Knowledge acquisition on electronic and internet-based solutions for voting

Prepared on behalf of the Ministry of Local Government and Regional Development

osloeconomics

NR

About Oslo Economics

Oslo Economics provides reports on issues and advice to public authorities, organisations and companies. We understand the issues that exist where markets and politics meet.

We are a social analysis and advisory environment with experienced consultants with a background in public administration and various research and analysis environments. Oslo Economics currently has around 70 employees, more than 15 of whom have a doctorate. We offer insights based on technical expertise, sector experience and a network of co-operation partners.

About Norwegian Computing Centre

Norwegian Computing Centre was established in 1952 and is a private, independent organisation, which carries out commissioned research for companies and the public sector in Norwegian and international markets.

Norwegian Computing Centre is a leader in Norway within specific areas of information and communications technology. Norwegian Computing Centre's priority areas within ICT are digital security, digital inclusion and digital transformation. Norwegian Computing Centre's goal is to provide research findings that can be visibly applied.

Knowledge acquisition on electronic and internet-based solutions for voting/OE report 2022-118

Contact person:
Marit Svensgaard/Partner
msv@osloeconomics.no, tel. +47 982 63 985
Photo/illustration: iStock.com

Contents

Summary and conclusions

In recent years, a number of countries have introduced various forms of electronic voting for elections to elected bodies. This involves both electronic voting in polling stations (controlled surroundings), and voting over the internet in places other than polling stations (uncontrolled surroundings). In Norway, trials involving electronic voting over the internet were carried out in selected municipalities for municipal and county council elections in 2011 and the 2013 parliamentary election. Due to a lack of political unity, these trials were not taken further.

In 2017, an Election Act Commission was appointed to provide proposals for a new Election Act and to assess changes to the electoral system. In 2020, the Commission concluded that electronic voting solutions are not yet secure enough, and that further knowledge and experience acquisition on electronic voting was necessary. This report, produced by Oslo Economics and Norwegian Computing Centre, provides an updated knowledge base regarding the use of electronic voting in order to weigh up the opportunities, risks, benefits and costs against each other.

Framework for analysing electronic voting solutions

There are three main categories of voting systems: electronic, internet-based and paper-based systems. In what we have defined as electronic systems, voting takes place in a polling station using machines with and without an internet connection (controlled environment). In what we have defined as internet-based systems, voting takes place over the internet in places other than a polling station (uncontrolled surroundings).

The purpose of the report is to provide a basis for weighing up the opportunities, risks, benefits and costs of different systems against each other. For this purpose, we have developed an analysis framework based on the Council of Europe's recommendations on standards for e-voting. These recommendations provide countries wishing to introduce electronic or internet-based voting with some minimum standards to ensure that the principles for conducting democratic elections are observed.

The recommendations of the Council of Europe are made up of 49 criteria, grouped into eight categories. We have chosen the criteria that are most relevant for analysing the different voting systems and have also made some adjustments. This has resulted in a total of 13 criteria. We have sorted these into three main categories: *security*, *transparency and auditability*, and *usability and inclusion*. The recommendations of the Council of Europe are primarily designed for solutions for electronic voting. In our analysis, we have nevertheless included an assessment of paper-based solutions, represented by the current Norwegian electoral system. We did this in order to have a baseline for our assessment of electronic and internet-based systems.

There is great deal of variation between different technical solutions for electronic voting. When we assess electronic and internet-based systems regarding the criteria categories security, transparency and auditability, and usability and inclusion, we do so conceptually and not for specific technical solutions. Furthermore, in this analysis, we have assessed the conceptual voting system types in isolation and not examined using combinations of paper-based, electronic and/or internet-based systems in the election process.

Since it is the *concept* of electronic and internet-based voting that is being analysed and not specific solutions, our attention was focused more on the principles than the practicalities regarding the possibility of introduction of electronic voting. However, we have carried out an overall assessment of the resources needed at a local and central level if electronic or internet-based systems are to be introduced as a *supplement* to the current paper-based election process. The review shows that a partial introduction of electronic systems will be costly for both municipalities and the state. For municipalities, the costs come from the procurement and operation of voting machines. Internet-based solutions may reduce resource use in many areas for municipalities, though a larger proportion of the costs will be borne by the state. The solutions are demanding in terms of system development and security, something which affects the cost of materials, equipment, systems and staffing.

Analysis of the main categories of voting systems

Table A below outlines the categories, criteria and overall assessment outcomes that indicate whether a criterion is met to a limited, some, or a great extent. The assessments are interpreted as follows:

- **To a great extent:** There are no major challenges for the voting system, and the criteria are met to a great extent.
- **To some extent:** There are certain challenges for the voting system hindering the fulfilment of the criteria, but the challenges are not significant, or the solution allows for the fulfilment of the criteria in another way.
- **To a limited extent:** There are significant and/or insurmountable challenges for the voting system, which mean that the criteria are fulfilled to a limited extent.

The current paper-based electoral system in Norway comes out best in the **security assessment**. It is our assessment that the system meets almost all security criteria for an electoral system to a great extent. The only criterion the Norwegian system did not fulfil completely is the criterion regarding verifiability, even though verification is partially possible in the current electoral system.

Electronic systems come out weaker in the security assessment. The main reason for this is the risk that the election result could be manipulated through electronic systems, something which could have consequences for the election outcome. This risk is reflected in the criteria relating to election integrity and correctness. In electronic systems, there will also be a greater risk of someone gaining access to and publishing some of the election results in advance of official announcements. In this case, this would be in conflict with the criterion for the absence of influence.

Internet-based systems come out the worst in the security assessment. Internet-based systems have the same risk elements as electronic systems related to manipulation and advanced publication of election results. In addition, voting with internet-based systems takes place in uncontrolled surroundings, meaning it is much more challenging to verify that the right person is voting and that the vote is secret. These risk elements were observed in the criteria for authentication, anonymity and preventing of coercion. Finally, there is a systemic vulnerability in that internet-based systems are centralised systems. Only a few trusted employees are involved in vote management, something which makes the system more dependent on individuals than the current paper-based system. Under the current paper-based system in Norway, the votes are handled locally by local election workers. For a majority of electronic systems, vote counting is done locally.

The current paper-based electoral system in Norway also comes out best for the assessment of **transparency and auditability**. The main reason for this is that election observers can observe all stages of the voting process, and thus monitor that the election is in accordance with the pertaining rules. In electronic and internet-based systems, the stages, which are easily observable in a paper-based system, such as counting and checking votes, are more inaccessible to election observers; relevant data will be stored securely and can only be checked by election observers with specific technical competence.

As for the assessment of **usability and inclusion**, it is important to point out that *usability* can mean different things to different voter groups. Usability concerns both how and whether voters are able to use the solution, as well as the opportunities afforded by the solution through its use.

Our overall assessment is that paper-based systems, such as the Norwegian one, only meet the criteria for usability and inclusion to some extent. Paper-based systems are beneficial for voters with low technical competence. For blind or partially sighted voters, the solution is difficult to use, and for individuals within this group, the solution does not allow for unassisted voting.

Our overall assessment for electronic systems is that they also only meet the criteria for usability and inclusion to some extent. The advantage of these systems is that they open up opportunities for interactive solutions and allow for the use of aids for those users with special needs. This can lead to increased usability through clarifying for voters the options they have for voting, and it can prevent voters from making mistakes inadvertently. This can also allow for unassisted voting to a greater extent than paper-based systems such as the one Norway has today. The disadvantage of these systems is that they will be challenging to adopt for people with weak digital skills and can thus contribute to digital exclusion. There is also uncertainty about whether it is practically feasible to design solutions that allow for unassisted voting for all voters.

Our overall assessment is that internet-based systems also meet the criterion for usability to some extent, but meet the criterion for inclusion to great extent. Internet-based systems share many characteristics with electronic voting systems, but provide good physical accessibility, and have the potential to make unassisted voting a possibility for all voters.

Table A: Summary assessment of the voting systems*

	Paper-based systems	Electronic systems	Internet-based systems
Security			
Absence of influence – no provisional results shall be made public before voting has ended			
Authentication – potential voters shall be authenticated so that only eligible people may vote			
Anonymity – it should not be possible to find out who has voted for whom			
Prevention of coercion – it should not be possible to force a voter to vote in a certain way			
Election integrity – it should not be possible to change votes cast or the result of the vote			
Correctness – the votes must be correctly counted, and the result of the vote must be published correctly			
Verifiability – each voter can check that their cast vote has been counted, and anyone can verify that all valid votes have been counted			
Accessibility – the voting system must be accessible in accordance with the specified voting period			
Transparency and auditability			
Transparency – ability to check, observe, evaluate and verify			
Auditability – ability to audit the integrity of votes cast and that the results of the vote are protected			
Usability and inclusion			
Usability – the voting system shall be easy to understand and use for voters generally, voters with different technical competency and for voters voting abroad			
Inclusion of groups with special needs – the voting system shall be easy to understand and use for voters with special needs and make it possible for such voters to vote unassisted			

***Green indicates that the criterion has been met "to a great extent", blue indicates "to some extent", and red indicates "to a limited extent".**

Summary of opportunities, risks, benefits and costs

The analysis shows that none of the three main categories of voting systems are better than the two other systems across all factors. The current paper-based system is the only one to satisfy the criteria for anonymity, vote integrity, correctness, transparency and auditability to a great extent, while internet-based systems are the only ones to satisfy the criterion for inclusion of groups with special needs to a great extent. According to our assessment, the differences between the systems reflected in the analysis are not primarily the result of how far technological developments have come, or how the systems are currently designed. In the future, it will likely be challenging to meet the criterion for the inclusion of groups with special needs with the current paper-based electoral system, and it will not be possible to fully guarantee the security of using electronic and internet-based systems.

The fact that it is not possible to guarantee the security of electronic solutions entails a risk of a loss of trust. The Election Act Commission points out that if security around the election process is weakened, it will have very serious consequences for the election as a central democratic process, confidence in the election process and the election result. Weakened trust in the election process can arise even without an actual security breach. A mere doubt in a valid election result among parts of the population could impact the public trust in the election process. One option to ensure better accessibility for more people, while also limiting the risk of a loss of trust, is to offer electronic voting to only selected voter groups. Not because their vote is less important, but because a security breach will have lower economic and social costs in the form of reduced trust the fewer votes it affects.

There are variations between how a country's authorities and how its voters view electronic and internet-based voting systems. Weighing up between potential benefits related to usability and inclusion and the risk related to security depends to a large extent on country-specific conditions and conditions related to the existing electoral

system. Personal preference is also significant. Some people may be willing to accept the security risk inherent in using electronic systems in exchange for an election process that is better suited to voters with special needs. Others have the opposite opinion to this.

In summary, experiences from other countries shows that there are a range of opportunities when it comes to introducing electronic voting. The risk is primarily related to security, while the potential benefits lie in better inclusion of groups with special needs, and voters that are not in Norway during the election period.

1. Background, purpose and focus of the knowledge acquisition

Oslo Economics and Norwegian Computing Centre have carried out this knowledge acquisition on electronic voting on behalf of the Ministry of Local Government and Regional Development. The report has identified six main categories of voting systems and analysed these six systems based on the Council of Europe's criteria for the introduction of electronic voting.

1.1 Background and purpose

Norway is a democratic constitutional monarchy, and citizens elect representatives at the local, regional and national level. The election process in Norway is set out in the Act relating to parliamentary and local government elections (the Election Act). The Election Act aims to facilitate the populace being able to elect their representatives to municipal councils, county councils and the Starting through a free, direct and secret election. The Election Act aims to facilitate the populace to elect representatives to municipal councils, county councils and the parliament through a free, direct, and secret election.[1]

In Norway, elections are held using paper ballots, however trials involving electronic voting over the internet were carried out in selected municipalities during the 2011 municipal and county council elections and the 2013 parliamentary election. Electronic voting refers to solutions where voters cast their vote digitally. In 2014, the Ministry of Local Government and Modernisation decided that trials for voting over the internet should not be continued. There was a lack of political unity on the use of electronic voting, and political disunity related to the election process itself could be harmful for trust in the election (Kommunal- og moderniseringsdepartementet, 2014).

However, digital solutions, such as the electronic election management system, are used extensively by electoral authorities for municipal, county council, parliamentary and Sami elections. Variations of electronic elections have been held in Norway in relation to school elections, university management elections, and recently in relation to the referendum on whether Innlandet County should remain or be divided into Hedmark and Oppland. These elections were carried out without assistance from the central electoral authorities, but many advisory elections have used solutions that were developed in connection with the trials in 2011 and 2013.

In recent years, a number of countries have introduced various forms of electronic voting for elections to elected bodies. This involves both electronic voting in polling stations (controlled surroundings), and voting over the internet in places other than polling stations (uncontrolled surroundings). Examples of where electronic voting machines have been adopted include national elections in Brazil and India. Internet voting has been used for public elections in France, Estonia and Switzerland.

In 2017, an Election Act Commission was appointed to propose a new Election Act and assess changes to the electoral system (NOU 2020: 6). The Commission examined and assessed all aspects of the election process, including whether electronic voting solutions should be used in Norway. The Commission's conclusion was that the security of electronic voting was not good enough to be introduced in Norway at that time. The report was put out for public consultation in autumn 2020, and a majority of consultative bodies supported the Election Act Commission's assessment relating to the introduction of electronic voting. However, the Commission and a majority of the consultative bodies believed further knowledge and experience gathering was necessary relating to electronic voting in line with technological developments and the introduction of electronic voting solutions in other countries.

This report, prepared by Oslo Economics and Norwegian Computing Centre, will provide an updated knowledge base for the use of electronic voting. The purpose of the report is to provide a basis for comparing opportunities, risks, benefits and costs against each other.

The report covers electronic voting at polling stations using machines with or without an internet connection (controlled surroundings) and voting over the internet in places other than polling stations (uncontrolled surroundings).

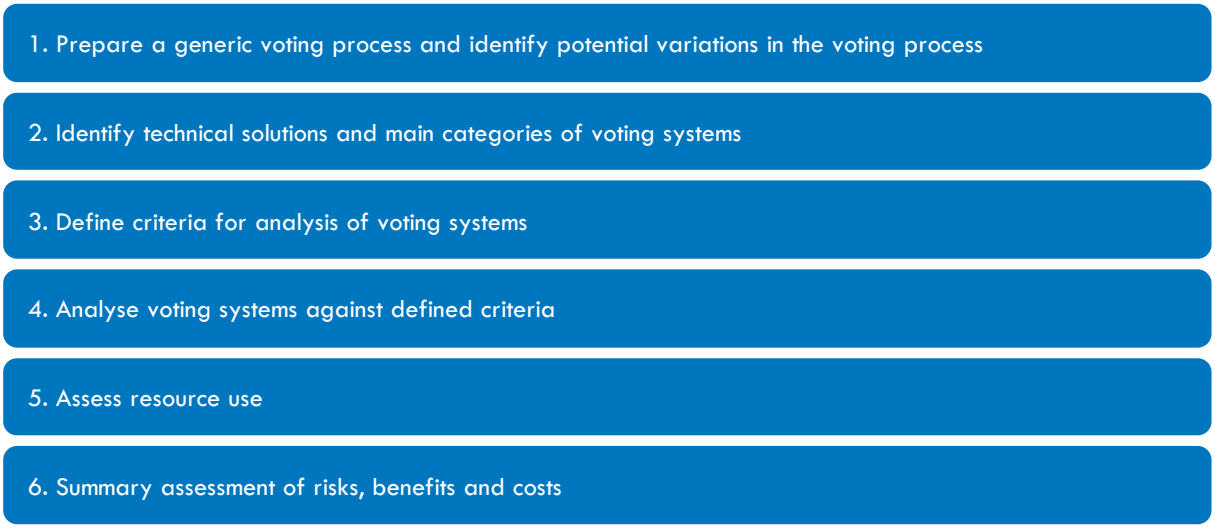
Solutions for electronic voting in controlled surroundings are referred to in the report as *electronic solutions*, while solutions for electronic voting in uncontrolled surroundings are referred to as *internet solutions*.

[1]The process for the Sami Parliament is not set out in the Election Act, but rather in the *Act on the Sami Parliament and other Sami legal matters*, and in the *Regulations relating to elections to the Sami Parliament*.

1.2 Method and implementation

The knowledge acquisition was carried out in six stages, as illustrated in Figure 1-1. The assessments are based on comprehensive literature studies, interviews with selected key people nationally and internationally, and discussions with a reference group made up of election experts.

Figure 1-1: The six stages of knowledge acquisition



Stage 1: Prepare a generic voting process and identify potential variations

The first step of the work has been to identify a way of classifying voting systems. We have done this by defining a generic voting process and the variations found in each stage of the voting process. The generic process consists of the following six stages:

1. The voter is registered to vote.
2. It is checked that the voter is on the electoral register and has the right to vote.
3. The voter casts their ballot in a ballot box.
4. The votes are counted and tabulated for each local precinct.
5. The collated results are summarised and published as the election result.
6. The voter verifies their vote (option).

Each stage has one or more choices for implementation. We have called these potential variations *dimensions*. An example of a dimension is *Location of the counting of votes*, which is related to stage 4. The alternatives put forward are either *local* or *central*. The stages of the voting process provide a framework for describing the structure and essence of different voting systems.

Stage 2: Identify technical solutions and main categories of voting systems

The next stage of the work has been to identify potential voting solutions and sort them according to the stage of the voting process and dimensions.

There are three main categories of voting systems: paper-based, electronic and internet-based systems. Based on the review of current solutions, we have defined two sub-groups for each main category: classic systems and end-to-end systems.

End-to-end systems allow for the verification of the *integrity* of the election result as a whole, as well as the voter's ability to check that their own vote is a step in achieving this. Election integrity means that it should not be possible to change cast votes or the result of the vote. This is discussed in more detail in Chapter 2.

Stage 3: Define criteria for analysis of voting systems

For the third stage, we developed an analysis framework that takes its basis in the recommendations of the Council of Europe (Europarådet, 2017). The recommendations of the Council of Europe consist of 49 criteria, grouped into eight categories, and provide countries wishing to introduce electronic or internet-based voting with some minimum standards to ensure that the principles for conducting democratic elections are observed.

We have chosen the criteria that are most relevant for analysing the different voting systems and have also made some adjustments. This has resulted in a total of 13 criteria, sorted into the three main categories of

- security
- transparency and auditability
- usability and inclusion

In addition to the categories that can be derived from the recommendations of the Council of Europe, we have included an assessment of the resource use as a separate category.

In addition to the criteria that can be derived from the recommendations of the Council of Europe, further principles have been derived for the Norwegian electoral system in particular. Based on the Constitution of Norway, Norway's international human rights obligations and the principles from the Venice Commission, the Election Act Commission derived the following principles for the Norwegian electoral system:

- The election must be free and fair.
- The election shall be secret.
- The election shall be direct.
- The right to vote shall be universal and equal.
- Elections shall be held periodically.
- Everyone with the right to vote shall have the opportunity to vote.
- Everyone with the right to vote shall be able to be elected.
- Every vote shall count equally.
- The electoral system shall ensure geographical representation.

Our main categories and criteria also contain the relevant principles from the Election Act Commission's report. This is discussed further in Chapter 4.

Stage 4: Analyse voting systems against defined criteria

In stage 4, we have analysed the three main categories of voting systems against our criteria for the choice of voting system. We then assessed each voting system in isolation and did not examine combinations of paper-based, electronic and/or internet-based systems in the election process.

The standards of the Council of Europe, which the criteria build upon, are primarily designed for solutions for electronic voting. In our analysis, we have nevertheless included an assessment of paper-based solutions, represented by the current Norwegian electoral system. We did this in order to have a reference for our assessment of electronic and internet-based systems.

There is great deal of variation between different technical solutions for electronic voting. When we assess the *security*, *transparency and auditability,* and *usability and inclusion* of electronic and internet-based systems, we do so conceptually and not for specific technical solutions. We make a distinction between whether the systems meet the criteria to a large, some or limited extent:

- **To a great extent:** There are no major challenges for the voting system, and the criteria are met to a great extent.
- **To some extent:** There are certain challenges for the voting system hindering the fulfilment of the criteria, but the challenges are not significant, or the solution allows for the fulfilment of the criteria in another way.
- **To a limited extent:** There are significant and/or insurmountable challenges for the voting system, which mean that the criteria are fulfilled to a limited extent.

Since it is the concepts of electronic and internet-based voting that is being analysed and not specific solutions, we have focused on conceptual aspects of electronic voting rather than the practical aspects. To illustrate the difference of the practice and the principle, we can start with an internet-based system. The practical/technical sides of designing a system for internet voting will influence whether a solution ensures voter anonymity to a greater or lesser extent. However, internet voting takes place under uncontrolled conditions and will, in principle, be different from paper voting when it comes to anonymity: Regardless of how the technical a solution for internet voting is designed, there is a greater potential risk for disclosure of votes (Saglie & Segaard, 2016).

Analysis of security

Security at elections, as defined in this context, means that the voters should be confident that the votes are not manipulated in any way, that the ballot is secret, that sensitive data is not disseminated and that all votes are counted as they are cast.

The analysis of *security* was carried out as a risk analysis. The basis for risk analyses is that "something can go wrong". We started the analysis by identifying potential events that may occur in each dimension of the voting process, and thus influence the security of the different voting systems. We make a distinction between intentional events, unintentional events and adverse situations (see Annex A).

The next stage was to define the *scope* of each dimensional value, and thus the scope of an event when something goes wrong. The scope has three levels: personal level, local level and central level. The variation between the levels can be illustrated through two examples:

- One dimension deals with how the voter is authenticated. This dimension has four possible choices: present identification to officials, use of electronic credentials, use of biometric authentication or no authentication. In this case, all four values are related to the *personal level*.

- A second dimension is whether the vote is to be cast at a local polling station. This dimension has two potential values: either yes, *locally at a polling station*, which comes under the scope of *local level*, or *no*, which means that the vote is cast in uncontrolled surroundings (for example postal votes and internet voting) and comes under the scope of *personal level*.

After having defined the scope, risk assessments were conducted. This include assessing consequences for possible negative events during the election process and probabilities that those events may occur. These have five levels each, as shown in the risk matrix. The risk matrix is adjusted slightly to provide a more nuanced spread of risk compared to the NIST 800-30 standard (Joint Task Force Transformation Initiative, 2012).

Finally, the scope and risk (probability and consequence) provide a score for each evaluation criterion. The principle is that for two different voting systems with the same assessed risk, but with different scopes, the voting system with criteria with a low scope will get a better score.

Figure 1-2: Risk matrix used in security assessments

Probability \ Consequence	Very little	Little	Medium	Large	Very large
Very high	L	M	H	VH	VH
High	L	M	H	VH	VH
Medium	VL	L	M	H	VH
Low	VL	L	M	H	H
Very low	VL	VL	VL	M	H

Illustration: Oslo Economics and Norwegian Computing Centre

Analysis of transparency and auditability, and usability and inclusion

Transparency and auditability deals with the fact that the electoral authorities, voters and independent election observers shall be able to observe the voting process, while *usability and inclusion* deals with the fact that there shall be a low barrier to voting, both for the average voter and for voters with special needs.

While we have conducted the security assessment by means of a risk assessment, for the analysis of *transparency and auditability* and *usability and inclusion*, we have carried out a qualitative assessment without a detailed report of the probability and consequences. The approach of the analysis of the two criteria is the same.

Stage 5: Assess resource use

Unlike the analyses of *security*, *transparency and auditability* and *usability and inclusion*, the analysis of *resource use* is not an analysis of voting systems against set criteria. Instead, we have taken our basis in the current electoral system in Norway, and assessed the implications it has for offering electronic or internet-based voting as a supplement to the current paper-based system. The conditions assessed were:

- materials, equipment and systems
- staffing and training
- premises
- information and guidance

In the assessment, we make a distinction between conditions for the initial introduction and ongoing operation, and we make a distinction between the conditions and costs at a local and national level.

Local level refers here to the municipal and county council level. In Norway, municipalities have practical responsibility for the execution of both municipal council elections, county council elections, Sami Parliament elections and parliamentary elections. The overall governmental responsibility for the election process lies with the Ministry of Local Government and Regional Development, while the Norwegian Directorate of Elections shall aid and support municipalities and county authorities in their practical execution of elections.

Stage 6: Summary assessment of risks, benefits and costs

The purpose of the knowledge acquisition is to provide updated knowledge about electronic voting in controlled and uncontrolled surroundings, and thereby create a basis for weighing the opportunities, risks, benefits and costs against each other. Based on the analyses, for the final stage, we have made a summary assessment of the risks, benefits and costs of introducing electronic voting.

1.3 Sources of information

The two information sources the report is primarily based on are

- document studies
- interviews

In addition, we have discussed the issues of the assignment on the way with a reference group of election experts. The information sources form the basis for both the overview and description of the technical solutions, country experiences, and assessment of the strengths and weaknesses of the different solutions.

Document studies

Document studies have formed the core of information gathering. For this part of the work, we took our starting point in the methodology described by Hart (2001). The three steps in the methodology are

1. look for relevant articles and reports using different combinations of relevant key words
2. extraction and systematisation of information from the articles and reports
3. quality assurance of the articles and reports. Below, we go into more detail as to what each of these stages involve

Interviews

As a supplement to the document studies, we have interviewed the following experts

- Kristian Gjøsteen, the Norwegian University of Science and Technology (NTNU)
- Audun Jøsang, the University of Oslo (UiO)
- Stephane Adamiste, researcher (Switzerland)
- Carsten Schürmann, researcher (Denmark)
- Mihkel Solvak, researcher (Estonia)
- Cato Lie, the Norwegian Federation of Organisations of Disabled People
- Sverre Fuglerud and Terje André Olsen, the Norwegian Association of the Blind and Partially Sighted

The interviews were conducted as semi-structured interviews. This means that the topics and questions vary naturally between the different interviewees, and that the issues and topics in the interview guide acted only as guides, so that all relevant issues, topic areas and questions were covered during the interviews.

Reference group

The reference group is made up of

- Signe Bock Segaard, researcher at the Norwegian Institute for Social Research (ISF)
- Jo Saglie, researcher at ISF
- Dag Arne Christensen, researcher at Norce

During the project period, we had two meetings with the reference group: the first was to discuss the focus of the assignment, and the other was to discuss our preliminary findings.

1.4 Structure of the report

Chapter 2 describes the generic voting process used to classify voting systems, while Chapter 3 uses the voting process to define and describe six solutions for voting based on experiences from Norway and other countries.

Chapter 4 describes the criteria used in the analysis of the voting systems, before Chapters 5, 6 and 7 present the analyses of *security*, *transparency and auditability*, and *usability and inclusion*.

Chapter 8 discusses the human and financial resources required for the introduction of electronic and internet-based voting systems as a supplement to the current paper-based election process, before Chapter 9 provides a summary assessment of the opportunities, risks, benefits and costs related to the different voting systems.

2. The voting process

At a general level, voting systems have the same voting process It begins with checking that the voter has the right to vote, followed by the voter casting their vote, and ends with the votes being counted and published in the determination of the election result. What differentiates voting systems from each other is how the stages in the voting process are carried out. In this chapter, we define a generic voting process, provide an introductory description of the potential variations of the voting process and discuss the significance of cryptography.

2.1 The stages and dimensions of a voting process

We have defined a generic model for a voting process (Figure 2-1). The voting process itself has six stages, and each stage can be implemented in a range of different ways. We call these *dimensions* in the voting process. The model allows us to define each concrete voting system as a combination of how the system responds to different dimensions, and thus we can understand the structure and essence of various voting systems. This provides a basis for describing and analysing different systems in a systematic and comparable way.

We differentiate between centralised and decentralised voting solutions. This distinction is the basis for many of the dimensions mentioned and is of crucial significance for how we assess a given electoral system. The current Norwegian electoral system is an example of a decentralised voting solution. Here, the voter casts their vote locally at a polling station, which involves a decentralised location for the ballot box. A centralised voting solution is when there is only one ballot box for the entire election, which for a national election means that the solution must be internet-based.

Figure 2-1: The stages and dimensions of a voting process

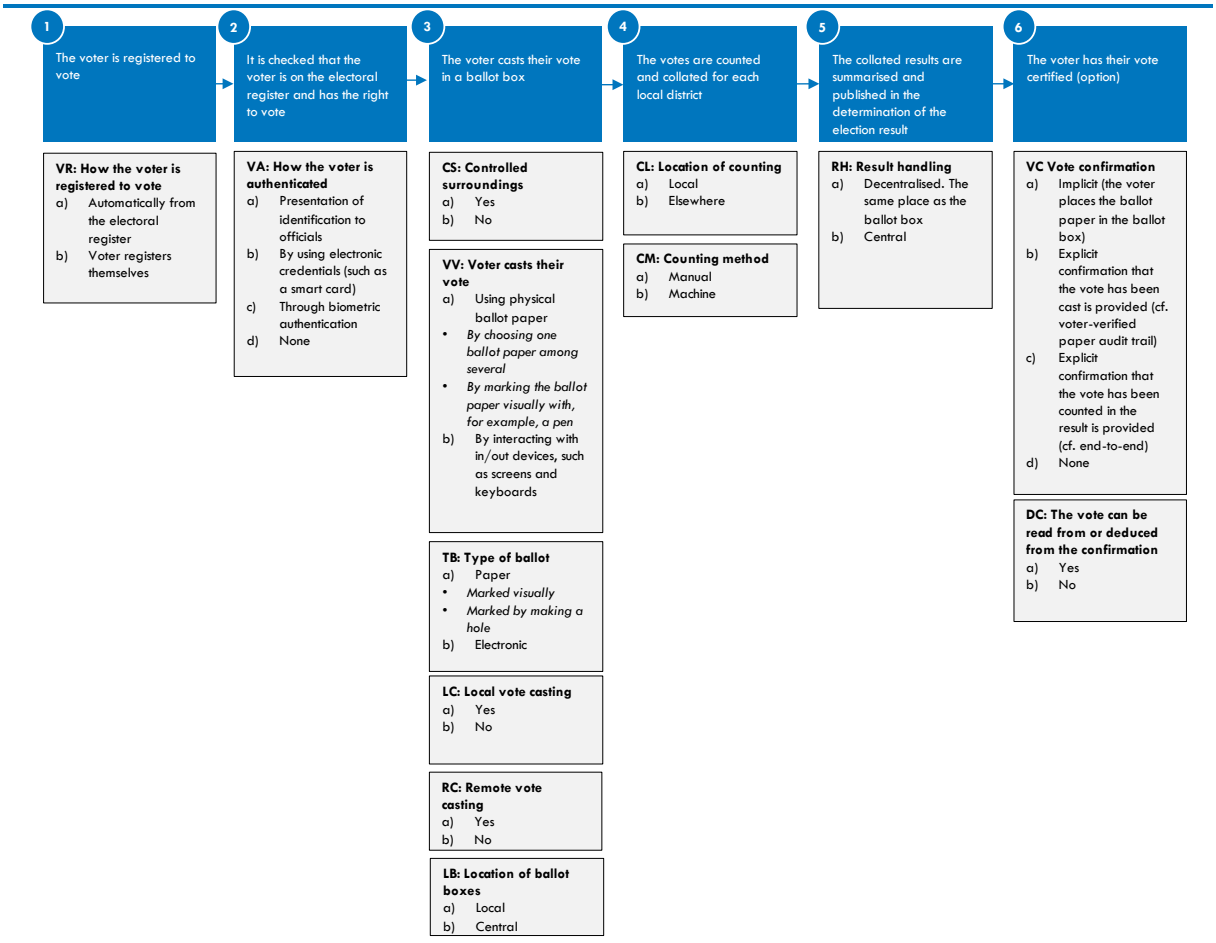


Illustration: Oslo Economics and Norwegian Computing Centre

2.2 Registration of votes

VR: How the voter is registered to vote

a) Automatically from the electoral register (as in Norway)

b) The voter registers themselves (for example, in the USA)

VR: Registration of voters can primarily occur in two ways, either automatically from a form of register such as the electoral register we have in Norway today, or by the voter having to register themselves, such as for Sami Parliament elections in Norway, for example, and for elections at local, state and federal levels in the USA (USA.gov, 2022).

The electoral register, which decides who can vote in Norway, is transferred to election management system from the Norwegian Directorate of Taxes. The electoral register has many purposes. It ensures that only those with the right to vote are able to cast a vote, and moreover provides oversight of which constituency the eligible voters belong to and thus where the vote is to be cast or sent to for counting.

2.3 Checking the voter's identity

VA: How the voter is authenticated

a) Presentation of identification to election officials

b) By using electronic credentials (such as a smart card, BankID)

c) Through biometric authentication

d) None (for postal votes)

VA: Authenticating voters is a mechanism for proving an alleged identity, i.e. that someone is the person they claim to be (Kommunal- og regionaldepartementet, 2006).

In principle, authentication is done based on something the voter *has*, *knows* or *is*. Presenting identification to election clerks and using electronic credentials refer to something the voter has. In addition, electronic credentials will also use something voters know, such as a password when using BankID. Biometric authentication is an example of authentication through something the voter is. Biometric properties may be someone's face, fingerprint, iris, voice or similar.

2.4 The voter casts their vote

The stage at which the voter casts their vote in a ballot box can be further resolved through the three stages

- the voter selects their vote
- it is registered in the electoral register that the voter has cast their vote
- the voter receives a receipt for their vote (option)

CS: Controlled surroundings

a) Yes

b) No

CS: The difference between controlled and uncontrolled surroundings is a difference between whether the voting occurs at a polling station under the control of election officials, or in uncontrolled conditions outside of polling stations.

Whether there are controlled or uncontrolled surroundings affects a number of central aspects such as authentication of voters, resource use in municipalities, and moreover the registration, transfer and counting of the votes.

VV: How voters cast their vote

a) Physical ballot paper

   i. By choosing one ballot paper among several

   ii. By marking the ballot paper visually with, for example, a pen

b) By interacting with input/output devices, such as screens and keyboards

VV: In voting systems based on paper ballots, the voter can cast their vote by choosing one paper ballot among several, or by marking visually with, for example, a pen.

Electronic solutions may employ touch screens or standard computer equipment such as regular personal computers, where the voter uses a keyboard and mouse to carry out the act of voting.

TB: Types of ballots and ballot boxes

a) Paper
   i. Marked visually
   ii. Marked by making a hole
b) Electronic

TB: Type of ballot refers to the format in which the vote is cast. An appropriate difference in this context is between votes in paper format and votes that are represented electronically. In paper format, votes can either be marked with a pen (visually) or by stamping a hole in given area.

LC: Local vote casting

a) Yes
b) No

LC: When voting in controlled surroundings, the casting of the vote is in the same place as the ballot box.

RC: Remote vote casting

c) Yes
d) No

RC: By casting a vote in uncontrolled surroundings, the voting location will be different to that of the ballot box. This will be the case for postal votes and internet-based voting.

LB: Location of the ballot box: *centralisation versus decentralisation*

e) Decentralised
f) Central

LB: With the current paper-based system in Norway for municipal, county council and parliamentary elections, votes will either be cast or sent to a ballot box at the precinct where the voter is registered in the electoral register. This means that the ballot boxes are decentralised. On the other hand, for example for internet-based voting in uncontrolled surroundings, it is possible to have a centralised ballot box.

2.5 Counting of the votes

CL: Location of the counting of votes (handling and transport of votes)

a) The same place as the ballot box
b) Elsewhere

CL: The location of the counting of the votes can be the same place as that of the ballot box, something which means that the counting is decentralised. On the other hand, the counting can be done at a different place than where the voting took place. In such circumstances, it is clear that the count is centralised in one or more locations.

CM: Counting method

a) Manual
b) Machine

CM: Counting votes can either be done manually or using machines. Manual counting means that election officials manually assess the validity of ballot papers, before they are counted.

Machine-based counting tends to be done using an optical reader that reads the printed and written marks, including bar codes, from paper and converts these data to bit patterns. In Norway, EVA scanning is used by municipalities and county authorities who want to read the ballots mechanically.

Electronic voting systems allow for electronic counting. As long as the computers are correctly programmed, the opportunity for manual errors in the counting are almost non-existent.

2.6 Publishing the results

RH: Result handling

a) Decentralised
b) Central

RH: If the location of the counting of votes is decentralised, the result must then be transmitted to a centralised location or authority. We refer to this process as decentralised result handling. Cases where it is not necessary to pass on results from a local to a central site are referred to as centralised result handling.

2.7 The voter has their vote certified (option)

VC: Vote confirmation

a) Implicit (the voter places the ballot paper in the ballot box)

b) Explicit confirmation that the vote has been cast is provided (cf. voter-verified paper audit trail)

c) Explicit confirmation that the vote has been counted in the result is provided (cf. end-to-end)

d) None

VC: For paper-based systems, such as the Norwegian system, there is no form of explicit confirmation that a result has been cast or counted in the election result. However, even though there is no explicit confirmation, many paper-based systems have a form of implicit confirmation that the vote has been cast by the fact that the voter sees that their ballot paper is placed into the ballot box or they place it in there themselves.

A method to provide verification that a cost has been cast is referred to in the literature as voter-verified paper audit trail (VVPAT). VVPAT is a method for providing confirmation that a vote has been counted using electronic, ballot paper-less systems.[2] With VVPAT, a receipt is printed out for the voter, providing them with confirmation of how they voted. However, this receipt does *not* provide the voter with confirmation that the cast vote has been included in the election result. To achieve this, a system known as "end-to-end auditable" or "end-to-end verifiable" can be used.

Confirmation for the voter that the vote has been counted is valuable in that it can ensure the integrity of the election result. Election integrity means that it should not be possible to change votes cast or the result of the vote. The main purpose of end-to-end verification is to ensure the integrity of the election result as a whole, and the voter's ability to check that their own vote is a step in achieving this. It is sufficient that a small percentage of voters check their votes in order to be sufficiently sure of the integrity of the system as a whole (Benaloh et al., 2014).

End-to-end verification covers two principal components:

- Each voter can check that their selected vote has been counted.
- Anyone can verify that all valid votes have been counted.

This is in line with Benaloh et al. (2014), and the two principles can be achieved in three phases:

1. Cast as intended – the voter's will shall be freely expressed
   - The voter casts their vote, and at the time of casting they can receive plausible confirmation that their encrypted vote reflects their choice.
2. Included as cast
   - The voter can check that their encrypted vote has been correctly included. This can be done by the voter finding their encrypted vote on a public list of encrypted, cast votes.
3. Counted as included
   - Anyone can check that all published, encrypted votes are included in the count without knowing how any specific person has voted.

Common to the different solutions for this system is that the count takes place with a cryptographic voting protocol, even if the vote has been cast on paper (see Chapter 2.8 for more information on cryptography).

Different end-to-end solutions have different ways of implementing their tasks. Below, we describe what an end-to-end system might look like.

Using a cryptographic secret mask, a vote can be disguised. This can provide a confirmation that the vote has been cast as intended, as any party can subsequently unmask the votes in a universally verifiable manner. An adversary can force a voter to reveal the masked vote. However, voters can generate fake mask transcripts for any possible mask such that the masked vote is consistent with any fake vote, thus providing prevention of coercion.

There are various technical solutions to assure the voter that the vote has been cast as intended. A frequently used solution is to allow voters to produce as many encrypted ballots as they want, but where the voter only casts one vote. This means that the voter marks their vote before the electronic solution (the machine) creates an encrypted version of the vote without casting it. Instead of casting the vote, the solution will ask the voter whether they want to cast the vote or "challenge" it. If the voter trusts that the machine copy of the vote reflects the intended vote, the voter can choose to cast the vote with the encrypted version of

[2] VVPAT is not possible under internet-based systems as it is dependent on dedicated machines with a paper strip that can be checked after the voting has ended.

the vote. In cases where the voter does not trust in the machine, the voter can challenge it. In such cases, the solution will provide data that allows the voter or an outside party to check that the masked copy actually generates the intended vote. This can be done, for example, by using a public data encryption algorithm. The central characteristic of this method is that the machine binds itself to a given encryption of the vote before the voter decides whether the vote shall be cast. The voter can carry out this process until they trust that the solution is casting the vote as intended (Benaloh et al., 2014).

Once the voting period has ended, the system publishes all the masked copies of the votes on an electronic notice board, which may be a website. Publication means that the voter can see that the vote has been included and is unchanged – it is as it was cast.

In the final stage, all published, encrypted votes will go through cryptographic protocols and create the election result. Here, anyone can check that all published, encrypted votes are included in the count without knowing how any specific person has voted.

DC: The vote can be read from or deduced from the confirmation

a) Yes

b) No

DC: This concerns how any confirmation of the vote is represented to the user, something which is highly significant to the system's endurance against pressure and coercion. The confirmation can be represented in two fundamentally different ways. One is the user being able to read their vote directly from the confirmation or indirectly deduce this, for example by checking a code sheet sent out to users. The other is that the user can only check that their ballot paper has been included in the result, and not that it reveals the vote that has been cast.

2.8 Cryptography in voting systems

Security is fundamental to all electronic and internet-based voting systems, and it is a central premise that a range of well-defined security requirements are in place when designing such systems. Cryptographic methods are central to ICT-based security solutions.

Cryptographic methods are mathematical methods used to "secure" information, but have nothing to do with software security and vulnerability of computer programmes and computer systems.

Cryptographic methods apply to data that are sent over networks (in transport) and that are stored.

The most common security properties for encryption are

- confidentiality protection – protection against information being revealed to unauthorised parties.
- integrity protection – protection against manipulation of the system or changes to the data
- authenticity protection – protecting the source of the information

The most basic types of cryptographic methods are encryption and decryption to ensure confidentiality protection, and digital signatures (signing and signature verification) to ensure integrity protection and verifiability in the form of data authentication.

Encryption is done by converting a text (or bit pattern) into a cipher text that is incomprehensible, which can only be decrypted using the pertaining encryption key. Encryption and decryption keys are special bit patterns that are necessary for carrying out encryption and decryption.

The purpose of a digital signature is to link a person (or a computing device) to some information or data. The signature confirms that the information originates from the signer and has not been altered. By verifying the signed data against the signature and the person's public key, so it is possible to establish that the person in question has signed. Digital signatures also provide integrity protection in the form of an integrity check, because if the data were changed in retrospect, either due to a deliberate attack or an unintentional error during the data transfer, then the verification will fail.

2.8.1 Anonymity protocols

A basic problem of communication in the data network from a data protection perspective is that all such communication will be traceable. A central condition of voting systems is that the vote must be cast in an anonymous manner[3] so that it cannot be linked to a specific voter. In other words, this is the opposite of the data authentication mentioned above.

So-called mix nets are anonymity protocols that require a chain with multiple so-called proxy servers and the use of public key encryption. A proxy server is a trusted computer, which must not be controlled by a stakeholder, i.e. they must be controlled by trusted

[3] Anonymity is a security requirement for electronic and internet-based systems. We present the background and content of this requirement in Chapter 4.

and independent parties. Each sender encrypts their message on each proxy server (by using the public key for each server), so that the final encrypted message consists of the same number of encryptions – layer on layer like an onion (the message length is the same). Each sender sends their encrypted text to the first proxy server. Each proxy server waits until it has received a sufficient number of encrypted texts, decrypts (and thus removes the layer of encryption), and sends the encrypted text on in a random order to the next proxy server. In this way, it will not be possible for the subsequent proxy servers or the final recipient to link the messages to the original sender, unless all proxy servers bar one are compromised or collaborators. By compromised we mean that a trusted entity (computer or party) is no longer neutral and independent, and is used by another party whose aims involve one or more security criteria being breached.

2.8.2 Conditions for using cryptographic voting protocols

The use of cryptography in a voting system crosses the stages in a voting process and the dimensions. Cryptographic methods can be used in electronic and internet-based voting systems to ensure the most important security requirements. It is unclear how many electronic and internet-based voting systems actually use cryptographic voting protocols, however, encryption and cryptographic signing of votes is common. This does not provide any anonymity in and of itself, but assumes that there is a trusted party (election workers) handling the encrypted votes confidentially.

The necessity of trusted parties is a basic premise for all cryptographic security solutions. In a centralised system, this can be a major weakness since only one dishonest individual can be enough to compromise central parts of the system or the system in its entirety. The same is the case in the event of a serious incident or an attack. In a decentralised system where an incident only has a local impact, the consequences will far lesser.

Another basic premise for all crypto-solutions is that key management is secure. This assumes that secure hardware components are used (which makes it impossible to recreate or compromise crypto keys), stored securely to prevent compromise (due to a threat actor or that they otherwise go astray), and that crypto operations are carried out securely.

2.8.3 Specific information on the use of blockchain technology

Electronic and internet-based solutions use blockchain technology[4]. Blockchain technology makes it possible to maintain a decentralised transaction log that can be updated and verified by all parties, and which cannot be falsified by any party. It is thus possible to create consensus on a historical account, even though no party has control over the entire system. It is these properties that allow for cryptocurrencies such as Bitcoin, and they have also meant that blockchain technology has become seen as a promising mechanism for carrying out electronic elections by using a blockchain as an electronic ballot box. A more thorough analysis shows, however, that the use of blockchain technology for this purpose can create more problems than it solves (Park et al., 2021). It is difficult to run blockchains, they introduce an extra layer of complexity for the solution, updating software requires more time and effort, and it is difficult to implement it correctly. On the other hand, they do not resolve problems related to secrecy, verifiability, or manipulation of equipment used for voting.

[4] An example for this Vocdoni, presented in sub-chapter 3.3

3. Potential solutions for voting

There are three main categories of voting systems: paper-based, electronic and internet-based; however, there are significant differences between these categories. In this Chapter, we use the dimensions of a voting process to define six solutions for voting, and we provide a description of the six solutions based on experiences from Norway and other countries.

3.1 Categorising solutions

The dimensions of a voting process, presented in Chapter 2, provides the basis for systematising systems or technologies into three main categories of voting systems – paper-based, electronic and internet-based systems. We divide these three categories into two further subcategories – classic or end-to-end systems.

Within these categories, there may be individual variations, and there may also be hybrids between categories, but they have shared traits that mean that we believe it relevant to group them together. Table 3-1shows how different systems or technologies implement the different dimensions, as described in Chapter 2. Letters *a*, *b*, *c* or *d* refer to how the dimensions are responded to. For example, the letter *a* under VR refers to "Automatically from the electoral register". We also provide a description of each category, supplemented with concrete examples of the systems and technologies.

Table 3-1: Categorisation of potential solutions for voting

Class	System or technology	Country	VR	VA	CS	VV	RV	LC	RC	LB	CL	CM	RH	VC	DC
Classic paper-based	The Norwegian system – election day	NO	a	a	a	a	a	a	b	a	a(b)	(a)b	a	a	-
	The Norwegian system – advance votes	NO	a	a	a	a	a	a	b	a	b	(a)b	a	a	-
	The Norwegian system – postal votes	NO	a	d	b	a	a	b	a	b	b	(a)b	a	a	-
End-to-end paper-based	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
Classic electronic	2003 Norwegian trial	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	-
End-to-end electronic	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
Classic internet-based	2011 and 2013 Norwegian trials	NO	a	b	b	b	b	b	a	b	b	b	b	b	a
	The Estonian system	EE		b	b	b	b	b	a	b	b	b	b	b	a
End-to-end internet-based	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

Source: Oslo Economics and Norwegian Computing Centre. Note: A dash indicates that it is not a relevant field, while a blank field indicates that it is unknown.

3.2 Paper-based systems

Paper-based systems are a widespread and well-tested means of voting. Most comparable countries to Norway use a paper-based system. All these systems are variants on classic, paper-based systems. There are no countries that use end-to-end paper-based systems at national, legislative elections.

3.2.1 Classic paper-based systems

In classic paper-based systems, voting generally takes place under controlled circumstances, but it can be easily adapted for use in uncontrolled circumstances through postal votes. The systems are characterised by the voter selecting their vote on a physical ballot paper and places the ballot paper in a ballot box. The voter receives an implicit confirmation of a vote cast by the fact that the vote is placed into the ballot box, but receives no form of confirmation beyond this that the vote has been included in the count or counted as cast. Votes can be cast manually, with a machine or with both.

The current Norwegian electoral system is a classic paper-based system. In the Norwegian system, voters are registered automatically. This is in contrast to, for example, the election process in the USA and in Sami parliamentary elections in Norway, where voters are required to register to vote. In Norway, polling cards

are sent out to everyone, though it is not necessary to have a polling card in order to vote.

When it comes to voting in person, this is primarily based on ballot papers being placed in ballot boxes under controlled conditions. This can happen either on **election day** or by **early voting** in a polling booth. It is also possible to vote at home for people who cannot vote in advance in the normal way as a result of an illness or disability. This is called ambulatory voting. For votes cast in a polling booth during the early voting period, ballot papers must be transported and stored until they are counted. Counting early votes can start the day before election day (Valgmedarbeiderportalen, 2022).

When a voter wanting to vote during the early voting period is registered in the electoral register in a different municipality, the vote is not placed in a ballot box. The ballot paper is placed in a ballot paper envelope, which in turn is placed in a cover envelope with voter identification. This is sent in a forwarding envelope to the municipality where the voter is registered in the electoral register. Ballot paper envelopes can also be used on election day itself. This could be in municipalities that do not have an electronic electoral register, voting in specific envelopes such as when the returning officers cannot find a voter in the electoral register or they are already crossed off, or as an emergency procedure, i.e. during a power outage or interruption of communication with the electoral register.

Otherwise, it is also possible for voters living abroad to use a **postal vote**. For this purpose, the same system of envelopes is used, but this is done only by the voter themselves under non-controlled circumstances, and thus without authentication. This alternative, including the approaches, is defined in the Election Act (*Lov om valg til Stortinget, fylkesting og kommunestyrer (valgloven)*, 2022) and applicable regulations (*Forskrift om valg til Stortinget, fylkesting og kommunestyrer (valgforskriften)*, 2022). The alternatives are supported by the electronic election management system used by municipalities and county authorities, called EVA. This is a support tool municipalities use in the various phases of the election process.

All municipalities and county authorities use EVA in the election process, though the use of EVA is not statutory, and it is therefore not mandatory for municipalities and county authorities to use the system. It is also not mandatory for the municipalities to use the tools the Norwegian Directorate of Elections offers. This means that the municipalities and the county authorities can choose to use alternative systems to conduct elections. However, no municipalities or county authorities have chosen not to use EVA (NOU 2020: 6). EVA Admin is the main application for the election process. It contains information about registered voters and is used to register votes cast by the voter. EVA Scanning is used by municipalities and county authorities who want to read the current paper-based ballots mechanically rather than counting manually.

By voting in a polling station, either on election day or during the early voting period, the voter must provide proof of identity to election officials. There are no formal requirements for identification beyond name, date of birth and a photo. This is different from early voting with a postal vote where the voter does not provide proof of identity. This alternative is only permitted for voting from abroad and, as a whole, postal votes constitute an extremely small proportion of votes.

On election day and for early voting in the voter's own municipality, there are ballot papers for all parties participating in the election inside the polling booth. The voter takes a ballot paper for the relevant party that the voter wants to cast their vote for. The voter may potentially cast a personal vote by changing the ballot paper. The voter then takes the ballot paper with them outside of the booth and gives it to the returning officer who stamps the paper before the voter places it in the ballot box. The voter is crossed off as having cast their vote.

There is a general ballot paper with braille printed on it for visually impaired voters. For the general ballot paper, the parties are listed in alphabetical order. There is a box in front of the party's name in which the voter places a cross. There is also guidance in braille and large print. On this type of ballot paper, it is not possible to change the candidates of the individual party's lists (Norges Blindeforbund, 2021). Not all municipalities use the general ballot paper (Saglie et al., 2022). There are no requirements in the Election Regulations that general ballot papers should be used. Section 26 of the Election Regulations states that "Blind and partially sighted voters shall be able to vote without having to request assistance".

Once the ballot paper is placed in the ballot box or the ballot paper envelope, the voter receives an implicit receipt in the form of the voter having received an oral explanation of what is happening. However, the voter does not receive any form of confirmation that the vote has actually be counted, and that it has been included in the final election result.

When a ballot paper and cover envelope are used, the election official, who will eventually open the envelopes, checks the information on the cover envelope against the electoral register and crosses off that the voter has voted. Then, the election official opens the ballot paper envelope and takes out the ballot paper. The opening of the two envelopes must

be done so that the election official cannot know how the voter has voted.

Municipalities count early votes and votes cast on election day separately. All the ballots must be counted at least twice in the municipality. At county council elections and parliamentary elections, ballots are also counted by county authorities. In the counting phase, EVA is used to approve the counts, reject ballots, report results to the media and keep track of the counting process in the municipality. When municipalities count manually, the data from the count is entered manually into EVA. For machine counting, the results are entered into the system using EVA scanning. The first count of the ballots is called the provisional count and will be done manually by all municipalities. The municipalities can choose whether to make the final count manually or using scanners (NOU 2020: 6). There is guidance for security measures for the use of EVA scanning, but there is otherwise no special security requirements for machines that are used for optical reading and EVA scanning (Valgdirektoratet, 2021).

3.2.2 End-to-end paper-based systems

On the surface, end-to-end paper-based systems resemble classic paper-based systems, but they are based on cryptographic voting protocols. This means that the voter can receive confirmation that the vote has been included in the final result (end-to-end verifiability). The voter verifies that the vote has been counted in the result through publicly available information

It is not known whether End-to-end paper-based systems have been used at large scale, but the Scantegrity II system has been tested at a small scale (Carback et al., 2010). The Norwegian electoral system, for example, is too complex to use an end-to-end paper-based system. Due to practical limitations of the technology, end-to-end paper-based systems are limited to placing a cross on a common ballot paper. Therefore, there is no such system that can be used for an election where both a vote is cast for a party and modified ranking of candidates within a party can be made, such as in the Norwegian system, for example.

When it comes to the implementation of end-to-end paper-based systems, there will be largely similar considerations as for classic paper-based systems. Authentication, and transport and storage of votes, can be resolved with varying levels of quality and security.

Examples of end-to-end paper-based systems include Scantegrity II, PunchScan, Prêt à Voter, ThreeBallot and Scratch and Vote. Common to these voting systems is that they are cryptographic voting systems based on paper ballots, but they are counted electronically.

Scantegrity II (Chaum et al., 2008) is, as mentioned, a system that has been tested on a small scale. The system was proposed in 2008 by David Chaum, Peter Ryan, Ronald Rivest and several other researchers. Scantegrity II is compatible with existing, classic paper-based voting systems, where the voter votes by marking a ballot paper optically, and it can be used to enhance such systems with end-to-end verifiability. This does not require the modification of optical scanning equipment used for classic paper-based voting, but it does require the use of different types of ballot papers than those used for such elections.

After authentication and authorisation, the voter is handed a ballot paper with a unique number and a special pen. The voter then votes using the pen to mark a "bubble" next to the relevant option. This reveals a code written in invisible ink in the bubble, and this code can be copied over to a receipt, which is torn off and which also contains the unique number. Once voting has finished, the verification code is published for each unique number, and the voter can verify that this corresponds with the code that was noted on the receipt.

Scantegrity II was tested at the local elections in Tacoma Park, Maryland in 2009. The city has 11,000 registered voters, and 1,728 of these voted using Scantegrity II (Carback et al., 2010). In this context, a customisation for remote vote casting was tested, called Remotegrity.

The system **PunchScan** is issued as an open source code and was developed by the University of Ottawa, based on an original suggestion from David Chaum in 2005.

The system uses ballot papers consisting of two sheets stuck together. On the bottom sheet, letters appear in a random order. On the upper sheet, the candidates are associated with letters, also in a random order. In addition, the ballot paper has holes that are placed so that the letters on the bottom sheet can be seen through the holes. Both sheets are provided with the same, unique ID number.

The voter uses a coloured ink to mark their chosen option, so that the ink covers both the top and the bottom sheets. When the sheets are separated, neither of them has enough information for an outsider to find out what the vote was. The voter chooses one of these sheets and places it in the ballot box or scans it. In the counting system, there is information that links each ID number to an order of candidates and letters on each sheet, and thus it can work out what the vote was. All ballot papers are published, for example in a newspaper or a website, so that the voter can verify

their vote, but that an outsider cannot find out how the person in question has voted.

Prêt à Voter (Ryan et al., 2009), **ThreeBallot** (Rivest, 2006), **Scratch and Vote** (Adida & Rivest, 2006) are all examples of end-to-end paper-based systems that were developed in the 2000s. The systems have their own unique characteristics in their design, but respond to dimensions in the stages of the voting process in similar ways.

3.3 Electronic systems

For electronic systems, voting still takes place in controlled surroundings, but the ballot boxes and ballot papers are replaced with electronic storage and an electronic representation of the votes, respectively. In practice for voters, this system means that voting takes place in polling stations with regular or customized computers. In the literature, this type of system is known as Direct-Recording Electronic (DRE).

3.3.1 Classic electronic systems

In classic electronic systems, the voter casts their vote by interacting with in/out devices on a computer. After the vote has been cast, the vote is stored in local electronic storage. This can either be encrypted or plain text. The further transfer for the counting system can also either be encrypted or in plain text.

Authentication in electronic systems has similarities with authentication in paper-based systems, as both systems deal with controlled circumstances. For electronic systems, authentication can be carried out with varying levels of quality and safety. Authorisation to vote can be given by the voter being supplied either a one-time code or a smart card that is used to activate the voting machine.

Voting machines have the quality that they can be adjusted to a large extent to or used with aids for voters with disabilities. Partially sighted voters have a desire to use aids and adapted solutions that can improve the voting process (NOU 2020: 6).

The Norwegian trial in 2003, and the use of voting machines in a number of countries are examples of classic electronic systems.

The Norwegian trial in 2003 was a trial using electronic voting for municipal and county council elections in the Oppdal, Bykle and Larvik municipalities and for the county council election in Longyearbyen (Christensen et al., 2004). The trial covered around 11,000 eligible voters, who were able to vote electronically. The technical solution that supplied by the company ErgoEphorma was computers with touchscreens and equipment for reading smart cards. The assessment of the trial was primarily an assessment of the usability and its general implementation, where voters reactions in particular were key. The technical solution was not assessed. The assessment concluded that there was good usability, but that the solution could be better adjusted to the needs of people with disabilities. This applied in particular to the partially sighted.

The solution worked in a way that the voters received a smart card when checking off the electoral register and used this to identify themselves on the voting machine. After voting has finished, the votes are transferred from the voting machine over the internet to a central server where they are counted.

There are a range of voting machines used in different countries. They share many of the same qualities, and we call attention to some examples of solutions used and experiences of using them.

NEDAP/Groenendaal ES3B (Gonggrijp & Hengeveld, 2007) is an example of an electronic system. The machine has been used for electronic voting in the Netherlands. NEDAP manufactures the machine, while Groenendaal develops the software on the machines. The voter interacts with the machine to cast their vote, which is stored in a memory module. When the solution was used in the Netherlands, counting of the votes took place in each precinct by the results from the machines being added up and put together with manual votes.

The Netherlands used electronic voting machines in many elections up to 2008. The machines were placed in polling stations, i.e. controlled surroundings. A number of incidents led to the use of the machines eventually being phased out. Among other things, the machines made a sound that made it possible for other in the polling station to identify who the voter had voted for. In addition, there were challenges in the form of voters not understanding whether or not they had voted. This led, among other things, to an election worker in a polling station going in after a voter thought they had voted and changed their vote. An activist group procured a voting machine and showed that it was vulnerable to simple manipulation (Loeber, 2008).

Another country that has used electronic voting machines is the USA. **Diebold AccuVote-TS** (Feldman et al., 2006) is the most widespread machine in the USA, with more than 33,000 machines in operation. When a voter needs to use a voting machine in the USA, the machine is activated by an election worker to ensure that each voter only votes once. Once a voter has voted, the voting data is stored on a memory module, so that it can be copied from the voting system.

Other countries with experience of voting machines includes countries such as India, Brazil and France.

In India, the use of voting machines has been described as a successful system. The machine contributed to a great extent to making the administration, implementation and counting of votes more efficient and reliable, particularly in the light of the large numbers of people casting votes at national elections (over 600 million). From the start of the 1980s and into the 2000s, there was also a large amount of trust in the security of the system. The security of the system and lack of official technical evaluations were later viewed more critically (Wolchok et al., 2010).

Brazil started using electronic voting in 1996 and was the first country with wholly electronic elections in 2000. As a result of this, the country is often described as a pioneer in this area. As with India, the implementation in 2000 was regarded in many fora as a success, while in recent times, criticism has been aimed at the system's security mechanisms and other conditions related to transparency and auditability. Furthermore, some of the literature criticises the voting system as it has not had the desired effect of voter turnout and trust in the political system, in spite of major investments (Aranha & van de Graaf, 2018).

France has used electronic voting machine the early 2000s. It is only used in 60 municipalities and available to 2 percent of eligible voters. Extensive criticism was aimed at the voting machines during the 2007 election. The criticism related to their general security, but also to specific conditions such as transparency, certification and auditability of the machines. The criticism led to the French authorities pausing the introduction of the voting machines in municipalities that had not already adopted them, and the situation has remained unchanged since then (Enguehard & Noûs, 2020).

3.3.2 End-to-end electronic systems

End-to-end electronic systems have major similarities with electronic systems, but they are based on cryptographic voting protocols, which means that the voter can receive confirmation that their vote has been included in the result. There is a large number of overlapping considerations for end-to-end electronic systems as for classic electronic systems when it comes to implementation.

In practice, end-to-end systems transfer all responsibility for election integrity to the counting of votes itself. If one were to design an extremely simple end-to-end system for a simplified version of the Norwegian election, one could publish a table where each row is a national identity number and each column is a political party. The votes are placed as a cross in the table, and we can thus count how many votes each party has received. Election integrity is protected as each voter can verify that their own vote is correct and that everyone can verify that the crosses have been counted correctly. How the votes are arranged in the table plays no role for election integrity, meaning that there is no need to trust is how this is done. This system thus provides extremely good election integrity, but no anonymity. What complete end-to-end system means in practice is keeping these properties that provide election integrity, while also using different cryptographic methods to anonymise votes. It is thus possible to achieve high election integrity and anonymity.

We do not know that end-to-end electronic systems have been used at large scale, but different systems have been tested at smaller scales, including elections at the regional level in countries.

Examples of end-to-end electronic systems include ElectionGuard, Votebook, STAR-Vote and vVote.

ElectionGuard (Election Guard, 2022) is a software development package issued as an open source code, which can be used to store paperless cryptographic voting systems. The system was developed by Microsoft in collaboration with Galois in 2019.

Votebook (Kirby et al., 2016) is a paperless cryptographic voting system designed for use in controlled circumstances. In contrast to the other examples, Votebook is based on blockchain technology. Blockchain technology makes it possible to keep a distributed transaction log that can be updated and verified by all parties, and which cannot be falsified by any party. It is these qualities that form the basis of cryptocurrencies, such as Bitcoin.

The final example, **STAR-Vote** (Bell et al., 2013), is an electronic cryptographic voting system designed for use in controlled surroundings. The system was developed in 2013 under the leadership of Travis County in Texas.

A distinctive element of STAR-Vote is that even though the voter interacts with a machine with in/out devices, and the vote is registered electronically, a ballot paper is printed out, which the voter then casts by scanning it at a suitable station. The electronic vote is not valid until the ballot paper has been scanned. The voter can potentially invalidate the vote and use it as a test vote to check the system.

vVote (Burton et al., 2016; Eldridge, 2018) is an electronic cryptographic voting system designed for use in controlled surroundings. It has been designed as an electronic version of the paper-based system Prêt à Voter and was used for the state election in Victoria, Australia in 2014. The system also has adaptations that mean that it can be used by the blind and partially sighted.

3.4 Internet-based systems

Internet-based systems are, in this context, electronic voting in uncontrolled surroundings. They can be described as the electronic equivalent of postal votes in paper-based systems.

3.4.1 Classic internet-based systems

With an internet-based system, the voter votes in uncontrolled surroundings, on browsers on personal computers or through an app on a mobile telephone. The votes are entered into a central electronic store and counted up by a machine.

The voter is authenticated with electronic credentials. Authentication of voters and transferring votes to the ballot box can be done with varying levels of quality and security. Once the vote has been cast, it can be placed in the ballot box either in an encrypted way or in plain text. The further transfer for the counting system can also either be encrypted or unencrypted.

As for electronic systems, internet-based systems can be adjusted or used with aids for voters with disabilities.

The Norwegian trials in 2011 and 2013 were trials using internet-based systems in one municipal and county council election and one parliamentary election (Segaard et al., 2014). The trials covered around 168,000 and 250,000 eligible voters, who were able to vote over the internet. The system was only used for the early voting period. Voters were able to cast multiple votes over the internet, and the final vote cast was counted in the determination of election result. Voters were also able to cast a paper vote during the early voting period or on election day, and then it was the paper vote that would be counted.

The system was developed by the Spanish company Scytl, apart from the service that manages the electoral register, which was developed by Ergo.

To vote over the internet, the voter must use a browser and open the website "valg.stat.no". The voter then authenticates themselves using MinID or an approved smart card. In the 2013 trial, BankID was also one of the authentication options. Voters were then sent an SMS receipt. The receipt contained a verification code, a number that could be used to check which party the voter had voted for, and that the vote was received. All voters in the municipalities with electronic voting as a supplement to the regular ways of voting received a polling card with codes on it. These codes and numbers were unique for each individual voter, and in this way, the voter could use the information in the SMS to decode or compare the code with the codes on the polling card.

The use of codes for authentication and verification are still relevant solutions for use in electronic voting systems. Switzerland is a country that has carried out comprehensive trials of electronic voting. Many different voting systems have been used at the same time. Since 2005, 15 cantons in Switzerland have offered internet voting for some of their voters, and a total of 300 trials have been carried out (Swiss Federal Chancellery, 2022). In particular, the systems in the cantons of Geneva and Neuchâtel have continued over time and are currently known as the Geneva system and the Swiss Post system (Applegate et al., 2020). After changes to the law that ensure more insight into the source code of the various systems, the Swiss Post system's code was made available in 2019. This revealed multiple security flaws and led to debate around internet voting and security in Switzerland. As of 2022, some cantons are planning to reintroduce a redesigned version of the Swiss Post system. For the new version, the issuing of codes to voters is central with regard to both authentication and verification purposes. We describe this new version in more depth in the next subchapter, as it can be described as an end-to-end system.

The Estonian system is based on electronic votes cast in uncontrolled surroundings (Springall et al., 2014). The voter downloads an app to their personal computer and uses this to cast their vote. For authentication, the system primarily uses Estonia's national ID card, which is a smart card that is capable of performing cryptographic operations and is used to authenticate and authorise the voter. Alternatively, there is also a system called Mobile-ID, which is based on mobile phones and SIM cards, but this is used much less frequently.

The protocol is similar to using ballot paper envelopes and cover envelopes. The vote is encrypted and signed electronically by the voter. It is then sent over a secure connection (TLS) to central machines. The voter receives a unique ID that refers to the encrypted vote. By sending in this ID, the voter can receive the encrypted vote and this check that the encrypted vote has been registered as cast. It is possible to vote multiple times, and it is only the last vote that counts. The voter also receives a receipt that the vote has been cast, but cannot verify that it has been included in the result.

The encrypted votes are stored alongside voters' identities on central machines, and when voting has concluded, the voter's electronic signature is checked for each vote. After this, all the encrypted votes are written onto a DVD without identifying information, which is then sent to a counting machine in a public place. Here, the votes are decrypted and counted, and the determination of election result is printed out.

3.4.2 End-to-end internet-based systems

End-to-end internet-based systems are characterised by many of the same distinctive elements as classic internet-based systems, but they are based on cryptographic voting protocols, which means that the voter can receive confirmation that their vote has been included in the result.

Belenios, an internet-based, cryptographic voting system, was used for elections to legislative assemblies in France in June 2022. Through Belenios, the voter is sent credentials via email. These are used to carry out voting on a browser, and the voter receives an acknowledgement code that can be checked against published electronic ballot papers. The voter can cast their vote in a number of ways so that it is only the last vote that counts.

Belenios is based on the **Helios** system (Adida, 2008). Helios is an internet-based, cryptographic voting system, which is provided as open source code. The system was proposed by Ben Adida of Harvard University in 2008.

Internet voting has been a theme discussed in France, especially in recent decades. In 2012, French people living abroad were allowed to vote electronically over the internet for the first time at the national elections. This was only for parliamentary elections, and not for presidential elections. Electronic voting was a supplement to using paper ballots, but the voters were only allowed to vote once. In 2017, the possibility of internet voting for people living abroad was suspended after concerns about the security of the system and the risk of hacker attacks and manipulation of the election (NOU 2020: 6). In 2020, France reintroduced internet voting for voters living abroad, but only for certain parts of the electoral system.

While improving the **Swiss Post** system, which individual cantons in Switzerland plan to use, there is a desire to ensure end-to-end verification. The system works in a way that each voter is sent a sheet with codes on it in advance, which is used to carry out voting in a browser. Voting typically involves multiple questions that are up for the vote. Voting takes place in two phases: first, the voter makes a choice with codes to answer all the questions, and then a special code is used to make the votes final. Finally, the voter is sent a receipt code that corresponds to an acknowledgement code that is printed on the code sheet. In contrast to many other voting systems in the same category, a cast vote is final and cannot be changed later.

Preliminary findings from surveys of the solution show that the systems proposed fall short in specific areas, including documentation, security architecture and implementation of security protocols, but that the technical challenges appear to be manageable (Ford, 2022). The independent surveys also point out that the solutions appear imperfect when they are measured against a theoretical ideal, while the system largely achieves its specified goals based on the threats which the system is meant to withstand.

Another end-to-end internet-based voting system is Vocdoni (Aragon, n.d.), an internet-based, cryptographic voting system based on the Ethereum blockchain technology.

4. Assessment criteria for electronic voting systems

The Council of Europe has established criteria for the introduction of electronic voting. These provide countries wishing to introduce electronic voting with some minimum standards to ensure that the principles for conducting democratic elections are observed. This chapter provides a description of how we have adapted and supplemented the Council of Europe's criteria for use in the analysis of different electronic and internet-based solutions for voting in Norway.

4.1 Background and development of assessment criteria

Norwegian law is assumed to be in accordance with international law. Principles for democratic elections are reflected in a range of international obligations. For the area of elections, it is obligations through co-operation with the Council of Europe, which are of the greatest significance (Kommunal- og regionaldepartementet, 2006).

The Council of Europe was set up in 1949 and has 46 member states, including Norway (Store Norske Leksikon, 2022). The most important task of the Council of Europe today is to protect human rights, democracy and the principle of the rule of law. Co-operation within the Council of Europe has resulted in a network of international agreements and conventions, including the European Convention on Human Rights and the Code of Good Practice in Electoral Matters. The Council of Europe's criteria for the introduction of electronic voting, which forms the basis of the assessment criteria, can be derived from the above-named convention and code.

4.1.1 The European Convention on Human Rights

It is a condition of being a member of the Council of Europe that the country ratifies the European Convention on Human Rights. Article 3 of the European Convention on Human Rights from 1950 (additional protocol) determines that members states are obliged to hold free elections at reasonable intervals with secret voting, under conditions that ensure that the people can freely express their opinion during elections for legislative assemblies. The provisions shall ensure free and secret elections. In accordance with practice laid down by the European Court of Human Rights, the provisions refer not just to the obligation to hold free elections, but also guarantee the voter's individual right to cast a vote and to stand for election. The same applies to universal and equal voting rights for all. This means that the individual voter has individual rights in accordance with the provisions. Elections shall be carried out in such a way that free voting is safeguarded. In addition, the vote shall take place under such circumstances that ballot papers are kept secret. In accordance with legal practice, the rights in article 3 are not absolute, they are the object of implied limits. Members states thus have the opportunity to exercise discretion when setting the conditions for universal voting rights and the electoral system. Such limits and conditions must, however, serve a legitimate purpose (Kommunal- og regionaldepartementet, 2006).

4.1.2 Code of Good Practice in Electoral Matters

The Code of Good Practice in Electoral Matters from 2002 provides guidelines for the implementation of elections in members states of the Council of Europe. The Code is set by the Venice Commission, which was established by the Council of Europe. The Venice Commission is the European commission for democracy through legislation.

The Code of Good Practice in Electoral matters defines "European electoral heritage" through two aspects. The first can be described as constitutional principles that are common to European elections – the right to general, equal, free, secret and direct elections. In Europe, this is expressed through article 3 of the European Convention on Human Rights. The second aspect deals with fundamental conditions that must be in place, such as the rule of law, respect for fundamental rights, and the stability of election laws.

4.1.3 Council of Europe's recommendation on standards for e-voting

In 2004, the Council of Europe published its recommendations with criteria for the introduction of electronic voting. The recommendations are not legally binding, but provide general legal, technical and operational guidelines for electronic and internet-based voting. The recommendations build on the *Code of Good Practice in Electoral Matters* from 2002, and address topics regarded as relevant for electronic and internet-based voting in particular. The purpose of the guidelines is to provide countries wishing to introduce electronic voting with minimum standards to work from. This is to contribute to ensuring that the principles of implementing democratic elections are protected. The Council of Europe points out, however, that even if the recommendations are followed, this does not provide any guarantee for the democratic quality of electronic elections. National legislation can set further

requirements, and an electronic election must be assessed in its entirety and in detail based on its context. Nevertheless, following the recommendations will be an important step in the direction of ensuring the democratic quality of the election process.

The recommendations from the Council of Europe were issued in 2004, few European countries had experience with electronic voting. Accordingly, the recommendations were largely based on theoretical principles rather than practical experience. In 2017, an updated version came that expanded the definition of elections to also include machine counting of votes (Europarådet, 2017).

The updated version considered the development of the field over recent decades. New, stricter recommendations on risk management were included, and topics related to authentication mechanisms, verifiability, auditability and openness are covered extensively in the updated version. This comes, amongst other things, as a result of the fact that this type of assessment has been more relevant due to the growth in internet-based solutions.

The Council of Europe recommends that electronic and internet-based electoral systems be introduced gradually with a feasibility study and thorough testing before being used in elections.

The recommendations cover a total of 49 criteria[5], which the Council of Europe groups into eight categories:

- Universal suffrage
- Equal suffrage
- Free suffrage
- Secret suffrage
- Regulatory and organisational requirements
- Transparency and observation
- Accountability
- Reliability and security of the system

4.1.4 Development of assessment criteria

From the 49 criteria, we have defined a smaller selection of criteria that we regard as relevant for the analysis of voting systems. We have omitted criteria that concern conditions other than the qualities of the systems, such as recommendations related to the implementation of electronic and internet-based elections in general. We have grouped the criteria into fewer, but broader, categories. The three categories are[6]

- security
- transparency and auditability
- usability and inclusion

In addition, we have included a category referred to as *resource use*. Conditions related to resource use cannot be derived directly from the recommendations of the Council of Europe. Knowledge on resource use is, however, important in order to assess the opportunities, risks, benefits and costs of electronic voting, and is therefore included in the knowledge acquisition.

The recommendations of the Council of Europe are designed for solutions for electronic voting. However, as mentioned in the introduction, we will also assess paper-based solutions in our analysis. We do this to have a reference from which to assess electronic and internet-based solutions.

4.2 Security

Security at elections means that the voters should be confident that the votes are not manipulated in any way, that the ballot is secret, that sensitive data is not disseminated and that all votes are counted as they are cast (NOU 2020: 6). The category *security* is meant to underpin that intentional and unintentional events can affect parts or the entirety of the voting process or election outcome. Intentional events may be caused by individual people, groups or foreign powers hoping to gain insight into the voter's choice, affect or cast doubt on the election outcome. Unintentional events can be due to accidents, which then depends on what type of solutions is used. The category *security* consists of the following criteria:

[5] The Council of Europe refers to "standards" in its recommendations, while we use "criteria" in this report.
[6] Criteria in the Council of Europe's recommendations that concern universal, equal and free suffrage, and secret voting are included in the analyses, even though they cannot be directly derived from the categorisation. The principles of universal, equal and free suffrage and secret voting are included in the categories security, transparency and auditability, and usability and inclusion. As previously mentioned, the development of criteria for the analysis and the categorisation of these, designed to be useful for the purpose of the analysis.

Absence of influence – no provisional results shall be made public before voting has ended

Authentication – potential voters shall be authenticated so that only eligible people may vote

Anonymity – it should not be possible to find out who voted for who

Prevention of coercion – it should not be possible to force a voter to vote in a certain way

Equal suffrage – it should be possible to cast a maximum of one vote (or the same number of votes) per voter

Election integrity – it should not be possible to change votes cast or the result of the vote

Correctness – the votes must be correctly counted, and the result of the vote must be published correctly

Verifiability

- Each voter can check that their selected vote has been counted
- Anyone can verify that all valid votes have been counted

Accessibility – the voting system must be accessible in accordance with the specified voting period

The criteria create the foundation for the design of security measures for the voting systems, and the above-mentioned criteria also apply to cryptographic voting protocols.[7] A major difference between e-voting systems and paper-based methods is that the proper use of cryptography in e-voting systems can directly realise certain security requirements that otherwise would be under human and/or machine control, such as anonymity and integrity protection. Other criteria are of a functional or system-oriented nature, such as accessibility (the voting system must be accessible in accordance with the specified voting period) and voter eligibility (authentication), for example. These requirements cannot be achieved or ensured through cryptography.

The anonymity criterion means that it should not be possible to find out who has voted for whom, and is relevant both during and after voting. For analysis purposes, anonymity during voting (secret voting) is limited to assessing anonymity for the general voter. Conditions related to secret voting for voters with special needs are covered by *usability and inclusion* (see Chapter 4.4).

The anonymity criterion is also related to the purchase and sale of votes. The value of the purchase and sale of votes is limited when it is not possible to find out who someone has voted for (Saglie & Segaard, 2016).

We choose to include "Equal suffrage" as a separate criterion since it is key voting principle. On the other hand, we do not assess the solutions according to this criterion. All computer systems can be exposed to vulnerabilities the allow for an attack. It is therefore imaginable that an attacker could be successful in modifying the programme code in such a way that individual votes are deleted, replaced or duplicated. This constitutes a breach of integrity, which we cover in the "election integrity" criterion.

As described in Chapter 2, confirmation for the voter that the vote has been counted is valuable as it can ensure the integrity of the election result. This illustrates the dependence between two of the security criteria: election integrity and verifiability. This dependence also leads to a certain perspective of how to secure e-voting systems: "verify the election result, not the voting system" (Ryan et al., 2009).

In some cases, it may be desirable that e-voting systems have functionality to counteract the danger that voters may be exposed to coercion. An example of the functionality that may contribute to counteracting coercion is to provide eligible voters with the opportunity to vote multiple times. The electoral system may, if possible, decide that it is the last vote cast that counts, or that the vote on election day is counted, and not the electronically cast vote.

4.3 Transparency and auditability

Transparency and auditability are key conditions for the election process. In general, the arrangement of the monitoring of elections contributes to increasing transparency and trust in the election. Transparency will also be necessary for the auditability of a system, which in turn is vital for ensuring the integrity of the votes cast.

The choice of voting system, either paper-based or electronic, has implications for how transparency and auditability are arranged, but also for what it means to have transparent and auditable systems.

For the category *transparency and auditability*, we have the following criteria:

[7] Cryptographic voting protocols are described in more detail in sub-chapter 2.8.

Transparency: The voting system and sub-components of the system shall be open to checks, observation, evaluation and verification, according to technical and security-related requirements for the voting system.

Auditability: It should be possible to audit the integrity of votes cast and that the results of the vote are protected It should be possible to audit the counting of the votes, for example by using observers.

Transparency is closely related to both trust and security in the election process (NOU 2020: 6). For trust in the election process, it is regarded as important that voters understand, or have the opportunity to understand, the election process. There may be intrinsic value in the fact that the crucial processes can be observed and controlled without the need for specialist expertise (NOU 2020: 6). However, some argue that the understandability for how the election process is implemented in some cases may come at the cost of the security of the system (Rogers, 2021). If parts of the election process require complex technical solutions and the need for encryption and security clearances, it will lead to less transparency and that most people will not be able to describe how the election process takes place. On the other side, it is necessary to have a sufficient level of security to create trust in the election process. In such cases, security measures must be combined with transparency around the workings of the solution. This illustrates the dependencies between transparency and auditability in the election process.

Our design of the assessment criteria for transparency and auditability emphasises how electronic voting systems allow for transparency and auditability.

For electronic voting systems, transparency can involve the documentation of software and the cryptographic voting protocols used. This is necessary to ensure the auditability of the system. Auditability and good monitoring procedures ensure accountability and are a source of the election result being regarded as trustworthy. The current, regular, paper-based electoral system in Norway can only audit the election result by re-counting paper votes.[8] Auditability of electronic voting is related to verifiability to a greater extent. It should be possible to verify that the operations used in the electronic solution are correct and that the result is correct.

[8] This is the case given that votes are stored safely for the necessary period of time.

4.4 Usability and inclusion

The category *usability and inclusion* is related to the use, understanding and easy accessibility of the voting solution, as well as the inclusion of people with disabilities that entail a need for adapted voting. We discuss this group as voters with *special needs*.

The recommendations of the Council of Europe emphasise that the electronic systems should be user-friendly. It should be easy for voters to understand how to participate in the election and how to cast their vote. We have used the following criteria:

Usability: The voting system shall be easy to understand and use

- for voters in general
- for voters with different levels of technical understanding
- for voters voting from abroad

Inclusion

- The voting system shall be easy to understand and use for voters with special needs.
- The voting system shall make it possible for voters with special needs to vote unassisted.

For the *usability* criterion, attention is focussed on voters in general, voters with different levels of technical understanding, and voters voting from abroad. Usability concerns both how and whether voters manage to adopt the solution, and, moreover, what opportunities the solution provides for use. For example, electronic and internet-based solutions can allow for interaction during the voting process, something which is not possible in the same way with paper-based solutions. Interaction in this context refers to the interaction or interplay between the voter and the computer system in the voting. For example, the computer system may provide a response to a voter that the voter has not cast their vote correctly before the vote is sent off.

Another aspect that contributes to usability is physical accessibility, i.e. what times and at which locations is it possible to cast a vote.

The *inclusion* criterion has two aspects. The first concerns whether the solution is user-friendly and understandable for voters with special needs. Relevant factors are how different solutions can be adapted for the use of aids that provide better usability. The other aspect is the condition for unassisted voting. This deals with whether the voting system can be designed so

that blind and partially sighted voters can vote without assistance. See also the discussion on *anonymity* in Chapter 4.2.

4.5 Resource use

Resource use concerns what is required in terms of human and financial resources at the state and municipal level at the introduction and operation of electronic or internet-based voting as a supplement to regular, paper-based election processes.

Awareness is targets at resource use in the practical election process. The criteria do not include work related to any necessary changes to regulations, and also does not assess how the introduction of electronic or internet-based voting will affect voters' resource use when they need to cast their vote.

Resource use at the local and national level refers to

- materials, equipment and systems
- staffing and training
- premises
- information and guidance

Materials, equipment and systems concerns the things the state and municipalities need to develop, procure, implement and operate in terms of software and hardware relating to electronic and internet-based voting systems.

Staffing and training concerns how the state and municipalities' need for staffing will change. For example, will municipalities need to employ more election workers, or will they manage with fewer? And is there a need for different types of skills and/or training?

Premises concerns whether municipalities need to make adaptations to the premises they use for elections, and whether the state, as a result of the introduction of electronic and/or internet-based elections, will need to establish need central electronic storage sites.

Information and guidance concerns whether the state and municipalities must run more active information efforts aimed at voters, and whether municipalities will need to increase the guidance during the election process.

5. Security

Security concerns the fact that all voters should be confident that the votes are not manipulated, that the vote is secret, that sensitive data is not disseminated and that all votes are counted as they are cast. It is our assessment that a paper-based system safeguards the requirements for security to a greater extent than electronic and internet-based systems. In this chapter, we provide a more detailed description of our assessments.

5.1 Primary findings: Security

Figure 5-1 summarises how we have assessed the various criteria related to the *security* category.

As mentioned in Chapter 1, we have carried out a risk analysis and assessed the degree to which electoral systems fulfil the respective criteria described in Chapter 4. The degree of fulfilment is provided on a three-tiered scale:

- **To a great extent:** There are no major challenges for the voting system, and the criteria are met to a great extent.
- **To some extent:** There are certain challenges for the voting system hindering the fulfilment of the criteria, but the challenges are not significant, or the solution allows for the fulfilment of the criteria in another way.
- **To a limited extent:** There are significant and/or insurmountable challenges for the voting system, which mean that the criteria are fulfilled to a limited extent.

To start with, there are many types of paper-based systems and different variations of electronic and internet-based systems. In the analysis, we have considered the Norwegian electoral system as the basis for the paper-based system, and the part of the election where votes are cast in polling stations on election day. For electronic and internet-based systems, it is the concepts which we are analysing. We do not examine the conditions related to the design and implementation of concrete solutions in more detail, such as the significance of cryptography (see Chapter 2.8). It is difficult to say how cryptographic methods will impact systems on a general basis. This is due to the fact that the use of cryptographic methods is closely related to the implementation of the specific solution that is to be introduced. There can be very subtle aspects of many stages of the voting process, which can have an impact on the actual result.

The current paper-based electoral system in Norway comes out best in the security assessment. It is our assessment that the system meets almost all security criteria for an electoral system to a great extent. The only criterion the Norwegian system did not fulfil completely is the criterion of *verifiability*, even though verification is partially possible in the current electoral system.

Electronic systems come out weaker in the assessment of the *security* category. The main reason for this is the risk that the election result could be manipulated through electronic systems, something which could have consequences for the election outcome. This risk is reflected in the criteria relating to election integrity and correctness. In electronic systems, there will also be a greater risk of someone gaining access to and publishing some of the election results in advance of official announcements. This would be a breach of the criteria of absence of influence.

Internet-based systems come out weakest in the assessment of the *security* category. Internet-based systems have the same risk elements as electronic systems related to manipulation and advanced publication of election results. In addition, voting with internet-based systems takes place in uncontrolled surroundings, meaning it is much more challenging to verify that the right person is voting and that the vote is secret. These risk elements were observed in the criteria for authentication, anonymity and preventing coercion.

Electronic and internet-based voting systems have an additional intrinsic vulnerability factor due to their centralisation. For end-to-end electronic systems, only vote management is centralised, while for internet-based systems, every aspect of the vote process is centralised. Significantly fewer election officials are involved in centralised systems, and these systems require and assume that the few clerks involved are fully trusted.

Below, we describe in more detail how each of the electoral systems do against each of the security criteria described in Chapter 4.

Figure 5-1: Assessment of voting systems against security criteria

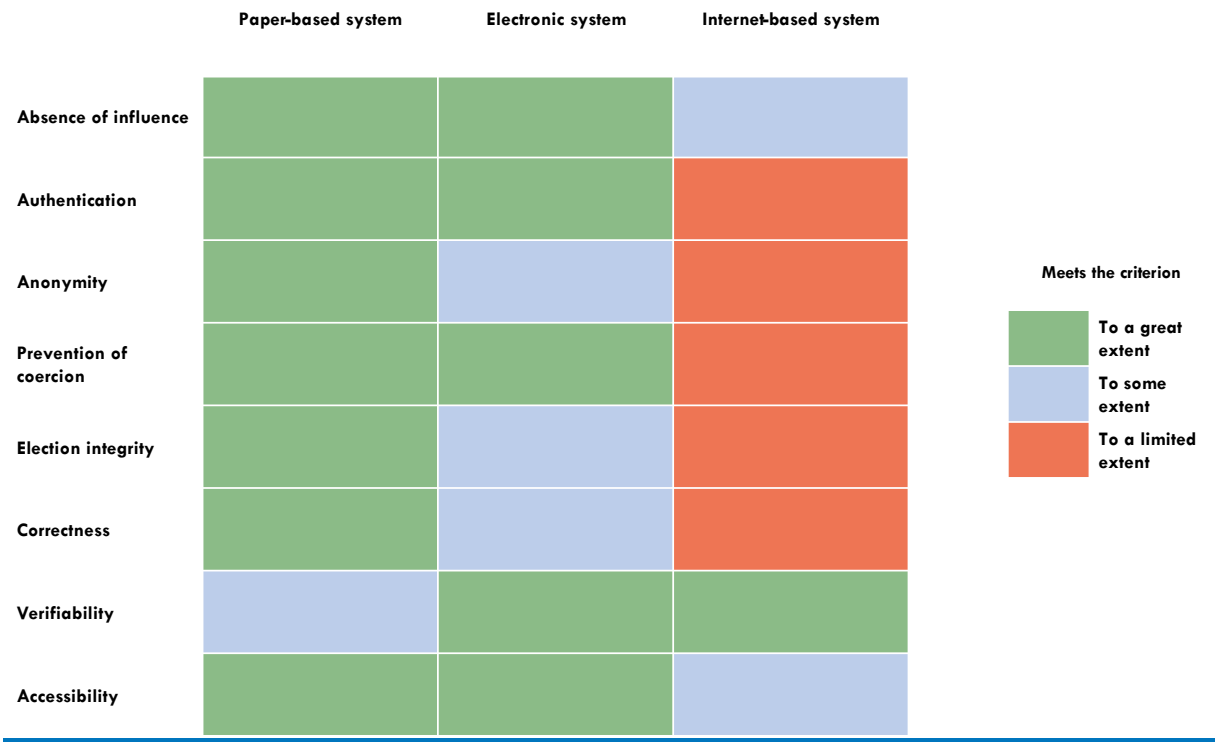


Illustration: Oslo Economics and Norwegian Computing Centre

5.2 Paper-based systems

5.2.1 Absence of influence

This criterion concerns the fact that voters should not have any preliminary information about the election result when they are voting. In the Norwegian system, this criterion is fulfilled by having clear guidelines for when the counting of votes shall begin, something which (implicitly) determines when the result can be published. This criterion can, however, be breached if someone gets access to preliminary results, and they publish this before the publication date of the result. Nevertheless, our assessment is that the Norwegian system meets the criterion of absence of influence to a great extent.

5.2.2 Authentication

The criterion of authentication concerns the fact that it must not be possible to successfully masquerade as pretend to be someone else during the voting process. In the Norwegian system, the voter authenticates themselves by showing identification to an election official, which the election official then checks against the electoral register. This criterion can be breached if someone uses someone else's identification. However, there have been few reported cases of this in the current electoral system. Given that voting takes place in controlled surroundings, it is difficult to successfully pretend to be someone other than who you are. It is therefore our assessment that the Norwegian system meets the authentication criterion to a great extent.

5.2.3 Anonymity

The anonymity criterion concerns the fact that it should not be possible to find out who has voted for whom, and is relevant both during and after voting. Anonymity during voting may be compromised, for example, if someone is observing the voting, while anonymity after voting concerns no one being able to link a specific vote to a voter. As discussed in Chapter 4, this criterion concerns the anonymity of the general voter. Conditions related to secret voting for voters with special needs is covered by *usability and inclusion* in Chapter 7.

In the Norwegian system, anonymity is ensured by the voter marking their choice on a ballot paper in an enclosed booth and then folds it up, which keeps it concealed from the booth to the ballot box. Once the ballot paper has been placed in the ballot box and has been mixed with the other votes, it is not possible to link it back to a voter. It is possible to breach this criterion if, for example, voters or election clerks look inside a polling booth when someone is picking who they will vote for. There have only been a few reported cases of this in the current system. It is our assessment that the Norwegian system meets the anonymity criterion to a great extent.

5.2.4 Prevention of coercion

The criterion of prevention of coercion concerns the fact that it should be difficult to force a voter to vote for a specific party or a specific candidate. As a basis, it will be difficult to subject voters to coercion in

the Norwegian system. The basis for this is that voting takes place in controlled surroundings, where election officials ensure that voters are alone in the polling booth when they cast their vote.[9] Someone trying to coerce another cannot know how they voted, and thus the voter will be able to cast their vote without fearing consequences from the third party. It is therefore our assessment that the Norwegian system meets the prevention of coercion criterion to a great extent.

5.2.5 Election integrity

The criterion of election integrity concerns that all votes are correctly reflected in the election result. In the Norwegian system, as well as other paper-based systems, this security criterion can be breached if votes from certain selected parties are systematically changed or rejected. We are not aware of reported cases of this in Norway, and voters have great trust that their vote is handled in a secure manner (Bock Segaard, et al., 2014). It is therefore our assessment that the Norwegian system meets the election integrity criterion to a great extent.

5.2.6 Correctness

The criterion of correctness concerns the fact that votes shall be counted and reported in a proper manner.

In the current Norwegian system, the counting of votes takes place in two rounds [10]. Systematic fraud will therefore need the co-operation of many election officials. We are not aware of any reported cases of this in Norway. In the case of individual errors, this will be of little significance for the final election outcome. For the 2021 parliamentary election, 4,517 votes were discarded (*Innst. 1 S (2021-2022)*, 2021). A missing stamp on the ballot paper is the most common grounds for rejection and is often due to the fact that the voter uses a separate ballot paper as an "envelope" for their actual vote, typically to hide what they had voted for. In such cases, where only the envelope is stamped, the actual vote is then discarded (*Innst. 1 S (2021-2022)*, 2021). This can be avoided with electronic or internet-based systems, as discussed in more detail below. It may also be that paper votes re misplaced or that they are not sent to the place where votes are counted. If this is detected, the electoral committee must assess whether the election can be approved. Given the history and the security systems in place, it is our assessment that the Norwegian systems meet the correctness criterion to a great extent.

5.2.7 Verifiability

The criterion of verifiability concerns the fact that the voter should receive a confirmation that their vote has been cast, that it has been included in the final election result, and that all valid votes have been counted in the final election result.

The Norwegian system partially fulfils the criterion of verifiability because the voter can (implicitly) verify that the vote has been cast when they place it in the ballot box. However, the voter cannot verify that the vote has been included in the final election result, or that all valid votes have been counted in the final result. It is therefore our assessment that the Norwegian system only meets the verifiability criterion to some extent.

5.2.8 Accessibility

The criterion of accessibility concerns the fact that the voting system must be accessible in accordance with the specified voting period. In paper-based systems, there is a limited risk landscape for breaches of accessibility. Breaches of accessibility in this context will be related to physical conditions at the polling station. This may be a power outage or fire, for example. It is our assessment that the Norwegian system meets the accessibility criterion to a great extent during election time.

5.3 Electronic system

5.3.1 Absence of influence

This criterion concerns the fact that voters should not have any information about election results when they are voting. With electronic systems, there is a low risk that preliminary election results will be published before voting has finished. The reason for this is that anyone hoping to publish the results in advance must gain access to voting machines and extract the results from these. In practice, this would be difficult to achieve, and we are not aware of such events in countries that have adopted electronic systems. It is therefore our assessment that electronic systems meet the election confidentiality criterion to a great extent.

5.3.2 Authentication

The criterion of authentication concerns the fact that it should not be possible to successfully pretend to be someone else during the voting process. Electronic systems are also used in controlled surroundings, where an election official checks the voters' identification upon arrival at the polling station. We are not aware of electronic systems with an integrated authentication solution, even though this may be possible. Voter authentication is, in other words, like the current Norwegian paper-based system, and the likelihood that a person is able to successfully pretend to be someone else is low as it would require the false use

[9] It is important to remember here that the analysis concerns voting that takes place in polling stations. Other assessments will apply to voting that takes place via postal votes.

[10] The methods of counting in the two rounds are also independent of each other – one machine and one manual.

of identification. It is therefore our assessment that electronic systems meet the authentication criterion to a great extent.

5.3.3 Anonymity

The criterion of anonymity concerns the fact that votes must remain hidden to everyone else throughout the voting process. By and large, the same assessments apply here as for paper-based systems: it is possible to imagine events, for example that someone sees how others are voting at the polling station, which would breach the anonymity criterion. However, the likelihood of these events is low.

Nevertheless, there are some other events that are also relevant when assessing the anonymity of electronic systems. The most important of these is that someone links the voter's identity and vote after the vote has been cast. This breach of security is possible in an electronic system because there is an electronic connection between the voter and how the voter has voted. If someone gains access to the voting machines used, it could be possible to identify who has voted for whom. How difficult this is will depend on the conditions underpinning the system. Cast votes are protected with encryption, but since crypto keys are established by a trusted party associate with the conduct of the election, anonymity protection depends particularly on the trusted party and how key management is carried out.

It is important to highlight that the likelihood of a security breach of this type is relatively low as it would require that someone gains access to the voting machines. However, this is an additional risk of electronic systems that does not exist for paper-based systems. It is therefore our assessment that electronic systems meet the anonymity criterion to some extent.

5.3.4 Prevention of coercion

The criterion of prevention of coercion concerns the fact that it should be difficult to force a voter to vote for a specific party or a specific candidate. As a result of the above criterion, there will be good protection of the voter against coercion in an electronic system. The basis for this is that properly securing anonymity makes it difficult for third parties to know how a person has voted, and they thus cannot exercise actual coercion over people. Anonymity is ensured largely because voting takes place in controlled surroundings, where election officials ensure that voters are alone in the polling station when they cast votes.

Overall, it is our assessment that electronic systems meet the criterion of prevention of coercion to a great extent.

5.3.5 Election integrity

The criterion of election integrity concerns the fact that the voter's vote is included the actual election result.

Election integrity can be breached in many ways in an electronic system. The most obvious way will be that someone changes the software in the machine ahead of the election. An illustrated example of this emerges in relation to a security analysis (Feldman, et al., 2006) by Diebold Accuvote-TS, which is widely used in elections in the USA. The analysis of the machine concluded that everyone with physical access to the machine could easily install malicious program code that changes votes. This is also not a unique example. An analysis of the NEDAP ES3B voting machine (Gonggrijp & Hengeveld, 2007), which is used at elections in the Netherlands, Germany, France and Ireland, has shown that it was similarly easy for attackers to get control of them. These examples illustrate the vulnerability of the integrity of electronic voting systems. This also means there is a high vulnerability of internal secrecy regardless of whether it is a classic system or an end-to-end system.

It is difficult to assess the likelihood of the risk elements described above actually happening. In the event that they were to occur, the consequences for the election outcome would likely be somewhat greater than in the case of a breach of electoral integrity in the current Norwegian system. The reason for this that it will affect all votes from a voting machine and not just individual votes. A factor that contributes to limiting the potential consequences is that the counting of votes for the majority of the electronic systems takes place locally. It is therefore our overall assessment that electronic systems meet the election integrity criterion to some extent.

5.3.6 Correctness

The criterion of correctness concerns the fact that votes shall be counted and reported in a proper manner. For electronic systems, voting will primarily take place through an automatic process: When voters cast their vote, it will be stored in an electronic memory, and when voting has closed, it will be counted up. The method of counting itself will vary from system to system, but in the majority of cases, the counting takes place.

The most common way that a security breach/compromise/attack could occur, could be according to the same method of attack that was outlined in the assessment of election integrity: someone gains access to the software in the counting machine and makes changes so that the count is incorrect.

The automation of the counting process may contribute to reducing the likelihood of sources of errors found in

manual counting, but the consideration related to the scope and risk of errors features heavily in our assessments. Our assessments of the likelihood of the criterion being breached, and the consequences of this, are the same as for our assessment of election integrity in the chapter above. As such, electronic systems meet the correctness criterion to some extent.

5.3.7 Verifiability

The criterion of verifiability concerns the fact that the voter should receive a confirmation that their vote has been cast, that it has been included in the final election result, and that all valid votes have been counted in the final election result. As a starting point, it is easier to have end-to-end system with full verifiability when someone uses electronic systems compared to paper-based systems. The reason for this is that end-to-end solutions assume that it is possible to cast votes based on a number of possible combinations of choices. In the Norwegian electoral system, where it is possible to cast a personal vote, there are many potential combinations of voting choices. It will never be possible to have a paper ballot for each of these combinations in a paper-based election, but it is possible when the ballot papers are electronic, as in an electronic system. It is therefore our assessment that electronic systems meet the verifiability criterion to a great extent.

5.3.8 Accessibility

The criterion of accessibility concerns the fact that the voting system must be accessible in accordance with the specified voting period. Since electronic systems, like paper-based systems, are in controlled surroundings, electronic systems share the same risk landscape when it comes to physical accessibility as paper-based systems.

When it comes to electronic vulnerability, voting takes place on voting machines, something which increases the vulnerability. Given that the machines are connected to the internet, it is our assessment that there will not be a significant increase in the risk compared with paper-based systems, and that the criterion is met to a great extent.

5.4 Internet-based systems

5.4.1 Absence of influence

This criterion concerns the fact that voters should not have any information about preliminary election results when they are voting.

With internet-based systems, there is a risk that preliminary election results could be published before the voting is finished. This may happen if the attacker gets access to those parts of the system where the already cast votes are stored. This risk is not present in paper-based systems such as the Norwegian one. This is because the votes are not stored at a central site. Due to this risk, it is our assessment that an internet-based system meets the absence of influence criterion to some extent.

5.4.2 Authentication

The criterion of authentication concerns the fact that it should not be possible to pretend to be someone else during the voting process. Internet-based systems differentiate themselves from the other two systems in that voting takes place in uncontrolled surroundings. This has consequences for how voter identifies themselves. In an internet-based system, the voter will identify themselves by using electronic credentials, such as BankID or codes. Others can gain access to these credentials, pretend to be the voter and thus breach the authentication criterion. Credentials that use two-factor authentication[11] or biometric authentication may be more secure, but it is still our assessment that internet-based systems meet the authentication criterion to a limited extent.

5.4.3 Anonymity

The criterion of anonymity concerns the fact that the voter's vote should remain hidden to everyone else throughout the voting process. The anonymity of voters may be challenged in a number of ways with an internet-based system. First and foremost, there is a risk that one or more persons are together with the voter when the vote is cast, and are thus able to observe the vote. In the same way as with electronic systems, there is also a possibility of linking a voter to his or her vote. This security issue is possible in an internet-based system because there is an electronic link between the voter and the vote.

If someone breaches an internet-based system, it will in theory be possible to identify who has voted for who, and this will not necessarily be noticed. This type of attack can be carried out by manipulating software in those parts of the system where the voter's identity can be linked to their vote. This applies both to the client, which is typically either a browser or dedicated app, and it can be carried out through a supply chain attack, for example by placing a trojan horse in a library module used by the software. This risk does not exist with paper-based systems.

It is therefore our assessment that internet-based systems meet the anonymity criterion to a limited extent.

[11] Use of two-factor authentication may make it difficult for individual voter groups to vote.

5.4.4 Prevention of coercion

The criterion of prevention of coercion concerns the fact that it should be difficult to force a voter to vote for a specific party or a specific candidate. As it is possible to observe the voter when they are casting their vote, there is a risk from the outset that a voter may be subject to coercion when it comes to the use of internet-based systems.

A factor that can reduce this risk is to design the system in such way that the voter can change their vote until the end of the voting period.[12] However, this does not change the overall picture since anyone wishing to coerce a voter to vote for a party or a candidate can be present right up until the deadline. It is therefore our assessment that internet-based systems meet the prevention of coercion criterion to a limited extent.

5.4.5 Election integrity

The criterion of election integrity concerns the fact that the voter's vote is included the actual election result. For an internet-based system, this criterion can be breached by someone gaining access to the system, and changes it so that the party or candidate a voter has voted for does not appear in the vote count.

The breach of integrity may occur either through the operating system or directly through the software application. Different operating systems may have different access control policies to limit what applications can do with the system, such as, for example, what sort of applications can be installed and the permissions they can have. There is a difference between discretionary access control, where the user themselves makes decisions at their own discretion, and mandatory access control, where the rights are managed according to fixed rules. The latter provides, in principle, less leeway to corrupt the system and has been implemented in Android 5 and later, for example. When it comes to the transfer of an application from an "app store" to a local device, it would be very difficult to corrupt an application at this stage, as all such application chains use digital signatures.

An alternative method of attack is to corrupt the application itself during its development. This is not only a theoretical possibility. Modern applications are based on a large number of software libraries[13]. They may originate from different vendors, and there are concrete examples of libraries that are known to have been corrupted and libraries that have shown serious vulnerabilities that have only been uncovered after a long period of time. If a software/library module used by a voting application is compromised, the attacker can undetectably install a trojan horse in the software/library module, and thus take control of the voting application. This type of attack can also be used against browsers and enable what is known as a "man-in-the-browser" attack, where the attack can manipulate the information that goes through web browsers.

In general, it will be difficult to assess the likelihood for these types of security breaches. Should this occur, the consequences for the election outcome, however, will be extremely large. Potentially it could be scalable and affect all votes cast over the internet. It is therefore our assessment that internet-based systems satisfy the election integrity criterion to a limited extent.

5.4.6 Correctness

The criterion of correctness concerns the fact that votes shall be counted and reported in a proper manner. For internet-based systems, voting will primarily take place through an automatic process. The most common way that a security breach could occur is the one outlined under election integrity: someone breaches the system and changes it so that the counting is erroneous.

As for electronic systems, the automation of the counting process may contribute to reducing the likelihood of sources of errors found in manual counting, but the consideration related to the scope and risk of errors features heavily in our assessments. Our assessments of the likelihood of the criterion being breached, and the consequences of this, are therefore the same as for our assessment of election integrity in the chapter above. It is our assessment that internet-based systems meet the correctness criterion to a limited extent.

5.4.7 Verifiability

The criterion of verifiability concerns the fact that the voter should receive a confirmation that their vote has been cast, that it has been included in the final election result, and that all valid votes have been counted in the final election result. As a starting point, it is easier to have an end-to-end solution with full verifiability when someone uses internet-based systems compared to paper-based systems. The basis here is the same as that for electronic systems. It is therefore our assessment that internet-based systems meet the verifiability criterion to a great extent.

[12] Such a possibility was accommodated during the trial elections using internet voting in 2013 (Saglie & Segaard, 2016)

[13] A library is a collection of sub-programmes to achieve a specific purpose, so that common functionality can be collated into one place then be reused by multiple programmes.

5.4.8 Accessibility

The criterion of accessibility concerns the fact that the voting system must be accessible in accordance with the specified voting period. Internet systems are centralised and thus enable certain events may lead to a breach of accessibility that may affect voting for the entire election.

It is our assessment that internet-based systems meet the verifiability criterion to some extent.

6. Transparency and auditability

Transparency and auditability concern the fact that it should be possible to monitor the entire voting process so that it can be ensured that the election has been carried out correctly. A paper-based system such as the Norwegian one comes out well for these criteria, while both electronic and internet-based systems come out less well. In this chapter, we provide a more detailed basis for our assessments.

6.1 Primary findings: Transparency and auditability

Figure 6-1 summarises how we have assessed the criteria related to the *transparency and auditability* category. As explained in Chapter 1, we assess whether the criteria have been fulfilled using the following three-step scale:

- **To a great extent:** There are no major challenges for the voting system, and the criteria are met to a great extent.
- **To some extent:** There are certain challenges for the voting system hindering the fulfilment of the criteria, but the challenges are not significant, or the solution allows for the fulfilment of the criteria in another way.
- **To a limited extent:** There are significant and/or insurmountable challenges for the voting system, which mean that the criteria are fulfilled to a limited extent.

To start with, there are many types of paper-based systems and different variations of electronic and internet-based systems. In the analysis, we have considered the Norwegian system as the basis for the paper-based system, and the part of the election where votes are cast at polling stations on election day. For electronic and internet-based systems, it is the concepts which we are analysing. We do not examine the conditions related to the design and implementation of concrete solutions in more detail.

The current paper-based electoral system in Norway is used as baseline, and it is this system that comes out the best in the assessment. The main reason for this is that election observers can observe all stages of the voting process, and thus monitor that the election is in accordance with applicable rules.

The stages that are easily observable in a paper-based system, for example the counting and checking of the votes, are more inaccessible for election observers regarding electronic and internet-based systems. Relevant data will be stored securely and can only be controlled by IT specialists.

Below, we describe in more detail how each of the electoral systems do against each of the security criteria described in Chapter 4.

Figure 6-1: Assessment of voting systems against the criteria for transparency and auditability

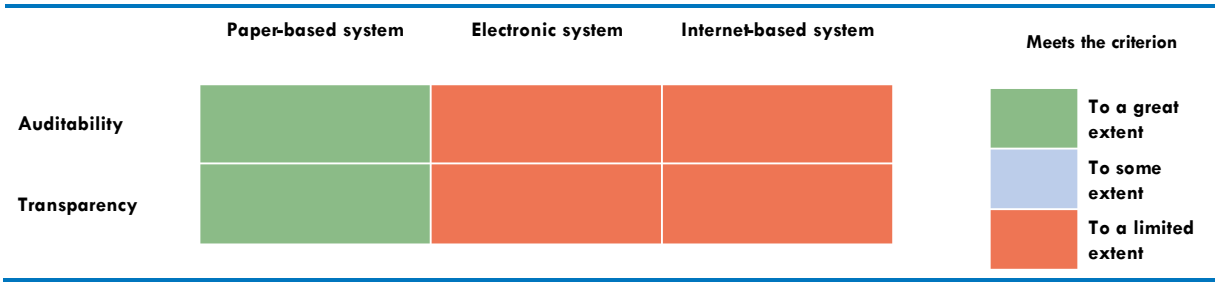


Illustration: Oslo Economics and Norwegian Computing Centre

6.2 Paper-based systems

6.2.1 Transparency

The transparency criterion concerns the fact that election observers should be able to observe the different stages of the voting process to monitor that the process is in line with the criteria for the election process. In a paper-based system, such as the Norwegian one, it is possible for election observers to observe all stages of the voting process, including the stages before and after the submission of votes into the ballot box. It is therefore our assessment that the current Norwegian system meets the transparency criterion to a great extent.

6.2.2 Auditability

Auditability concerns the fact that it should be easy for election observers to check that the integrity of the votes has been safeguarded and that the counting of votes has been conducted correctly. Since paper-based systems such as the Norwegian ones come out

well for the criteria transparency, it follows that they also do well when it comes to auditability. It is therefore our assessment that the Norwegian system meets the auditability criterion to a great extent.

6.3 Electronic systems

6.3.1 Transparency

The transparency criterion concerns the fact that election observers should be able to observe the different stages of the voting process to monitor that the process is in line with the criteria for the election process. Electronic systems, such as in Brazil, have received criticism for lacking transparency in their systems. The criticism against the Brazilian solutions concerns the fact that voters have no opportunity to know whether their vote has been included and correctly counted. The criticism also concerns whether there are logistical challenges during the testing of the system. It is impossible to prove that the tested software corresponds with the installed software on the machines, and that the machines used in the election work in the same way as those that were tested. In addition, a large and complex codebase provides limited opportunities to carry out security testing (Aranha & van de Graaf, 2018).

Electronic systems are less transparent than paper-based ones. The reason for this is that the digital information and program code, including voting data, are represented by complex bit patterns that are stored in different forms of electronic memory. In addition, the information is encoded by means of several layers of complex protocols and encrypted using different cryptographic mechanisms. The only way to make this information accessible and understandable to humans is using pertaining computer software and present it on an output device, such as a screen or a printer. The opportunity of observing what is happening in the system is also critically dependent on the mentioned software, which creates a new layer of uncertainty. It is therefore our assessment that electronic systems meet the transparency criterion to a limited extent.

6.3.2 Auditability

Auditability concerns the fact that it should be easy for election observers to check that the integrity of the votes has been safeguarded and that the vote count is taking place in a proper manner.

Auditing with regard to a paper-based system is simple, since regular paper ballots are humanly readable, and in principle, be handled, interpreted, understood and counted by practically anyone. As explained above, it is more difficult to audit an electronic system. The vote and the result rely on computer software, and a fundamental uncertainty factor is the extent to which you can trust the programme. For example, when a voter casts their vote using a regular electronic voting machine, the machine will display their selection on a screen. If the machine is manipulated or contains an error, the screen could display the correct choice to the voter while another vote would be actually registered in the memory. In classic electronic and internet-based systems, this uncertainty factor exists in principle at all points where it is desirable to audit the process. On the other hand, this is not present in paper-based systems, since interpreting the information is not necessary.

Simple electronic end-to-end systems will require less testing than other voting systems. In short, this is on the grounds that the results of the voting will be publicised in such a way that voters themselves can audit the results; if a small proportion of voters does so, this will be a sufficient audit of the system. However, it is unlikely that such an end-to-end electronic system will be introduced. The reason for this is that it will be extremely challenging for voters to use, something we will come back to in Chapter 7.5. It is therefore our assessment that electronic systems meet the auditability criterion to a limited extent.

6.4 Internet-based systems

6.4.1 Transparency

The transparency criterion concerns the fact that election observers should be able to observe the different stages of the voting process to monitor that the process is in line with the criteria for the election process. Internet-based systems, such as the one in Estonia, have received criticism for lacking transparency (Springall et al., 2014). Estonian authorities have, however, introduced measures to meet this criticism. They have provided for the participation of election observers, and they have published parts of the source code of the solution. In addition, there is a requirement for an independent expert evaluation of the result (Ehin et al., 2022).

For internet-based systems, as for electronic systems, information is represented by means of complex bit patterns that are stored on different types of electronic memory. In addition, the information is encoded by means of several layers of complex protocols and encrypted using different cryptographic mechanisms. In order to be able to observe and check the count in an internet-based system, election observers will require specialized technical knowledge and skills. Thus, fewer people will be able to become election observers, and the job of election observers will also be more demanding with an internet-based system. Overall, it is our assessment that internet-

based systems meet the transparency criterion to a limited extent.

6.4.2 Auditability

Auditability concerns the fact that it should be easy for election observers to check that the integrity of the votes has been safeguarded and that the vote count is taking place in a proper manner.

In the same way for electronic systems, internet-based systems are poorly auditable because of the lack of transparency. It is therefore our assessment that internet-based systems meet the auditability criterion to a limited extent.

7. Usability and inclusion

Usability and inclusion concern the fact that voting solutions shall be simple to understand and use, as well as to enable unassisted voting. All solutions have advantages and disadvantages; however, we assess that electronic and internet-based systems meet the criteria to a great extent because by-and-large they allow for unassisted voting for voters with special needs. In this chapter, we provide a more in-depth description of our assessments.

7.1 Primary findings: Usability and inclusion

Figure 7-1 summarises how we have assessed the criteria for *usability* and *inclusion*. As explained in Chapter 1, we assess whether the criteria have been fulfilled for the three main categories of voting systems according to the following three-step scale:

- **To a great extent:** There are no major challenges for the voting system, and the criteria are met to a great extent.
- **To some extent:** There are certain challenges for the voting system hindering the fulfilment of the criteria, but the challenges are not significant, or the solution allows for the fulfilment of the criteria in another way.
- **To a limited extent:** There are significant and/or insurmountable challenges for the voting system, which mean that the criteria are fulfilled to a limited extent.

To start with, there are many types of paper-based systems and different variations of electronic and internet-based systems. In the analysis, we have taken the Norwegian system as the basis for the paper-based system, and the part of the election where votes are cast in polling stations on election day. For electronic and internet-based systems, it is the concepts which we are analysing. We do not examine the conditions related to the design and implementation of concrete solutions in more detail.

Our overall assessment is that paper-based systems, such as the Norwegian one, meet the criteria for *usability* and *inclusion* to some extent. Paper-based systems are beneficial for voters with low technical competence. For blind or partially sighted voters, the solution is difficult to use, and for individuals within this group, the solution does not allow for unassisted voting. What Figure 7-1 does not show is that usability can mean different things for different voter groups.

Our overall assessment for electronic systems is that they meet the criteria for usability and inclusion to some extent. The advantage of these systems is that they open up opportunities for interactive solutions and allow for the use of aids for those users with special needs. This can lead to increased usability through clarifying for voters the options they have for voting, and it can prevent voters from making mistakes inadvertently. This can also allow for unassisted voting to a greater extent than paper-based systems such as the one Norway has today. However, we do not give a score of *to a large extent*, since the systems can be challenging for digitally excluded people to use.[14] There is also uncertainty about whether it is practically possible to design solutions that actually allow for unassisted voting for all voters.

In conclusion, our overall assessment is that internet-based systems also meet the criterion for usability to some extent, but meet the criterion for inclusion to great extent. Internet-based systems share many characteristics with electronic voting systems, but provide good physical accessibility, and have the potential to make unassisted voting a possibility for the blind and partially sighted.

Below, we describe in more detail how each of the electoral systems do against each of the criteria.

[14] Digital exclusion means lacking access to or the opportunity to use digital services that are necessary to exercise rights (Digdir, n.d.)

Figure 7-1: Assessment of voting systems against the criteria for usability and inclusion

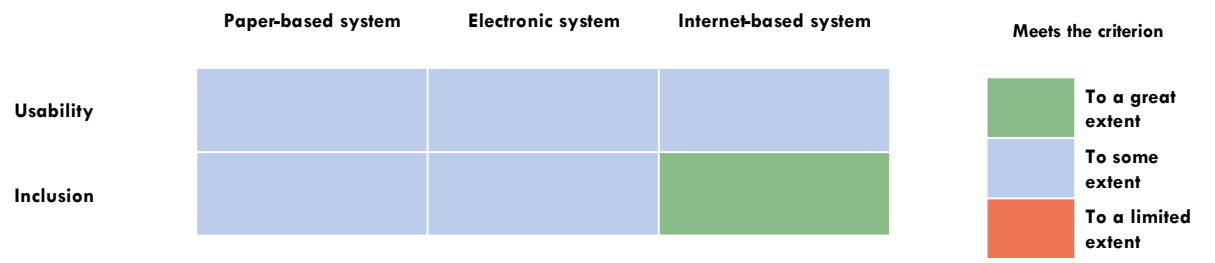


Illustration: Oslo Economics and Norwegian Computing Centre

7.2 Paper-based systems

7.2.1 Usability

The criterion of usability concerns the fact that the voting system shall be simple to understand and use for voters. When it comes to voting in person at the polling station, the Norwegian system comes out relatively well. The system is well-established, and voters have good understanding of how it works. It is a benefit for some voter groups that no technical skills required to use it.

A survey from the autumn of 2020 having around 3,000 respondents shows that around three percent of the population aged 16 years and older do not use the internet or digital tools such as a smartphone, computer or tablet, and eleven percent have poor basic digital skills (Bjønness, et al., 2021). For this group, electronic and internet-based solutions may provide insurmountable challenges, however this group is used to the regular, paper-based Norwegian system.

Paper-based systems also have weaknesses. Firstly, they are not interactive; the system cannot automatically check that the voter has cast their vote in the correct manner. Secondly, the Norwegian system is less user-friendly in terms of accessibility for voters in general compared to internet-based solutions. This concerns the difference between controlled and uncontrolled environments, where controlled conditions require the voter to go to a polling station to cast their vote. This is even more clear for voters voting from abroad since access to polling stations is limited.[15] The current paper-based system in Norway contributes to increased physical accessibility by offering early voting and ambulatory voting in special cases. Regardless, it will be less user-friendly than voting at home; however, the difference between voting in a polling station and voting at home will be less important if good early voting opportunities are available.

It is our assessment that paper-based systems meet the usability criterion to some extent.

7.2.2 Inclusion

The criterion of inclusion concerns the usability of voting systems for groups with special needs, for example, people with disabilities or reduced cognitive abilities, as well as how the system allows for unassisted voting.

The key thing when it comes to paper-based systems is the lack of opportunity to use digital aids. In the Norwegian paper-based system, the general paper ballots ("generelle stemmesedler") have braille print and some larger print than the other paper ballots used in Norway. This allows the blind and partially sighted in many cases to vote unassisted, something which is vital for secret voting. However, it is not only the blind and partially sighted that read braille, and not all municipalities allow for the use of general ballot papers (Saglie et al., 2022). General ballot papers also do not support cumulative voting.

Furthermore, for groups with special needs, having difficulties of going to polling stations, a paper-based system which requires voting at a polling station, will also not be favourable. It is therefore our assessment that paper-based systems meet the criterion of inclusion to some extent.

7.3 Electronic systems

7.3.1 Usability

The criterion of usability concerns the fact that the voting system shall be simple to understand and use for voters. An advantage of electronic systems is that they are interactive. In this manner, voters can be told automatically if they made a mistake during the voting process. This may help to prevent votes from being discarded because of an incorrectly filled-out paper ballot, which happens to a certain degree under paper-based systems. For the 2021 parliamentary election, 4 517 votes were discarded. As described in chapter 5.2.6, many votes are discarded because

[15] Note, in the analysis we take our basis in the part of the election where votes are cast in the polling station.

voters use ballot papers as envelopes for their own ballots. This is not a problem for electronic systems.

However, it can be difficult for groups with lower IT skills to use electronic voting systems, and since voting takes place in polling stations, going there can be a barrier for some voters.

Overall, for electronic systems there is a trade-off between the challenges faced by voters with low IT skills, and those advantages that interactive solutions may provide. It is therefore our assessment that electronic systems meet the usability criterion to some extent.

7.3.2 Inclusion

The criterion of inclusion concerns the usability of voting systems for groups with special needs, as well as how the system allows for unassisted voting. There are two things that are particularly relevant for the assessment of the usability of electronic systems for groups with special needs.

Firstly, electronic systems can be interactive and facilitate the use of aids. This can make the solution more user-friendly and understandable to use than paper-based systems, something shown by trials in this area (van Eijk et al., 2019). Partially sighted voters have a desire to use aids and adapted solutions that can improve the voting process (NOU 2020: 6).

However, there is uncertainty as to what degree electronic solutions actually do facilitate unassisted voting. A group that can vote unassisted using electronic solutions are voters that use ordinary paper ballots, but who want to cast a cumulated vote, something general ballot papers do not allow for. Another group is partially sighted and blind people who do not use braille, but use aids that electronic solutions can facilitate the use of. The challenge is to develop electronic solutions that allow this. Blind and partially sighted people may be dependent on PCs with specific software and aids they are familiar with in order to vote in this way. It will be challenging to set up and facilitate all variations of necessary aids in controlled surroundings.

Secondly, electronic systems in polling stations will also involve travelling, which will particularly affect some groups with special needs.

Overall, it is our assessment that electronic voting meets the inclusion criterion to some extent. However, it is worth to emphasise that electronic systems can be designed in ways that contribute to better usability for people with special needs in certain cases compared to paper-based voting.

7.4 Internet-based systems

7.4.1 Usability

The criterion of usability concerns the fact that the voting system shall be simple to understand and use for voters. As with electronic systems, internet-based systems can be made interactive with the advantages this brings along. Another advantage of internet-based systems is that they remove potential barriers related to commuting, something which will be particularly favourable for voters in rural areas with long commutes or voters abroad who need to travel to an embassy. Studies have shown that simplicity is an important factor for voters who choose to vote over the internet (Segaard et al., 2014). In Estonia, a larger proportion of voters have started to use the internet-based solution over time instead of paper-based alternatives (Ehin et al., 2022).

Segaard et. al (2014) point out that it has been discussed by the media and among the public that internet elections contribute to increased voter turn-out, but that research literature does not have the evidence to back this up. They investigated how voter turnout was impacted by the opportunity to vote over the internet during the trial election in 2013. In line with earlier research results, they did not find that the trial of voting over the internet led to increased voter turnout.

The challenge of usability of internet-based systems is the accessibility to voters with lower technical skills. These challenges are also present in electronic systems, but the challenges are likely greater for internet-based systems. The reason for this is that it is more difficult to offer guidance when voters do not vote in polling stations.

With all this in mind, it is our assessment that internet-based systems meet the criterion of usability to some extent.

7.4.2 Inclusion

The criterion of inclusion concerns the usability of voting systems for groups with special needs, as well as how the system allows for unassisted voting. As previously explained, a key condition is whether the voting solution allows for interactive solutions, facilitates the use of aids and whether there is a low travel barrier.

The assessment of inclusion for internet-based systems is largely the same as for electronic systems, if slightly better. As described under the assessment of inclusion in electronic systems, the blind and partially sighted may be dependent on PCs with specially adapted software they are familiar with. Internet-based systems can potentially be designed so that the use of

specialised aids can be used during voting, and thus allow for unassisted voting within this group.

In general, there has been limited research on disabled people and groups with special needs use of internet-based solutions (Fuglerud & Røssvoll, 2012), however, it is our overall assessment that internet-based systems meet the inclusion criterion to a great extent.

7.5 Usability of end-to-end systems

In some of the assessments above, we have outlined end-to-end electronic and internet-based systems as alternatives to classic systems. The use of end-to-end systems, either electronic or internet-based, is closely related to the usability of the system. The guaranteed integrity that such systems provide assume that the individual voter takes responsibility for checking that the vote has been correctly registered and to challenge the system by casting control ballots. In practice, it has emerged that voters have problems understanding the point and use of the systems in practice. A trial of three different end-to-end systems (Helios, Prêt à Voter and Scantegrity II) showed that voters found them "exceptionally difficult" to use in practice, they either use paper ballot papers or do not, with only 58 percent of votes being successfully cast (Acemyan et al., 2014). Another investigation showed that depending on which method of verification was used, 61.3 percent and 81.3 percent of first time voters respectively were able to verify that their vote was correctly cast, even though everyone was convinced that it had been (Marky et al., 2018).

A further study on the electronic end-to-end system vVote concluded that it was extremely easy to use (Burton et al., 2016). With such a large gap in results, there are grounds to further examine the methods used. A reasonable explanation is that while all the studies recorded how easy the voters thought the system was to use, it was only the former study that actually measured how many votes were successfully cast. So, there is reason to believe that the latter has significant methodological weaknesses.

With all this in mind, there is good reason to question the usability of end-to-end systems.

8. Resource use

Resource use concerns what is required in terms of human and financial resources for the introduction and operation of electronic and internet-based voting systems as a supplement to the current paper-based election process. For municipalities, the introduction of electronic voting systems will likely be the most resource-intensive, while for the state, it will likely be more resource-intensive to implement a system for internet-based voting. In this chapter, we provide a more detailed description of the factors that affect resource use.

8.1 Primary findings: Resource use

In our assessment of security, transparency and auditability, and usability and inclusion, we have assessed conditions related to paper-based, electronic and internet-based systems in isolation. However, if e-voting is to be adopted, it will likely be as a supplement to the current paper-based election process. Figure 8-1, which summarises our assessments related to resource use, therefore shows our assessments of the resources that will be required, at both a local and central level, for the introduction of electronic and internet-based systems as a supplement to the current paper-based election process.

In the short term, it will naturally be a lot more resource-intensive to operate a paper-based and an electronic electoral system at the same time rather than just one paper-based system. The costs will be reduced in the long-term, but it is more likely that a partial introduction of e-voting will also be more resource-intensive in the long-term than continuing with just the current paper-based system.

A partial introduction of electronic voting will be resource-intensive, both for municipalities and for the state. For municipalities, the costs come from the procurement and operation of voting machines.

Internet-based solutions may be viewed in many respects as a way of saving resources for municipalities. A large portion of the costs here will be borne by the state. The solutions are demanding in terms of system development and security, something which affects costs for both *Materials, equipment and systems* as well as *Staffing*.

Figure 8-1: Assessment of resource use against the current paper-based election process

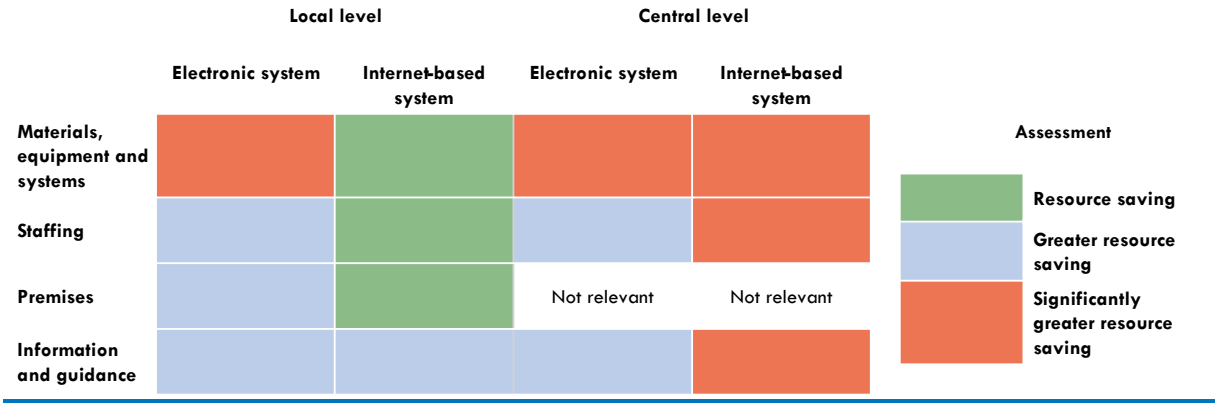


Illustration: Oslo Economics and Norwegian Computing Centre

8.2 Electronic system

We assume that the financing of the development of solutions for electronic voting will take place at a national level. This was also recommended by the knowledge acquisition for electronic voting from 2006 (Kommunal- og regionaldepartementet, 2006). The reason is based on the fact that there are benefits related to economies of scale for developing solutions centrally.

8.2.1 Resource use at the local level

For municipalities, the introduction of electronic systems as a supplement to the current paper-based election process will be resource-intensive. Even though it is reasonable to assume that the state will cover the costs of developing the systems, it is municipalities that will have to procure and operate the voting machines. There is comparatively large range of different types of voting machines. Different solutions for electronic voting range from ordinary computers to advanced voting machines. Accordingly, procurement costs vary

to a large degree. Voting machines used in India can cost around NOK 2,000, while machines used in the USA may have a price tag of several hundred thousand Norwegian kroner (Wolchok et al., 2010).

In addition to the cost of the systems, it is likely that further adaptations will need to be made to the premises used for elections by municipalities. Electronic voting machines may, for example, entail huge requirements for network infrastructure to/from the premises.

As for staffing, it is assumed that there will be no major changes to the need for election officials. It may be that the use of electronic credentials may lead to time savings in the receipt of votes compared to the current solution when providing identification, but the impact is regarded as being extremely limited. However, more resources will need to be used for training so that election officials can provide aid to voters wishing to vote electronically, and the scope of the information efforts in advance of the election are likely to increase.

In addition to election officials, municipalities will likely need to employ or enter into agreements with persons who can offer assistance if problems arise with the machines during the election process.

The fact that introducing electronic elections as a supplement to paper-based elections can be costly is supported by experiences of electronic elections in England (Christensen et al. 2004).

8.2.2 Resource use at the central level

The introduction of electronic systems means that the state must develop a system for voting, counting and registering votes. Implementing this process will in itself be resource-intensive. In addition, there will be a need for coordination and signing of agreements for the sale and distribution of voting machines to municipalities.

Furthermore, the introduction of electronic voting will lead to changed functionality of the EVA Admin. This will be as a result of the process of registering ballot papers being automated, and EVA Admin must be adapted to the amended voting process. EVA Scanning and scanning solutions are not relevant for most electronic systems since the voter does not use a physical ballot paper.

The need for informational campaigns aimed at voters will also increase from a central site. Electronic solutions will be more difficult to understand for voters, as discussed in Chapter 7. Informational campaigns should include descriptions of the practical implementation of voting. Furthermore, it may be desirable to communicate the built-in security mechanisms of the system architecture to ensure transparency of the solution.

We also expect that municipalities will have an increased need for information for electronic systems and an increased need for training from the Norwegian Directorate of Elections.

8.3 Internet-based systems

A key factor of internet-based solutions is that a range of practical work tasks are transferred from a local to a national level. This is because internet-based solutions are largely based on centralised solutions. This is described in-depth in Chapter 3.

8.3.1 Resource use at the local level

Internet-based solutions result in a reduced resource use for municipalities than electronic solutions. Studies support this, indicating that internet-based solutions are a less costly alternative than other voting systems (Krimmer et al., 2018, 2021). However, there is a limited number of studies in this area.

Since voting does not take place in controlled surroundings for internet-based voting systems, the votes are sent to a central ballot box, and as a result there is no local counting of votes or a need to adapt premises.

If the scale of internet voting was expanded, it may reduce municipalities' need for staffing in the long term for both the receipt and counting of votes. However, it may be necessary to have a form of locally accessible service personnel if technical issues should arise. For an important event such as an election, a national service centre will not necessarily be regarded as sufficient. There may be a number of voters who need in-person support to come and examine the actual issue.

8.3.2 Resource use at the central level

The introduction of an internet-based system means that the state must develop the system and have it adapted to both local conditions and the central election management system, EVA.

Compared to electronic systems, it is reasonable to assume the system development process will be more demanding. The threat landscape is greater for internet-based systems, which places greater demands on the security of the solution. Furthermore, authentication will be a key issue in the design of any internet-based system, and it will probably be demanding in both a technical and an organisational sense. Of the existing solutions for electronic credentials in Norway, BankID is a relevant alternative, but even in cases where authentication is based on existing solutions, it is expected that it will

be necessary to make adaptations to them to work in a voting system with the requirements this entails.

With internet-based system, it will not be necessary to coordinate and enter agreements for the sale and distribution of voting machines for municipalities. On the other side, the location of the ballot boxes and location of the counting is centralised. This will require the state to set up a central electronic storage site. In practice, this will typically be a central server in a data centre.

We therefore assume that the costs related to systems will be greater for internet-based systems compared to electronic ones. We also assume that the information requirements aimed at voters will increase from a central site.

When it comes to municipalities, there will be a needed for different type of training and guidance, compared to electronic systems. This is a result of the fact that municipalities do not have the same work tasks related to internet-based systems as for electronic ones. However, even though there only a few tasks when viewed in isolation, there may be a need for municipalities to assist voters and offer a degree of guidance in this area.

9. Summary assessment of risks, benefits and costs

The knowledge acquisition has discovered that there are a range of potential solutions for electronic voting. The risk for both electronic and internet-based voting systems is primarily related to security, while the potential benefits lie in better inclusion of groups with special needs. The knowledge acquisition does not provide a basis for drawing a specific conclusion as to what should be given the most weight of these considerations.

9.1 No system is perfect

The analysis shows that none of the three main categories of voting systems are better than the two other systems across all factors. The current paper-based system is the only one to satisfy the criteria for anonymity, vote integrity, correctness, transparency and auditability to a great extent, while internet-based systems are the only ones to satisfy the criterion for inclusion of groups with special needs to a great extent.

The differences between the systems reflected in the analysis are not primarily the result of how far technological developments have come, or how the systems are currently designed. In the future, it will likely be challenging to meet the criteria for the inclusion of groups with special needs with the current paper-based electoral system, and it will not be possible to fully guarantee the security of electronic and internet-based systems.

9.2 Risks of electronic and internet-based voting

The analysis of the security of different technical solutions for electronic voting have discovered that it is not currently possible to design technical solutions that can fully guarantee the security of the election process in the same way as paper-based systems. The challenge is related in particular to scalable attacks and attacks that are difficult to discover, or where it is likely that they will not be discovered. Furthermore, the major centralisation factor also poses a risk. End-to-end electronic systems have centralised vote handling, while internet-solutions are fully centralised, which poses a system vulnerability. Furthermore, there is a vulnerability in that there only a few specialists that fully understand the workings of the system.

The knowledge acquisition has discovered that assessments related to security aspects of electronic voting have a different backdrop today than previously. Many of the overall assessments are still the same today as those a working group set up by the then Ministry of Local Government and Regional Development concluded with in the 2006 report *Electronic voting – challenges and opportunities* (Kommunal- og regionaldepartementet, 2006).

Since 2006 and since the e-election trials in Norway in 2011 and 2013, there have been significant developments on the technology side, and digital solutions have become even more prominent. Many key societal functions are largely digitalised, and it is therefore relevant to ask whether or not the technology now makes it possible to guarantee the security of electronic voting systems.

To answer this question, it is relevant to examine the development of the security of electronic voting systems in the context of the development of data security in general in recent decades in Norway. Over the years, there have been very little that changes the basic conditions for how we work with security. An exception is perhaps the so-called "self-sovereign identity" (SSI). SSI means that the individual user issues their own decentralised digital identity and has full control over credentials that are issued to themselves and related to this identity. Electronic voting has been put forward as an area that can make use of SSI (Preukschat & Reed, 2021). However, SSI is so new that it probably will not be of any practical significance for many years yet. In general, it typically takes many decades before a discovery of fundamental significance becomes widespread and has practical consequences. It may therefore be appropriate to examine which technologies or practices have become widespread in recent years.

An example of a general trend that points towards an increased level of security is the steady expansion of two-factor authentication. This is a type of authentication that uses two authentication methods in combination. An example of this is BankID, where both a code generator and fixed password are used. It also more common that data is encrypted during transfer: unencrypted webpages are less common today than encrypted ones. On some platforms, it has become common to use more sophisticated systems of access control (so-called mandatory access control), something which generally limits the consequences of malware. When it comes to organisational changes, it has become more common, especially amongst larger

organisations, to have a security management system, such as ISO 27001.

Even though security of the systems has become better when viewed in isolation, systems remain exposed to increasingly sophisticated threats. The Confederation of Norwegian Enterprise publishes a report every other year, the Mørketallsundersøkelsen (Hidden Statistics Report), which concerns the condition of data security of Norwegian organisations. Both public bodies, such as the Norwegian National Criminal Investigation Service (Kripos), the Norwegian Police Security Service (PST) and the Norwegian National Security Authority (NSM), and private actors such as Norman, Mnemonic and Microsoft contribute to the analysis. Over the period 2012 to 2022, there has been an increase in digital operations from threat actors against Norwegian targets. This includes companies that fulfil important societal functions, particularly within sectors such as the armed forces, aerospace, maritime, petroleum, energy, transport, research and higher education, electronic communication and health.

Threat actors can both be state-funded and criminal actors, and the motives include personal gain, espionage and sabotage. These threat actors are becoming both more selective in their targets and more advanced in their methods, such as, for example:

- value chain attacks (supply chain attacks) – attacks against suppliers, partners and other third parties as a part of achieving a specific goal.
- spear phishing – CEO fraud
- ransomware
- extortion using DDOS attacks
- identity theft

The election process is a relevant target for digital operations. An investigation of whether foreign actors tried to influence the 2021 Norwegian parliamentary election has been carried out (Sivertsen et al., 2022). There was no indication that foreign actors tried to influence the election result, voter turnout or trust in the election. However, the findings of the report do show that informational influence against democracies is taking place to a significant extent. These unlawful activities are often subtle and are of a low intensity over long periods time. Probably the most known example of state actors influencing elections in other countries is Russia's actions in the presidential elections in the USA in 2016 and 2020. The National Intelligence Council, a US intelligence service, concluded in an investigation of foreign influence in the 2020 election that Russia did not try to change any technical aspects of the election process (National Intelligence Council, 2021). This covers the election process with voter registration, voting and counting. On the other hand, they found that there were widespread campaigns aimed against American voters with the aim of undermining voters' trust in the election process, and moreover increase socio-political differences.

Another development in data security related to electronic voting specifically concerns the relationship between mobile phones and personal computers. After the turn of the millennium, the difference between mobile phones and computers has become smaller and smaller, and many people use their mobile phone for tasks they would have previously used a computer for. For example, many people read text messages on laptops, and many use browsers on mobile phones. The internet-based solutions that were used in the Norwegian trial in 2013 used solutions based on an independency between mobile phones and computers for casting votes, but this may be a less relevant assumption in retrospect (Gjøsteen, 2013).

If you listen to data security and internet attack experts, the conclusion will be that it will never be possible to fully guarantee the security of digital voting systems. This is because the technological developments are happening so quickly that the authorities and technology experts will find it difficult to create a system that can withstand or prevent an attack with approximately 100 percent certainty. In practice, this means that the security ultimately rests on the possibility of detecting and responding to attacks and having good manual emergency procedures and measures (NOU 2020: 6).

9.3 Fundamental differences between voting systems

Even if it were possible to guarantee the security of electronic and internet-based systems, there would be fundamental differences between systems in other areas. This applies in particular between the current paper-based electoral systems, which takes place in controlled surroundings, and internet-based elections in uncontrolled surroundings.

In the introduction of the report, we describe how the Election Act Commission has issued the following principles for the Norwegian electoral system:

- The election shall be free.
- The ballot shall be secret.
- The election shall be direct.
- The right to vote shall be universal and equal.
- Elections shall be held periodically.
- Everyone with the right to vote shall have the opportunity to vote.
- Everyone with the right to vote shall be able to be elected.
- Each vote shall have equal weight.

- The electoral system shall ensure geographical representation.

The differences between elections in controlled surroundings and internet-based elections in uncontrolled surroundings become particularly clear in the principle that the ballot shall be secret.

As discussed in Chapter 7, it is only internet-based systems that fulfil the criterion for inclusion of groups with special needs to a great extent. This is related to the fact that internet-based systems enable unassisted voting for the blind and partially sighted. The current Norwegian electoral system allows for the blind and partially sighted to choose for themselves who should accompany them into the polling booth. Compared to the previous system, where election workers had to accompany them, this is regarded as an improvement. However, the ballot is still not secret if we assume an extreme interpretation of this principle.

Allowing for internet-based voting, however, creates other challenges for the principle of a secret ballot. Under the category of security in Chapter 5, we showed that internet-based systems satisfy the *anonymity* criterion to a limited extent. By voting in uncontrolled surroundings, the system in itself does not provide a guarantee that no one else is observing the ballot, and there is thus no guarantee of a secret ballot.

Internet-based voting also challenges the principle that the election shall be free. If voting can be observed by others, the risk that a voter may be coerced by someone else to vote in a specific way increases. As described in Chapter 5, it is possible to design the system in such way that the voter can change their vote until the deadline for voting passes, which reduces the risk of the use of coercion. This risk is reduced if internet-based voting is introduced as a supplement to paper-based elections, and, for example, be limited to the early voting period. Then systems can be designed so that cast paper votes on election day take priority over votes cast electronically during the early voting period.

The principle of a secret ballot is vital in Norway, and as uncovered by this knowledge acquisition, it is not clear which voting systems best protect this principle. However, it is relatively clear which groups cannot cast a secret ballot in Norway today: the blind and partially sighted. An alternative that has been presented is therefore to allow for internet-based voting for this group only.

The Election Act Commission (NOU 2020: 6) discussed the introduction of electronic voting for people with disabilities. Starting with internet-based solutions, the advantage of this is that it provides the blind and partially sighted the opportunity to vote alone weighed up against the challenges of secret ballots. The Commission believed that electronic voting at the polling station would make it possible for people with visual impairment to vote alone (NOU 2020: 6). The knowledge acquisition has uncovered that there are practical challenges in developing electronic solutions that allow for unassisted voting, and that it is probably only internet-based systems that allow for unassisted voting for the blind and partially sighted.

We have not further examined the financial and organisational resources required to set up such a solution, but we do see that a partial introduction in this way has both practical and principle aspects that are important to be clear on. Firstly, there is a challenge deciding who should be allowed to vote electronically or not. Secondly, there must be a collection and handling of votes in place that protects the principle of a secret ballot. In smaller municipalities, there will only be a small number of voters, perhaps only one, who qualifies to use electronic voting. In this case, the electronic votes cannot be counted together with the ordinary ballot papers. The votes must be sent to a central register in such a way that it is not possible to track how the individual voter has voted.

9.4 Costs for the state and municipalities

In the knowledge acquisition, we have assessed the resource use for the state and municipality for the use of electronic and internet-based systems for voting as a supplement to the current paper-based electoral system.

In the short term, it will naturally be a lot more resource-intensive to operate a paper-based and an electronic electoral system at the same time rather than just one paper-based electoral system. The costs will be reduced in the long-term, but it is more likely that a partial introduction of e-voting will also be more resource-intensive in the long-term than continuing with just the current paper-based system.

A partial introduction of electronic voting will be resource-intensive, both for municipalities and for the state. For municipalities, the costs come from the procurement and operation of voting machines.

Internet-based solutions may be viewed in many respects as a way of saving resources for municipalities. A large portion of the costs here will be borne by the state. The solutions entail major demands for system development and security.

The introduction of electronic voting will also entail completely different skill requirements than the municipalities currently have. Even with extensive use

of hired expertise, there will likely be a need for skills development in municipalities, and there will be a need regardless to provide election officials with more training. This applies in particular to electronic systems, where voting machines are place in polling stations, but also for internet-based systems, it is likely that municipalities will have to offer some form or another of support to its citizens.

9.5 Summarised reflections

The fact that it is not possible to guarantee the security of electronic solutions entails a risk of a loss of trust. The Election Act Commission points out that if security around the election process is weakened, it will have very serious consequences for the election as a central democratic process, confidence in the election process and the election result. Weakened trust in the election process is not dependent on an actual security breach. The mere perception amongst parts of the population of doubt in the validity of the election result could impact trust in the election process and the election result. One option to ensure better accessibility for more people, while also limiting the risk of a loss of trust, is to open up electronic voting to only selected voter groups. Not because their vote is less important, but because a security breach will have lower economic and social costs in the form of reduced trust the fewer votes it affects.

There are variations between how a country's authorities and how its voters view electronic and internet-based voting systems. Weighing up between potential benefits related to usability and inclusion and the risk related to security depends to a large extent on country-specific conditions and conditions related to the existing electoral system. Personal preference is also significant. Some people may be willing to accept the security risk inherent in using electronic systems in exchange for an election process that is better suited to voters with special needs. Others have the opposite opinion to this.

In summary, experiences from other countries shows that there are a range of opportunities when it comes to introducing electronic voting. The risk is primarily related to security, while the potential benefits lie in better inclusion of groups with special needs.

10. References

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. (n.d.). *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. (n.d.). *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 kommunestyrer (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

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., & Krivonosova, 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., Krivonosova, 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

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 kommunestyrer (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 Blindeforbund. (2021). *Tilrettelegging for valgdeltakelse*. Norges blindeforbund. https://www.blindeforbundet.no/om-blindeforbundet/nyhetsarkivet/tilrettelegging-for-valgdeltagelse-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 Preˆt 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., & Segaard, 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

Segaard, S. B., Baldersheim, H., & Saglie, J. (2012). *E-valg i et demokratisk perspektiv*. Institutt for samfunnsforskning.

Segaard, 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. Tilgjengelighten 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). Europaårdet. I *Store Norske Leksikon*. https://snl.no/Europar%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

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

Annex A Events and risk

We make a distinction between intentional events, unintentional events and adverse events. We present them below. We should point out that we do not expect this list to be exhaustive, it merely illustrates the risk landscape.

10.1.1 Intentional events

- One voter pretends to be another voter.
  - The voter uses false credentials to vote on behalf of another person.
  - The voter uses borrowed credentials to vote on behalf of another person.
- Another person is with the voter when they are to cast their vote. This may be an assistant there in the polling booth in a polling station, or a person watching on the screen.
- Family, friends or people known to the voter pressure them into casting a different vote than what they want themselves by watching them as they vote.
- The voter does not receive confirmation (implicitly, explicitly or end-to-end confirmation) of the vote cast.
- An attacker has corrupted the source code of an operating system or library for a specific browser or a dedicated voting programme to change each vote cast.
- An attacker has corrupted the source code of an operating system or library for a specific browser or a dedicated voting programme to see how individuals have voted.
- Votes in the ballot box are changed:
  - Ballot boxes are lost or stolen.
  - Cast votes are changed.
- Votes in the ballot boxes are read and counted. The result may be published in advance.
- An attacker reads the cast electronic votes, which are stored on a storage device, which includes the ballot box or other storage device for the count.
- An attacker is able to see how individual voters have voted.
- During manual or electronic vote counting, a disloyal election worker changes votes.
- Counting machines are corrupted and count incorrectly.
- An attacker corrupts the e-voting system so that it delivers incorrect local results.
- An attacker changes the total number of votes in a local result when it is added to the centralised overview.
- A disloyal worker changes the total number of votes in a local result when it is added to the centralised overview.

10.1.2 Unintentional events

- The polling station is subject to a serious event. For example, this may be a fire, flood, earthquake, power outage, lack of ballot papers.
- Due to poor technical implementation or routines, the votes are lost during the process.
- Election workers count incorrectly.

10.1.3 Adverse situations

- The voting procedure is so difficult to understand that voters are not able to cast their vote or do something meaning that their vote is invalid.
- The procedure of registering to vote is so difficult to understand that voters are not registered.
- Voters have disabilities. A barrier which has the consequence that the voter is not able to vote.
- Only a small number of experts understand how the voting system works.
- It is not possible to observe what is happening to ballot papers and votes in the process.

oslo economics

www.osloeconomics.no

Email and telephone:
post@osloeconomics.no
+47 21 99 28 00

Street address:
Klingenberggata 7a
0161 Oslo

Mailing address:
Post box 1562 Vika
0118 Oslo