere tilpasninger i lokalene som kommunene anvender til valg. Elektroniske stemmemaskiner kan eksempelvis stille større krav til nettverksinfrastruktur til/fra lokalene.

Når det gjelder bemanning antas det å ikke være omfattende endringer i behovet for valgfunksjonærer. Det kan være at bruk av elektroniske akkreditiver kan gi en tidsbesparelse i stemmemottak sammenlignet med dagens løsning med fremvisning av legitimasjon, men effekten antas å være svært begrenset. Det må imidlertid brukes mer ressurser på opplæring, slik at valgfunksjonærene kan yte bistand til velgere som ønsker å stemme elektronisk, og omfanget av informasjonsarbeid i forkant av valget vil sannsynligvis øke.

I tillegg til valgfunksjonærer må kommunen sannsynligvis ansette eller inngå avtaler med personer som kan yte bistand dersom det skulle oppstå problemer med maskinene underveis i valg gjennomføringen.

At det å innføre elektronisk valg som er supplement til papirbaserte valg kan være kostnadsdrivende understøttes fra erfaringer med elektroniske valg i England (Christensen et al. 2004).

### 8.2.2 Ressursbruk på sentralt nivå

Innføring av elektroniske systemer medfører at staten må utvikle et system for stemmegiving, telling og registrering av stemmer. Det å drive denne prosessen vil i seg selv være ressurskrevende. I tillegg vil det være behov for koordinering og inngåelse av avtaler for salg og distribusjon av stemmemaskiner til kommunene.

Ytterligere vil innføring av elektronisk stemmegiving medføre endret funksjonalitet i EVA Admin. Dette skjer som følge av at prosessen med registrering av stemmesedler blir automatisert, og EVA Admin må tilpasses til den endrede stemmeprosessen. EVA Skanning og skanneløsninger er ikke relevante i de fleste løsninger for elektroniske systemer ettersom velgeren ikke bruker stemmesedler av papir.

Behovet for informasjonskampanjer ut mot velgere vil også øke fra sentralt hold. Elektroniske løsninger vil være mer krevende å forstå for velgerne, slik drøftet i kapittel 7. Informasjonskampanjene bør omfatte beskrivelser av praktisk gjennomføring. Videre kan det være ønskelig å kommunisere hvilke sikkerhetsmekanismer som er innbygget i systemarkitekturen for å sikre transparens om løsningen.

Vi forventer også at kommunene vil ha et økt informasjonsbehov ved elektroniske systemer, og et økt behov for opplæring fra Valgdirektoratet.

## 8.3 Internettbaserte systemer

Et sentralt element ved internettbaserte løsninger er at en rekke praktiske arbeidsoppgaver løftes fra et lokalt til et nasjonalt nivå. Dette kommer av at internettbaserte løsninger i større grad er basert på sentraliserte løsninger. Dette er beskrevet inngående i kapittel 3.

### 8.3.1 Ressursbruk på lokalt nivå

Internettbaserte løsninger medfører mindre ressursbruk i kommunene enn elektroniske løsninger. Studier understøtter dette ved å antyde at internettstemmegiving er et mindre kostbart alternativ enn andre stemmesystemer (Krimmer et al., 2018, 2021). Det er imidlertid begrenset med studier på området.

Ved internettbaserte stemmesystemer foregår ikke stemmegivingen i kontrollerte omgivelser, stemmeavgivelsen blir sendt til en sentral urne, og det er følgelig ikke noen form for lokal optelling av stemmer, eller behov for å tilpasse lokalene.

Hvis omfanget av internettstemmegiving blir utbredt kan det på sikt redusere kommunenes behov for bemanning, både ved mottak og telling av stemmer. Det kan imidlertid være nødvendig med en form for lokalt tilgjengelig servicepersonell om det skulle oppstå tekniske problemer. For en viktig begivenhet som valg vil ikke nødvendigvis et nasjonalt service-senter oppleves tilstrekkelig. Det kan være en rekke velgere som har behov for at en fysisk serviceperson kommer og ser på det aktuelle problemet.

### 8.3.2 Ressursbruk på sentralt nivå

Innføring av et internettbasert system medfører at staten må utvikle systemet og få det tilpasset både lokale forhold og det sentrale valgadministrasjons-systemet, EVA.

Sammenlignet med elektroniske systemer er det rimelig å anta at systemutviklingen vil være mer krevende. Trusselbildet er større ved internettbaserte systemer, noe som stiller større krav til løsningenes sikkerhet. Videre vil autentisering være et sentralt spørsmål i utformingen av et internettbasert system, og det vil antakelig være krevende i både en teknisk og organisatorisk forstand. Av eksisterende løsninger for elektroniske akkreditiver i Norge er BankID et aktuelt alternativ, men selv i tilfeller der autentiseringen baserer seg på eksisterende løsninger er det forventet at det vil være nødvendig med tilpasninger for å fungere i et stemmesystem, med de krav det medfører.

Med internettbaserte systemer vil det ikke være nødvendig med koordinering og avtaler for salg og distribusjon av stemmemaskiner til kommunene. På den andre siden vil lokasjon av urne og lokasjon av opptellingen ligge sentralt. Dette vil kreve at staten oppretter sentrale elektroniske lager. I praksis vil dette typisk vil være en sentral server i et datasenter.

Vi antar derfor at kostnadene knyttet til systemer vil være større ved internettbaserte systemer, sammenlignet med elektroniske. Vi antar også at

informasjonsbehovet ut mot velgerne vil øke fra sentralt hold.

Når det gjelder kommunene vil det være behov for en annen type opplæring og veiledning, sammenlignet med elektroniske systemer. Dette som følge av at kommunene ikke har de samme arbeidsoppgavene forbundet med internettbaserte systemer som for elektroniske. Men selv om oppgavene isolert sett er færre, kan det være behov for at kommunene må bistå velgere, og tilby en viss veiledning på dette området.

## 9. Oppsummerende vurdering av risiko, gevinster og kostnader

*Kunnskapsinnhenting har avdekket at det finnes en rekke mulige løsninger for elektronisk stemmegiving. Risikoen ved både elektroniske og internettbaserte stemmesystemer er primært knyttet til sikkerhet, mens de mulige gevinstene ligger i bedre inkludering av grupper med særskilte behov. Kunnskapsinnhenting gir ikke grunnlag for å trekke en bestemt konklusjon av hva som bør veie tyngst av disse hensynene.*

### 9.1 Ingen systemer er perfekte

Analysen viser at ingen av de tre hovedkategoriene av stemmesystemer er bedre enn de to andre systemene på alle punkter. Dagens papirbaserte system er alene om å i stor grad tilfredsstillende kriteriene anonymitet, valgintegritet, korrekthet, transparens og etterprøvbarehet, mens internettbaserte systemer er alene om å i stor grad tilfredsstillende kriteriet for inkludering av grupper med særskilte behov.

Forskjellene mellom systemene som reflekteres i analysen er ikke primært et resultat av hvor langt den teknologiske utviklingen nå har kommet, eller hvordan systemene i dag er utformet. Trolig vil det også i fremtiden være krevende å imøtekomme kriteriet om inkludering av grupper med særskilte behov med dagens papirbaserte valgsystem, og en vil ikke kunne garantere fullt ut for sikkerheten til elektroniske og internettbaserte systemer.

### 9.2 Risiko ved elektronisk og internettbasert stemmegiving

Analysen av sikkerheten til ulike tekniske løsninger for elektronisk stemmegiving har avdekket at det per i dag ikke er mulig å utforme tekniske løsninger som fullt ut kan garantere for sikkerheten til valg-gjennomføringen på samme måte som papirbaserte systemer. Utfordringen er særlig knyttet til skalerbare angrep og angrep som ikke lar seg oppdage, eller som det er sannsynlig at ikke blir oppdaget. Videre skaper det sterke sentraliseringsmomentet en risiko. Ende-til-ende elektroniske systemer har sentralisert stemmehåndtering, mens internettløsninger er fullt sentraliserte, noe som gir en systemsårbarhet. Videre ligger det en sårbarhet i at det kun er noen få spesialister som fullt ut forstår systemets virkemåte.

Kunnskapsinnhenting har avdekket at vurderinger knyttet til sikkerhetsmessige aspekter ved elektronisk

stemmegiving har et annet bakteppe i dag enn tidligere. Mange av de overordnede vurderingene er likevel de samme i dag som det en arbeidsgruppe nedsatt av det daværende Kommunal- og regionaldepartementet konkluderte med i rapporten *Elektronisk stemmegiving – utfordringer og muligheter* fra 2006 (Kommunal- og regionaldepartementet, 2006).

Siden 2006, og siden e-valgforsøkene i Norge i 2011 og 2013 har det skjedd en betydelig utvikling på teknologifronten, og digitale løsninger har blitt enda mer fremtredende. Flere samfunnskritiske funksjoner er i stor grad digitalisert, og det er derfor nærliggende å spørre om ikke teknologien nå gjør det mulig å garantere for sikkerheten til elektroniske stemmesystemer.

For å besvare spørsmålet er det relevant å se utviklingen i sikkerhet for elektroniske stemmesystem i sammenheng med utvikling i datasikkerhet generelt de siste ti årene i Norge. I løpet av disse årene har det skjedd svært lite som endrer grunnleggende forutsetninger for hvordan man arbeider med sikkerhet. Ett unntak er muligens såkalt «self-sovereign identity» (SSI). SSI innebærer at den enkelte bruker utsteder sin egen desentraliserte digitale identitet og har full kontroll over akkreditiver som er utstedt til seg selv og koblet til denne identiteten. Elektronisk stemmegiving har blitt fremhevet som et område som kan nyttiggjøre seg av SSI (Preukschat & Reed, 2021). Imidlertid er SSI så nytt at det antagelig ikke vil få noen praktisk betydning på mange år ennå. Generelt tar det typisk flere tiår før en oppfinnelse eller oppdagelse av prinsipiell betydning får utbredelse og praktiske konsekvenser. Det kan derfor være mer hensiktsmessig å se på hvilke teknologier eller praksiser som har endret utbredelse de siste årene.

Et eksempel på en generell trend som trekker i retning av økt sikkerhetsnivå, er den stadig større utbredelsen av to-faktor autentisering. Dette er en form for autentisering der man benytter to autentiseringsmetoder i kombinasjon. Et eksempel på dette er BankID, der man benytter både en kodegenerator og et fast passord. Det er også blitt mer vanlig at data krypteres under overføring; ukrypterte nettsider er i dag mindre vanlige enn krypterte. På noen plattformer er det blitt vanlig med mer sofistikerte systemer for tilgangskontroll (såkalt obligatorisk tilgangskontroll), noe som generelt begrenser konsekvensene av skadevare. Når det gjelder organisatoriske endringer er det blitt mer vanlig, spesielt blant større bedrifter, å ha et styrings-system for sikkerhet, som for eksempel ISO 27001.



Selv om sikkerheten til systemene isolert sett har blitt bedre, stilles systemene overfor stadig mer sofistikerte trusler. Næringslivets sikkerhetsråd publiserer annethvert år rapporten *Mørketallsundersøkelsen*, som omhandler tilstanden for datasikkerhet hos norske bedrifter. Både offentlige instanser, som Kripos, PST og NSM, og private aktører, som Norman, Mnemonic og Microsoft, bidrar til analysen. I perioden 2012 til 2022 har det vært en økning av digitale operasjoner fra trusselaktører mot norske mål. Dette inkluderer virksomheter som ivaretar viktige samfunnsfunksjoner, særlig innen sektorer som forsvar, rom, maritim, petroleum, kraft, samferdsel, forskning og høyere utdanning, elektronisk kommunikasjon og helse.

Trusselaktørene kan både være statstilknyttede og kriminelle aktører, og motivene inkluderer vinning, spionasje og sabotasje. Disse trusselaktørene blir både mer selektive i sine mål og mer avanserte i sine metoder, som for eksempel

- verdikjedeangrep (leverandørkjedeangrep) – angrep mot leverandører, partnere og andre tredjeparter som et ledd for å nå et spesifikt mål
- spear phishing – direktørsvindel
- løsepengevirus
- utpressing med DDOS-angrep
- ID-tyveri

Valggjennomføring er et relevant mål for digitale operasjoner. Det er gjort undersøkelser av hvorvidt utenlandske aktører forsøkte å påvirke det norske stortingsvalget i 2021 (Sivertsen et al., 2022). Det ble ikke funnet indikasjoner på at utenlandske aktører forsøkte å påvirke valget, valgresultatet, valgdeltakelsen eller tilliten til valget. Funnene i rapporten viser imidlertid at informasjonspåvirkning mot demokratiet foregår i betydelig omfang. Denne illegitime aktiviteten er ofte subtil og med lav intensitet over tid. Det muligens mest kjente eksemplet på statlige aktørers valgpåvirkning i andre land er Russlands handlinger for påvirkning av de føderale valgene i USA i 2016 og 2020. National Intelligence Council, en del av amerikansk etterretningstjeneste, konkluderte i en undersøkelse av fremmede aktørers påvirkning på valget i 2020, at Russland ikke forsøkte å endre noen tekniske aspekt ved valggjennomføringen (National Intelligence Council, 2021). Dette omfatter stemmeprosessen med velgerregistrering, stemmegiving og telling. Derimot fant de at det var utbredte påvirkningskampanjer rettet mot amerikanske velgere, med mål om å undergrave velgeres tillit til valggjennomføringen, og dessuten øke de sosiopolitiske forskjellene.

En annen utvikling i datasikkerhet knyttet til elektronisk stemmegiving spesifikt omhandler forholdet mellom mobiltelefon og personlige datamaskiner. Etter år-

tusenskiiftet har skillet mellom mobiltelefon og datamaskin blitt mindre tydelig, og mange personer benytter mobiltelefonen sin til oppgaver der de tidligere ville brukt en personlig datamaskin. Eksempelvis leser mange personer tekstmeldinger på bærbare datamaskiner, og mange benytter nettlese på mobil. Den internettbaserte løsningen som ble brukt i det norske forsøket i 2013 benyttet løsninger som baserte seg på en uavhengighet mellom mobiltelefoner og datamaskin for stemmeavgivelse, men det kan være en mindre gyldig antakelse i ettertid (Gjøsteen, 2013).

Skal en lytte til eksperter på datasikkerhet og nettangrep vil konklusjonen være at en aldri vil kunne garantere fullt ut for sikkerheten til digitale stemmesystemer. Dette skyldes at den teknologiske utviklingen skjer så raskt at myndigheter og teknologi-eksperter vil ha svært vanskelig for å lage et system som med tilnærmet 100 prosent sikkerhet kan motstå eller avverge angrep. I praksis gir dette seg utslag i at sikkerhet til sist hviler på muligheten for å oppdage og respondere på angrep og å ha gode manuelle beredskapsrutiner og -tiltak (NOU 2020: 6).

### 9.3 Prinsipielle forskjeller mellom stemmesystemer

Selv dersom det var mulig å garantere for sikkerheten til elektroniske og internettbaserte systemer, ville det være prinsipielle forskjeller mellom systemene på andre områder. Dette gjelder særlig mellom dagens papirbaserte valgsystem, som foregår i kontrollerte omgivelser, og internettbaserte valg i ukontrollerte omgivelser.

I innledningen av rapporten beskriver vi hvordan Valglovutvalget har utledet følgende prinsipper for det norske valgsystemet:

- Valget skal være fritt.
- Valget skal være hemmelig.
- Valget skal være direkte.
- Stemmeretten skal være allmenn og lik.
- Valg skal holdes med jevne mellomrom.
- Alle med stemmerett skal ha mulighet til å stemme.
- Alle med stemmerett skal kunne velges.
- Hver stemme skal ha lik vekt.
- Valgordningen skal sikre geografisk representasjon.

Forskjellene mellom valg i kontrollerte omgivelser og internettbaserte valg i ukontrollerte omgivelser kommer særlig til syne i prinsippet om at valget skal være hemmelig.

Som drøftet i kapittel 7, er det bare internettbaserte systemer som i stor grad oppfyller kriteriet for inkludering av grupper med særskilte behov. Dette er

knyttet til at internettbaserte systemer muliggjør selvstendig stemmegiving for blinde og svaksynte. I dagens norske valgsystem er det åpnet for at blinde og svaksynte selv kan velge hvem som skal ledsage dem i stemmeavsluttet. Sammenlignet med tidligere, hvor valgmedarbeidere måtte brukes som ledsagere, er dette ansett som en forbedring. Men valget er fortsatt ikke hemmelig, om en legger en streng fortolkning av prinsippet til grunn.

En åpning for internettbasert stemmegiving skaper imidlertid andre utfordringer for prinsippet om hemmelige valg. Under kategorien sikkerhet i kapittel 5 viste vi at internettbaserte systemer i liten grad tilfredsstiller kriteriet *anonymitet*. Ved at stemmene avgis i ukontrollerte omgivelser, gir ikke systemet i seg selv en garanti for at ingen andre observerer stemmen, og dermed ingen garanti for hemmelige valg.

Internettbasert stemmegiving utfordrer også prinsippet om at valget skal være fritt. Ved at stemmegivingen kan observeres av andre, øker risikoen for at en velger kan presses av andre til å foreta et bestemt valg. Som beskrevet i kapittel 5, kan det å utforme systemet slik at velgeren kan endre stemmen inntil fristen for stemmegivingen går ut redusere risikoen for bruk av tvang. Risikoen reduseres dersom internettbasert stemmegiving innføres som et supplement til papirbaserte valg, og eksempelvis begrenses til forhåndsstemmeperioden. Da kan systemer utformes slik at avlagte papirstemmer på valgdagen trumfer stemmer avgitt elektronisk i forhåndsstemmeperioden.

Prinsippet om hemmelige valg står sterkt i Norge, og som denne kunnskapsinnhenting har avdekket er det ikke åpenbart hvilket stemmesystem som best ivaretar dette prinsippet. Det er imidlertid relativt åpenbart hvilke grupper det er som ikke kan foreta hemmelige valg i Norge i dag; blinde og svaksynte. Et alternativ som har blitt fremmet er derfor å åpne opp for internettbasert stemmegiving kun for denne gruppen.

Valglovutvalget (NOU 2020: 6), drøftet innføring av elektronisk stemmegiving for mennesker med funksjonsnedsettelse. Med utgangspunkt i internettbaserte løsninger ble fordelene ved at dette gir blinde og svaksynte mulighet til å stemme alene veid opp mot utfordringene med hemmelig stemmegiving. Utvalget mente at elektronisk stemmegiving i valglokalet vil kunne gjøre det mulig for personer med synshemming å stemme alene (NOU 2020: 6). Kunnskapsinnhenting har avdekket at det er praktisk utfordrende å utvikle elektroniske løsninger som tillater selvstendig stemmegiving, og at det sannsynligvis bare er internettbaserte systemer som muliggjør selvstendig stemmegiving for blinde og svaksynte.

Vi har ikke sett nærmere på hva som kreves av økonomiske og organisatoriske ressurser for å få etablert en slik løsning, men vi ser at delvis innføring på denne måten har både praktiske og prinsipielle sider som det er viktig å være klar over. For det første er det en utfordring å bestemme hvem som skal ha mulighet til å stemme elektronisk eller ikke. For det andre må det legges til rette for en innsamling og behandling av stemmene som ivaretar prinsippet om hemmelig valg. I mindre kommuner vil det kunne være et fåtall velgere, kanskje bare én, som kvalifiserer til bruk av elektronisk stemmegiving. Da kan ikke de elektroniske stemmene telles sammen med de ordinære stemmesedlene. Stemmen må rutes til et sentralt register slik at det ikke er mulig å spore hva enkeltvelgere har svart.

## 9.4 Kostnader for stat og kommune

I kunnskapsinnhenting har vi vurdert ressursbruk for stat og kommune ved bruk av elektroniske og internettbaserte systemer for stemmegiving som et supplement til dagens papirbaserte valgsystem.

På kort sikt vil det naturligvis være vesentlig mer ressurskrevende å drifte et papirbasert og et elektronisk valgsystem samtidig enn bare et papirbasert valgsystem. Kostnadene vil kunne reduseres på sikt, men det er mer sannsynlig at en delvis innføring av e-valg også på sikt vil være mer ressurskrevende enn å fortsette kun med dagens papirbaserte system.

En delvis innføring av elektroniske systemer vil være ressurskrevende, både for kommunene og for staten. For kommunene er det særlig anskaffelsen og driften av stemmemaskinene som er kostbart.

Internettbaserte løsninger kan på flere områder tenkes å være ressursbesparende for kommunene. Her vil en større del av kostnaden ligge på staten. Løsningene stiller store krav til systemutvikling og sikkerhet.

Innføringen av elektronisk stemmegiving vil i tillegg stille helt andre krav til kompetanse enn det kommunene i dag besitter. Selv med utstrakt bruk av innleid ekspertise er det trolig behov for kompetansebygging i kommunene, og det vil uansett være behov for å gi valgfunksjonærene utvidet opplæring. Dette gjelder i særlig grad ved elektroniske systemer, hvor stemmemaskinene er plassert i valglokalene, men også ved internettbaserte systemer er det sannsynlig at kommunen må tilby en eller annen form for support til innbyggerne.

## 9.5 Oppsummerende betraktninger

At det ikke er mulig å garantere for sikkerhet i elektroniske løsninger fører med seg en risiko for tap av tillit. Valgløtvalget påpeker at dersom sikkerheten rundt valggjennomføringen svekkes, vil det kunne få svært alvorlige konsekvenser både for valget som en sentral demokratisk ordning, for tilliten til valggjennomføringen og for valgresultatet. Svekket tillit til valggjennomføringen er ikke avhengig av et faktisk sikkerhetsbrudd. Kun en oppfatning blant deler om av befolkningen om tvil ved gyldigheten til valgresultatet, vil kunne påvirke tilliten til valggjennomføringen og valgresultatet. En mulighet for å sikre bedre tilgjengelighet for flere, og samtidig begrense risiko for tap av tillit, er å åpne for elektronisk stemmegivning kun for utvalgte velgergrupper. Ikke fordi deres stemmer er mindre viktige, men fordi et brudd på sikkerheten vil ha lavere økonomiske og samfunnsmessige kostnader i form av redusert tillit, jo færre stemmer det gjelder.

Det varierer hvordan et lands myndigheter, og velgerne i landet, ser på elektroniske- og internettbaserte stemmesystemer. Avveiningen mellom eventuelle gevinster knyttet til brukervennlighet og inkludering, og risikoen knyttet til sikkerhet avhenger i stor grad av landspesifikke forhold, og forhold knyttet til det eksisterende valgsystemet. I tillegg har personlige preferanser betydning. Noen kan være villig til å akseptere sikkerhetsrisikoen som ligger i bruk av elektroniske systemer i bytte mot en valggjennomføring som er bedre tilpasset velgere med særskilte behov. Andre har motsatt syn på denne avveiningen.

Oppsummert finnes en rekke muligheter for å innføre elektronisk stemmegiving, noe erfaringer fra andre land viser. Risikoen er primært knyttet til sikkerhet, mens de mulige gevinstene ligger i bedre inkludering av grupper med særskilte behov.

## 10. Referanser

- Acemyan, C. Z., Kortum, P., Byrne, M. D., & Wallach, D. S. (2014). *Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II*. 2(3).
- Adida, B. (2008). Helios: Web-based Open-Audit Voting. *Proceedings of the 17th USENIX Security Symposium*, 14.
- Adida, B., & Rivest, R. L. (2006). Scratch & vote: Self-contained paper-based cryptographic voting. *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society - WPES '06*, 29. <https://doi.org/10.1145/1179601.1179607>
- Applegate, M., Chanussot, T., & Vladlen, B. (2020, april 1). *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. GovWhitePapers. <https://govwhitepapers.com/whitepapers/considerations-on-internet-voting-an-overview-for-electoral-decision-makers/>
- Aragon. (u.å.). *Vocdoni, Easy and secure solutions for all your governance needs*. Hentet 3. juni 2022, fra <https://aragon.org/vocdoni>
- Aranha, D. F., & van de Graaf, J. (2018). The Good, the Bad, and the Ugly: Two Decades of E-Voting in Brazil. *IEEE Security & Privacy*, 16(6), 22–30. <https://doi.org/10.1109/MSEC.2018.2875318>
- Bell, S., Benaloh, J., Byrne, M. D., DeBeauvoir, D., Eakin, B., Fisher, G., Kortum, P., McBurnett, N., Montoya, J., Parker, M., Pereira, O., Stark, P. B., Wallach, D. S., & Winn, M. (2013). *STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System*. 1(1), 20.
- Benaloh, J., Rivest, R., Ryan, P. Y. A., Stark, P., Teague, V., & Vora, P. (2014). *End-to-end verifiability*.
- Burton, C., Culnane, C., & Schneider, S. (2016). vVote: Verifiable Electronic Voting in Practice. *IEEE Security & Privacy*, 14(4), 64–73. <https://doi.org/10.1109/MSP.2016.69>
- Carback, R., Chaum, D., Clark, J., & Conway, J. (2010). *Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy*. 16.
- Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R. L., Ryan, P. Y. A., Sherman, A. T., & Shen, E. (2008). Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. *EVT*, 13.
- Christensen, D. A., Karlsen, R., & Aardal, B. (2004). *På vei til e-demokratiet? Forsøkene med elektronisk stemmegivning ved kommune- og fylkestingsvalget i 2003*. Institutt for samfunnsforskning.
- Digdir. (u.å.). *Digitalt utenforskap | Digdir*. Hentet 4. oktober 2022, fra <https://www.digdir.no/rikets-digitale-tilstand/digitalt-utenforskap/3568>
- Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly*, 39(4), 101718. <https://doi.org/10.1016/j.giq.2022.101718>
- Eldridge, M. (2018). *A Trustworthy Electronic Voting System for Australian Federal Elections* (arXiv:1805.02202). arXiv. <https://doi.org/10.48550/arXiv.1805.02202>
- Enguehard, C., & Noûs, C. (2020). Some Things you may Want to Know about Electronic Voting in France. *Fifth Interntional Joint Conference on Electronic voting*.
- Europarådet. (2017). *Recommendation CM/Rec(2017)5[ of the Committee of Ministers to member States on standards for e-voting*. <https://rm.coe.int/0900001680726f6f>
- Feldman, A., Halderman, J. A., & Felten, E. (2006, september 13). Security Analysis of the Diebold AccuVote-TS Voting Machine. *Center for Information Technology Policy*. <https://citp.princeton.edu/our-work/voting/>
- Ford, B. (2022). *Auditing the Swiss Post E-voting System: An Architectural Perspective*. 21.
- Forskrift om valg til Stortinget, fylkesting og kommunestyre (valgforskriften)*. (2022, oktober 5). <https://lovdata.no/dokument/SF/forskrift/2003-01-02-5>
- Fuglerud, K. S., & Røssvoll, T. H. (2012). An evaluation of web-based voting usability and accessibility. *Universal Access in the Information Society*, 11(4), 359–373. <https://doi.org/10.1007/s10209-011-0253-9>
- Gjøsteen, K. (2013). The Norwegian Internet Voting Protocol. I A. Kiayias & H. Lipmaa (Red.), *E-Voting and Identity* (s. 1–18). Springer. [https://doi.org/10.1007/978-3-642-32747-6\\_1](https://doi.org/10.1007/978-3-642-32747-6_1)
- Gonggrijp, R., & Hengeveld, W.-J. (2007). *Nedap/Groenendaal ES3B voting computer: A security analysis*.
- Hart, C. (2001). *Doing a Literature Search: A Comprehensive Guide for the Social Sciences*. SAGE.
- Innst. 1 S (2021-2022)*. (2021). Stortinget.

- Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST SP 800-30r1; 0 utg., s. NIST SP 800-30r1). National Institute of Standards and Technology.  
<https://doi.org/10.6028/NIST.SP.800-30r1>
- Kirby, K., Masi, A., & Maymi, F. (2016). *Votebook: A proposal for a blockchain-based electronic voting system*. New York University.
- Kommunal- og moderniseringsdepartementet. (2014, juni 23). *Ikke flere forsøk med stemmegivning over Internett* [Pressemelding]. Regjeringen.no; regjeringen.no.  
<https://www.regjeringen.no/no/dokumentarkiv/regjeringen-solberg/aktuelt-regjeringen-solberg/kmd/pressemeldinger/2014/ikke-flere-forsok-med-stemmegivning-over-Internett-/id764300/>
- Kommunal- og regionaldepartementet. (2006). *Elektronisk stemmegiving—Utfordringer og muligheter*.  
<https://www.regjeringen.no/globalassets/upload/kilde/krd/rap/2006/0003/ddd/pdfv/272294-elektroniskstemmegivning.pdf>
- Kompetanse Norge. (2021). *Befolkningens digitale kompetanse og deltakelse*.  
<https://www.kompetansenorge.no/statistikk-og-analyse/publikasjoner/befolkningens-digitale-kompetanse-og-deltakelse/>
- Krimmer, R., Duenas-Cid, D., & Krivososova, I. (2021). New methodology for calculating cost-efficiency of different ways of voting: Is internet voting cheaper? *Public Money & Management*, 41(1), 17–26.  
<https://doi.org/10.1080/09540962.2020.1732027>
- Krimmer, R., Duenas-Cid, D., Krivososova, I., Vinkel, P., & Koitmae, A. (2018). How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia. I R. Krimmer, M. Volkamer, V. Cortier, R. Goré, M. Hapsara, U. Serdült, & D. Duenas-Cid (Red.), *Electronic Voting* (s. 117–131). Springer International Publishing. [https://doi.org/10.1007/978-3-030-00419-4\\_8](https://doi.org/10.1007/978-3-030-00419-4_8)
- Loeber, L. (2008). E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years. *Conference: 3rd International Conference, Co-Organized by Council of Europe, Gesellschaft Für Informatik and E-Voting, CC, August 6th-9th, 2008 in Castle Hofen, Bregenz, Austria*, 10.
- Lov om valg til Stortinget, fylkesting og kommunestyre (valgloven). (2022).  
<https://lovdata.no/dokument/NL/lov/2002-06-28-57>
- Marky, K., Kulyk, O., Renaud, K., & Volkamer, M. (2018). What Did I Really Vote For? On the Usability of Verifiable E-Voting Schemes. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3173574.3173750>
- National Intelligence Council. (2021). *Foreign Threats to the 2020 US Federal Elections*.
- Norges Blindforbund. (2021). *Tilrettelegging for valgdeltakelse*. Norges blindforbund.  
<https://www.blindforbundet.no/om-blindforbundet/nyhetsarkivet/tilrettelegging-for-valgdeltakelse-3>
- NOU 2020:6. (2020). *NOU 2020:6. Ny valglov—Frie og hemmelige valg*. Kommunal- og moderniseringsdepartementet.
- Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From Internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1), tyaa025. <https://doi.org/10.1093/cybsec/tyaa025>
- Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity*. Manning Publications.
- Rivest, R. L. (2006). *The ThreeBallot Voting System*. 15.
- Rogers, K. (2021, juli 7). New Laws Let Americans With Disabilities Vote Online. They've Also Resurrected The Debate About Voting Access vs. Election Security. *FiveThirtyEight*.  
<https://fivethirtyeight.com/features/new-laws-let-americans-with-disabilities-vote-online-theyve-also-resurrected-the-debate-about-voting-access-vs-election-security/>
- Ryan, P. Y. A., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2009). The Prent a` Voter Verifiable Election System. *IEEE Transactions on Information Forensics and Security*, 4, 662–673.
- Saglie, J., Christensen, D. A., Ervik, R., & Hesstvedt, S. (2022). Tilgjengelighet og -tilrettelegging for -funksjonshemmede ved stortingsvalget 2022. *Institutt for samfunnsforskning*, 80.
- Saglie, J., & Seggaard, S. B. (2016). Internet voting and the secret ballot in Norway: Principles and popular understandings. *Journal of Elections, Public Opinion and Parties*, 26(2), 155–169.  
<https://doi.org/10.1080/17457289.2016.1145687>
- Seggaard, S. B., Baldersheim, H., & Saglie, J. (2012). *E-valg i et demokratisk perspektiv*. Institutt for samfunnsforskning.
- Seggaard, S. B., Christensen, D. A., & Saglie, J. (2014). *Internettvalg—Hva gjør og mener velgerne?* Institutt for samfunnsforskning.

- Segaard, S. B., & Saglie, J. (2012). *Evaluering av forsøket med e-valg i 2011. Tilgjengeligheten for velgere, tillit, hemmelig valg og valgdeltakelse*. Institutt for samfunnsforskning.
- Sivertsen, E. G., Bjørgul, L., Endestad, I., Bornakke, T., Kristensen, J. B., Christensen, N. M., & Albrechtsen, T. (2022). *Uønsket utenlandsk påvirkning? – Kartlegging og analyse av stortingsvalget 2021*. Forsvarets forskningsinstitutt. <https://www.ffi.no/publikasjoner/arkiv/uonsket-utenlandsk-pavirkning-kartlegging-og-analyse-av-stortingsvalget-2021>
- Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security Analysis of the Estonian Internet Voting System. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 703–715. <https://doi.org/10.1145/2660267.2660315>
- Store Norske Leksikon. (2022). Europaåret. I *Store Norske Leksikon*. <https://snl.no/Europa%C3%A5det>
- Swiss Federal Chancellery. (2022). *E-Voting*. <https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html>
- USA.gov. (2022, august 9). *How to Register to Vote | USAGov*. <https://www.usa.gov/register-to-vote>
- Valgdirektoratet. (2021). *Veileder i sikkerhet—Hvordan gjennomføre sikre valg i kommuner og fylkeskommuner*. <https://valgmedarbeiderportalen.valg.no/media/reekxhft/veileder-i-sikkerhet.pdf>
- Valgmedarbeiderportalen. (2022). *Opptelling av forhåndsstemmer*. <https://valgmedarbeiderportalen.valg.no/tema/opptelling-av-forhandsstemmer/?role=1078>
- van Eijk, D., Molenbroek, J., Henze, L., & Niermeijer, G. (2019). Electronic voting for all: IEA 2018: 20th Congress of the International Ergonomics Association. *Proceedings of the 20th Congress of the International Ergonomics Association (IEA 2018) - Volume VII, VII*, 800–809. [https://doi.org/10.1007/978-3-319-96071-5\\_84](https://doi.org/10.1007/978-3-319-96071-5_84)
- Wolchok, S., Wustrow, E., Halderman, J. A., Prasad, H. K., Kankipati, A., Sakhamuri, S. K., Yagati, V., & Gonggrijp, R. (2010). Security analysis of India's electronic voting machines. *Proceedings of the 17th ACM Conference on Computer and Communications Security - CCS '10*, 1. <https://doi.org/10.1145/1866307.1866309>

## Vedlegg A Hendelser og risiko

Vi skiller mellom tilsiktede hendelser, utilsiktede hendelser og uønskede hendelser. Vi presenterer de i det følgende. Vi gjør oppmerksom på at vi ikke forventer at listen er uttømmende, men den illustrerer risikobildet.

### 10.1.1 Tilsiktede hendelser

- En velger utgir seg for å være en annen velger.
  - Velgeren bruker falske akkreditiver for å stemme på vegne av en annen person.
  - Velgeren bruker lånte akkreditiver for å stemme på vegne av en annen person.
- En annen person befinner seg sammen med velgeren i det han eller hun skal avgi stemmen. Dette kan være en hjelper som er med inn i valgavsluttet i et valglokale, eller en person som ser på skjermen.
- Familie, venner eller bekjente av velgeren presser vedkommende til å avgi en annen stemme enn det de selv ønsker ved å se på når stemmen avgis.
- Velgeren mottar ikke bekreftelse (implisitt, eksplisitt eller ende-til-ende-bekreftelse) på avgitt stemme.
- En angriper har korrumpert kildekoden til et operativsystem eller bibliotek for en bestemt nettleser eller et dedikert stemmeprogram til å endre hver avgitte stemme.
- En angriper har korrumpert kildekoden til et operativsystem eller bibliotek for en bestemt nettleser eller et dedikert stemmeprogram til å se hva den enkelte har stemmestemme.
- Stemmer som ligger i urne blir endret:
  - Urner mistes eller blir stjålet.
  - Avgitte stemmer blir endret.
- Stemmer som ligger i urne blir lest og talt. Resultatet kan bli publisert før tiden.
- En angriper avleser avgitte elektroniske stemmer, som er lagret på et lagringsmedium, som

inkluderer urnen eller et annet lagringsmedium for opptelling.

- En angriper får se hva den enkelte velger har stemt.
- Ved manuell eller maskinell telling av stemmer så endrer en utro valgmedarbeider stemmer.
- Tellemaskinen er korrumpert og teller galt
- En angriper kompromitterer e-stemmesystemet slik at det leverer uriktige lokale stemmeresultater.
- En angriper endrer summene av stemmene i et lokalt resultat når det legges inn i den sentrale oversikten.
- En utro medarbeider endrer summene av stemmene i et lokalt resultat når det legges inn i den sentrale oversikten.

### 10.1.2 Utilsiktede hendelser

- Stemmeloaleet blir utsatt for en alvorlig hendelse. Dette kan eksempelvis være brann, oversvømmelse, jordskjelv, strømbrudd, mangel på stemmesedler.
- Grunnet svikt i teknisk implementasjon eller rutiner, forsvinner det stemmer i løpet av prosessen.
- Valgmedarbeidere teller unøyaktig.

### 10.1.3 Uønskede tilstander

- Fremgangsmåten ved stemmegivning er så vanskelig å forstå at velger ikke får til å avgi stemme eller gjør noe som fører til at stemmen blir ugyldig.
- Fremgangsmåten ved registrering for stemmegiving er så vanskelig å forstå at velger ikke får registrert seg.
- Velger er funksjonshemmet. En barriere har som følge at velgeren ikke får stemt.
- Bare noen få eksperter forstår hvordan stemmesystemet fungerer.
- Det er ikke mulig å observere hva som skjer med stemmesedler og stemmer i prosessen.

oslo**economics**

*[www.osloeconomics.no](http://www.osloeconomics.no)*

E-post og telefon:  
[post@osloeconomics.no](mailto:post@osloeconomics.no)  
+47 21 99 28 00

Besøksadresse:  
Klingenberggata 7a  
0161 Oslo

Postadresse:  
Postboks 1562 Vika  
0118 Oslo