NTNU – Trondheim
Norwegian University of
Science and Technology

The Norwegian electoral system: a study of EVA Skanning, implemented error detection mechanisms, and applicability of risk-limiting audits

Vilde Elise Samnøy Amundsen

Submission date: January 2019
Responsible professor: Stig Frode Mjølsnes, IIK
Supervisor: Patricia Aas, TurtleSec AS

Norwegian University of Science and Technology
Department of Telematics

Abstract

The Norwegian electoral system is defined by a combination of manual and computerised processes. The voting itself is a manual process where the voter submits a paper ballot into an urn. All preparatory work and ballot counting, however, are simplified using the computer system *Elektronisk Valgadministrasjonssystem* (EVA). Prior to the election in 2017, there were speculations related to possible security vulnerabilities within the computer system, specifically the electronic ballot counting system, EVA Skanning. In addition, there were speculations related to non-reliable error detection mechanisms.

Complex software systems are notoriously difficult to secure and cannot be guaranteed to be perfect or secure. Therefore, a technology-dependent electoral system must implement reliable error detection mechanisms. A reliable error detection mechanism is defined as a mechanism that enforces *software-independence*. Software-independence means that an undetected error in software is incapable of causing an undetectable error in the election outcome. The concept of *risk-limiting audit* is considered best-practice for error detection in electoral systems, and enforces software-independence by manually examining the audit trail (e.g. paper ballots) strategically, and stops when the audit yields sufficient evidence of correct result. Risk-limiting audits are not currently implemented in the Norwegian electoral system.

The objectives of this master's thesis are to research the level of security within EVA Skanning, assess the reliability and performance of the currently implemented error detection mechanisms in the Norwegian electoral system, and analyse if, and how, risk-limiting audits should be applied. Mixed methods research is performed in form of semi-structured interviews with system engineers, operators, and managers, experimental testing of EVA Skanning, and a qualitative analysis of risk-limiting audit algorithms. The thesis provides methodology for the conducted research, corresponding results and discussion, and finally, conclusive remarks.

The main findings indicate that EVA Skanning is not sufficiently secured. Choice of architecture and protocols are not entirely motivated by security, but rather by practical considerations. The findings also show that the reliability of the currently implemented error detection mechanisms is low. The primary error detection mechanism is to compare the manual and electronic ballot counting result. Given deviation, a recount is performed electronically. An electronic recount undermines the manual result, and

thereby justifies two electronic counts. Due to poor security and low reliability of error detection performance, risk-limiting audits should be applied to the Norwegian electoral system. Two algorithms are discussed in this master's thesis: *ballot-polling audits* and *comparison audits*. Of the two, comparison audits are considered to be the most appropriate algorithm.

Sammendrag

Det norske valgsystemet er definert som en kombinasjon av manuelle og maskinelle prosesser. Stemmegivningen i seg selv er en manuell prosess, der den stemmeberettigede legger en stemmeseddel manuelt i en urne. Alt forberedende arbeid og stemmeseddeltelling, derimot, blir simplifisert ved bruk av datasystemet *Elektronisk Valgadministrasjonssystem* (EVA). Før valget i 2017 var det spekulasjoner relatert til mulige sikkerhetssårbarheter ved datasystemet, hovedsakelig ved det elektroniske stemmeseddeltellesystemet, EVA Skanning. I tillegg var det spekulasjoner knyttet til ikke-pålitelige mekanismer for å oppdage feil.

Komplekse programvaresystemer er notorisk vanskelig å sikre, og kan ikke garanteres å være fullstendig sikre. Derfor må et teknologiavhengig valgsystem implementere pålitelige mekanismer for å oppdage feil. En pålitelig mekanisme for å oppdage feil er definert som en mekanisme som sikrer *programvareuavhengig*. Programvareuavhengighet betyr at en uoppdaget feil i programvaren er uegnet til å forårsake en uoppdagbar feil i valgresultatet. Konseptet *risiko-begrensende revisjoner* er sett på som den beste metoden for å oppdage feil i valgsystemer. Konseptet sikrer programvareuavhengighet ved å manuelt undersøke revisjonsstien (f.eks. papirstemmesedler) strategisk, og stopper når revisjonen gir tilstrekkelig bevis for riktig resultat. Risikobegrensende revisjoner er foreløpig ikke implementert i det norske valgsystemet.

Målene med denne mastergradsoppgaven er å undersøke sikkerheten til EVA Skanning, vurdere påliteligheten av det norske valgsystemets nåværende mekanismer for å oppdage feil, og analysere om og hvordan risikobegrensende revisjoner burde implementeres. Blandet metodeforskning er utført i form av halvstrukturerte intervjuer med systemingeniører, operatører og ledere, eksperimentell testing av EVA Skanning, og en kvalitativ analyse av revisjonsalgoritmer. Oppgaven presenterer metodikk for de gjennomførte undersøkelsene, tilsvarende resultater og diskusjoner, og til slutt, avsluttende bemerkninger.

Hovedfunnene indikerer at EVA Skanning ikke er tilstrekkelig sikret. Valg av arkitektur og protokoller er ikke entydig motivert av sikkerhet, men heller av praktiske hensyn. Funnene indikerer også at påliteligheten til eksisterende mekanismer for å oppdage feil er svak. Hovedmekanismen for å oppdage feil er å sammenligne det manuelle og elektroniske resultatet. Gitt avvik, blir det gjennomført en elektronisk omtelling. En elektronisk omtelling undergraver det manuelle resultatet, og dermed rettferdiggjør

to elektroniske teller. Grunnet dårlig sikkerhet og lav pålitelighet knyttet til mekanismer som oppdager feil, bør risikobegrensende revisjoner innføres i det norske valgsystemet. To algoritmer diskuteres i denne mastergradsoppgaven: *ballot polling audits* og *comparison audits*. Av de to, anses comparison audits som den mest hensiktsmessige algoritmen for det norske valgsystemet.

Preface

This thesis has been submitted to fulfil the graduation requirements of the M.Sc. in Communication Technology at the Norwegian University of Technology and Science (NTNU). The main research and writing were carried out between September and December 2018.

The objectives of this master's thesis are to research the level of security within EVA Skanning, assess the reliability and performance of the currently implemented error detection mechanisms in the Norwegian electoral system, and analyse if, and how, algorithmic correctness verification methods (risk-limiting audits) should be applied.

The greatest appreciation is shown to my supervisor Patricia Aas for her invaluable contribution, and to professor Stig Frode Mjølsnes for great support and contribution to the project. Also, special thanks to the Directorate of Elections for graciously answering questions and sharing their knowledge. Finally, gratitude is expressed to all election officials that participated in the study.

Vilde Elise Samnøy Amundsen
Bergen, 30th of January 2019

Contents

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Introduction

The Norwegian electoral system is defined by a combination of manual and computerised processes. Prior to an election, all necessary ballot paper and polling card information is registered electronically. When a voter arrives at a polling station on Election Day, the voter may be checked off using an electronic poll book. Next, the voter selects a paper ballot of their desired party, and manually submits the ballot into an urn. Finally, the ballots may be counted manually by hand or electronically using a scanner. The result is registered electronically and published on a website.

The Directorate of Elections has developed a state-owned computer system for the computerised processes listed in the previous paragraph. The system is called *Elektronisk valgadministrasjonssystem* (EVA), and consists of three modules: EVA Admin (an administrative application for preparatory work and electronic poll book), EVA Skanning (an electronic ballot interpretation and counting system), and EVA Resultat (a website for publication of the result), see Appendix A.

Prior to the parliamentary election in 2017, a debate regarding the security of EVA was brought to the public's attention. First, it was questioned whether the scanners used for electronic ballot counting were connected to the Internet [SC17b]. Second, concerns related to poor error detection performance for result manipulation were discussed. Pursuant to § 10-4 (5) of the Election Act, all ballots must be counted at least twice to ensure result integrity. The Act, however, does not specify *how* the ballots shall be counted. The municipalities are free to decide how they wish to count, manually and/or electronically. The concerns were directed towards how result manipulation can be detected if both counts are performed electronically [SC17b]. Third, a browser update resulted in three certificates related to authentication of EVA Admin, became publicly available on the Internet. Although the certificates were not sufficient authentication alone, the certificates were deactivated when the information became public [SC17a]. Collectively, these vulnerabilities led the public

to question the integrity of the election result.

11 days before the election in 2017, the Minister of Local Government and Modernisation at the time, Jan Tore Sanner, stated in a press release that all ballots had to be manually counted at least once to ensure integrity of the result [HCE17]. The decision was justified by the speculations in the media related to possible security vulnerabilities, and the Ministry wished to emphasise that public could in fact trust the electoral system. The regulation was, however, only applicable for the election in 2017. Whether mandatory manual ballot counting will be implemented in future elections, is currently on hearing, see Appendix B.

1.2 Scope of the thesis

An electoral system is the most important instance of a democratic society. Therefore, in a technology-dependent electoral system, information security must be prioritised. A technology-dependent electoral system must implement a certain level of security to prevent "mainstream" attacks, such as man-in-the-middle attacks, evil-maid-attacks, and denial-of-service attacks. This master's thesis aims at researching the level of security within EVA Skanning, the Directorate's solution for electronic ballot counting. EVA Skanning is selected due to being a complex installation, and an obvious target for result manipulation.

Professor Matt Blaze argues in a hearing on technology used in elections in the U.S. [CYB17], that complex software systems are notoriously difficult to secure, and one cannot guarantee that a computer system is perfectly secure. All electoral systems that implement computer software and hardware, therefore require reliable error detection mechanisms. According to Lindeman et al. (2012) [LS12], a reliable error detection mechanism is defined as a mechanism that enforces *software-independence*. Software-independence means that an undetected error in software is incapable of causing an undetectable error in the election result [Riv08]. In a time where election manipulation is payed more attention, mechanisms for detecting such manipulation are imperative. In addition to researching the level of security in EVA Skanning, this master's thesis studies currently implemented error detection mechanisms in the Norwegian electoral system and assesses the reliability of these mechanisms.

The concept of *risk-limiting audit* is considered best-practice for reliable error detection in electoral systems. According to Goodman et al. (2012) [GCJ+12], risk-limiting audits enforce software-independence by manually examining portions of the audit trail strategically (i.e., select ballots at random, and stop when the audit yields sufficiently strong evidence of correct result). Risk-limiting audits are not currently implemented in the Norwegian electoral system. This master's thesis researches whether there is a need for risk-limiting audits, and how to apply such an algorithm

to the Norwegian electoral system.

1.3 Objectives and research questions

The objectives of this master's thesis are to research the level of security within EVA Skanning, assess the reliability and performance of the currently implemented error detection mechanisms in the Norwegian electoral system, and analyse if, and how, risk-limiting audits should be applied. Based on the objectives, three research questions are derived:

1. How is EVA Skanning architecturally structured and secured?
2. How are counting errors detected in the Norwegian electoral system?
3. How can risk-limiting audits be applied to the Norwegian electoral system?

1.4 Introduction of EVA Skanning

EVA Skanning is the Directorate of Elections' solution for electronic ballot counting in the Norwegian electoral system. EVA Skanning offers to administrate, interpret, verify, and count paper ballots cast in elections. *Boken om EVA Skanning* [Val15] provides a thorough understanding of the EVA Skanning module used in 2015. More recent documentation has not been published.

EVA Skanning consists of three Windows applications: EVA Jobbstyring, EVA Skann, and EVA Verifiser, with associated hardware, and a database server. A high-level view of the components are illustrated in Figure 1.1. All components of the EVA Skanning module are installed locally in the municipals, and the municipals themselves are responsible for securing the installation [Val15].

In this chapter, the components of the module are introduced. Further description of architecture and level of security is provided in Chapter 3.

1.4.1 EVA Jobbstyring, EVA Skann, and EVA Verifiser

EVA Skanning consists of three Windows applications and a database server. The three Windows applications are:

1. **EVA Jobbstyring:** a "dashboard application" used for administrating the scanning. The main functions of EVA Jobbstyring is to start, supervise, finish, and transfer results. EVA Jobbstyring transfers the result to EVA Admin via HTTPS [Val15].

2. **EVA Skann:** an application for interpreting the ballots that are scanned. A barcode associated with a box of ballots is scanned, the ballots are placed in the scanner, and the ballots are interpreted by EVA Skann. An image of the ballot and associate metadata is sent to the database. In the 2017 election, the ballots were interpreted with the commercial software ReadSoft FORMS [Val15]. ReadSoft FORMS will be replaced for the 2019 election with an open source software, see Appendix C.

3. **EVA Verifiser:** is used to verify all ballots that cannot be unambiguously interpreted by EVA Skann. If a ballot does not contain stamp, ambiguous person votes, or "danglers"[1], the ballot is sent to EVA Verifiser. The ballot is presented on a separate screen, and qualified personnel decide correct interpretation manually. The correct interpretation is registered and is sent back to the database [Val15].

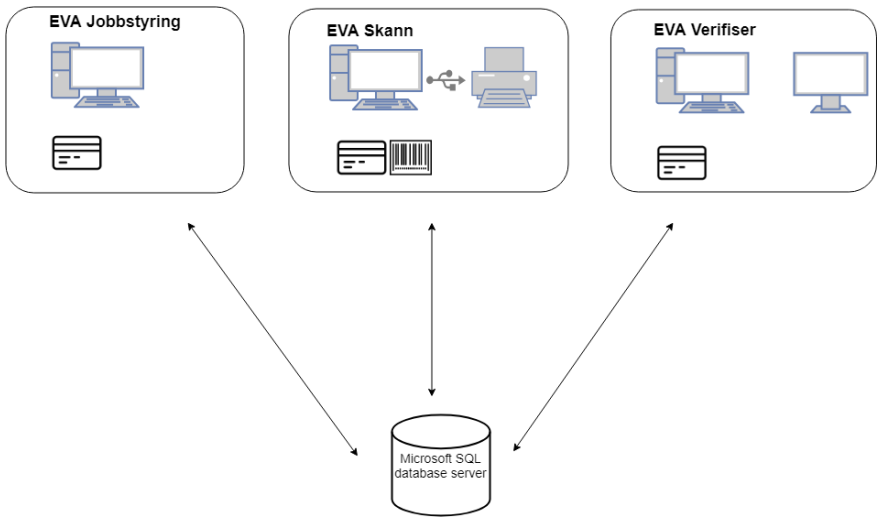


Figure 1.1: Overview of EVA Skanning components

All applications may be performed on the same Windows client. Larger municipals normally tend to install the applications on separate clients. The number of EVA Skann clients installed depend on the size of the municipal. Authentication with *ID-porten*[2] is necessary for all three applications [Val15]. The communication between the applications is through the database server, see Figure 1.1 and Appendix A.

[1] the voter gives a personal vote to candidates on other ballots (only applicable in municipal and county council elections)

[2] a common sign-on solution for public services, such as MinID or Buypass

1.4.2 Microsoft SQL Server

According to *Boken om EVA Skanning* [Val15], all data produced by the Windows applications are stored in a Microsoft SQL Server. Each scanning centre installs their own database server locally, which means that the municipals are responsible for administering the servers themselves.

The SQL servers are relational database servers with primary function of storing and retrieving data as requested by other software applications [Mic16] [Val15]. When each ballot is scanned and interpreted by EVA Skann, an image of the ballot and an associated metadata file are created and sent to the database. The ballot counting itself is performed in the database, see Appendix C. The database server edition installed in each municipal is dependent on the size of the municipal. Microsoft SQL Servers LocalDBs are installed in small municipals, where all the Windows applications and the database server are installed on the same client. In larger municipals, where the applications are installed on separate clients, the SQL server edition may either be Enterprise, Standard, or Express, see Appendix D.

Each client communicates with the database through direct database connections from the .NET code. The database server is not an application server and does not implement queue mechanisms that receives the data before they are stored [Val15]. To send data to the database the clients must be connected to the local area network, know the username and password of the database, and have knowledge of the *stored procedures*, see Appendix E.

1.5 Assumptions and limitations

Before continuing with further elaboration of the research questions and methodology, a few assumptions and limitations are discussed. These provide foundation for further reading of the master's thesis.

1.5.1 Assumptions

1. **Distinctions between parliamentary and municipal and county council elections are not addressed:** In parliamentary elections, representatives for the parliament are elected. The election is held every fourth year. In municipal and county council elections, representatives for the municipal and county councils are elected. This election is also held every fourth year. The elections are held two years apart, resulting in an election every second year.

   Distinctions between the two types of elections are not addressed in this thesis. In theory, the same principles are applicable. Both elections are defined by the Election Act, implement the same computer system, and follow more or less

the same guidelines and routines. The descriptions presented in this master's thesis are generalised and may be applied in both types of elections. In cases where there exist important distinctions, these are addressed accordingly.

2. **Municipals not implementing EVA Skanning are not addressed:** Approximately half of the municipals in Norway implemented EVA Skanning in 2017, see Appendices C and F. Each municipal decide whether to implement EVA Skanning or not. Municipals with below 10,000 inhabitants do not normally implement EVA Skanning. This is due to the module being a complex installation and may not contribute to efficiency in small municipals. The municipals not implementing EVA Skanning, perform two manual counts.

   Only municipals implementing EVA Skanning are of relevance to this study. Further descriptions of the electoral system assume implementation of electronic ballot counting.

1.5.2 Limitations

1. **Modification in research questions and methodology:** Initially, the thesis was defined by different research questions and methodology. Due to a change in the professor responsible for the thesis six weeks after the start of the research, both research questions and methodology were reevaluated. This has limited the research in both time and scope.

   At first, the thesis was defined by the research questions: 1) how errors are detected in the electoral system and 2) which measures are implemented if an error is detected. Now, the latter is extended with researching system architecture and assessing the reliability and performance of the currently implemented error detection mechanisms.

   The initial methodology was defined by interviews with election officials and representatives from the Directorate of Elections and the Ministry of Local Government and Modernisation, and suggesting a best practice for error detection based on the obtained information. Now, the methodology is extended to include experimental testing of EVA Skanning.

2. **No previous research and few publicly available sources on EVA Skanning:** First, there exist no previous research on EVA, or more specifically, EVA Skanning. EVA Skanning was developed as a part of the Internet election trials in 2011 and 2013. Two evaluations of the trials were published: Segaard et al. (2012) [SS12] and Segaard et al. (2014) [SCFS14]. These evaluations discussed user-friendliness and people's trust in Internet election, however, did not assess the technical aspects of the system, nor the security. Although EVA Skanning is still implemented in the Norwegian election, no research on the technical aspect of EVA has yet been performed.

The public has not been granted access to the computer system, and therefore there have not been opportunities for independent research. The Norwegian National Security Authority (NSM) has performed a penetration test on the EVA Skanning software, but the report is not publicly available [Gun18].

Second, there are few publicly available sources on system documentation. There exists one document, *Boken om EVA Skanning* [Val15], which provides a thorough understanding of the module used in 2015. This was initially an internal document that was published after a request from the public. Due to security concerns, the majority of the document is redacted, see Appendix C. According to the Directorate of Elections, the book is outdated and no longer relevant, the system has been further developed since 2015, see Appendix G.1. No new documentation has been published since 2015.

Both aspects limit the research. Due to the lack of previous research, related work is limited to international research. Due to few publicly available sources on system documentation, studying the system architecture requires more time and effort, and thereby results in a less comprehensive final result. Although, the Directorate of Elections have been graciously answering questions, this method of research may not be optimal. Better suited methods have not been possible due to these limitations.

3. **The research is performed in between two elections:** This master's thesis is written in between two elections, the 2017 and 2019 elections. The majority of the research is based on interviews with election officials and the Directorate of Elections. Performing interviews in between two elections and immediately before or after an election may provide different results, depending on how well the interviewees remember guidelines and routines. An election year requires intensive and thorough preparation.

   A limitation to writing the thesis in between two elections is that the information provided by the interviewees may not be accurate and complete. The election officials interviewed in the thesis have agreed to contribute to the research with reservations regarding non-complete information due to it not being an election year.

   The limitation is also relevant in relation to test EVA Skanning. Unfortunately, the Directorate of Elections do not have a version of the software used in 2017 available for testing. Due to it not being an election year, the system is currently under development.

1.6 Concept and word clarification

The master's thesis discusses the Norwegian electoral system. There may be concepts and words that are unknown in the English vocabulary. Table 1.1 depicts a concept

and word translation from English to Norwegian.

Table 1.1: Concept and word clarification

English	**Norwegian**
Advance voting	Forhåndsstemmegvining
Ballot paper	Stemmeseddel
Census	Manntall
Consultation memorandum	Høringsnotat
Counting station	Tellesentral
County	Fylke
County council	Fylkesting
Dangler	Slenger
Directorate of Elections	Valgdirektoratet
Election Act	Valgloven
Election threshold	Sperregrense
Electoral committee	Valgstyret
Electoral Regulation	Valgforskrift
Electronic poll book	Elektronisk manntall
Final count	Endelig telling
Municipal/Municipality	Kommune
Municipal council	Kommunestyre
Parliament	Storting
Parliamentary election	Stortingsvalg
Polling card	Valgkort
Polling station	Stemmelokale
Preliminary count	Foreløpig telling
Redacted	Sladder
Secret ballot	Hemmelig valg

1.7 Thesis outline

The structure of the master's thesis is as follows:

– Chapter 2: Presents research questions and chosen methodology. The methodology includes semi-structured interviews, experimental testing of EVA Skanning, and qualitative analysis and application of risk-limiting audit algorithms.

- Chapter 3: Provides a high-level illustration of the EVA Skanning architecture, and discusses security vulnerabilities and recommendations for improved security.
- Chapter 4: Presents currently implemented error detection mechanisms in the Norwegian electoral system, and discusses their reliability.
- Chapter 5: Introduces the concept of risk-limiting audits, and presents two algorithms that may be applicable for the Norwegian electoral system.
- Chapter 6: Summarises the findings, presents conclusive remarks, and suggests future work.

Chapter 2
Methodology

Chapter 1 has introduced the background, project scope, and research questions. Now, the methodology used to obtain the results is provided.

First, the research questions are thoroughly derived and explained. Second, mixed methods research is introduced as appropriate research method. Mixed methods research is applied in form of in-depth interviews, an experimental testing of EVA Skanning, and a qualitative analysis of risk-limiting audit algorithms. Finally, a description of how the data is analysed and interpreted is depicted.

2.1 Research questions

Before deciding which research paradigm and which specific methods are most suitable given the objectives, the project must be defined by appropriate research questions. According to Robson et al. (2016) [RM16], research questions are useful to explore and explain specific parts of the objectives. In addition, defining research questions can be useful for defining success, (i.e., a measurable criteria to evaluate when obtaining the results) and to limit the project scope (i.e., ignore what is not relevant for the questions). The research questions are based on the objectives presented in Chapter 1.3 and formulated in a way so that answering them are feasible. Based on the objectives, three research questions are derived:

1. How is EVA Skanning architecturally structured and secured?
2. How are counting errors detected in the Norwegian electoral system?
3. How can risk-limiting audits be applied to the Norwegian electoral system?

An objective of this master's thesis is to research the level of security within EVA Skanning. To facilitate such a study, the system architecture and its technical

requirements and capabilities must be known. Unfortunately, there exists few publicly available sources on system documentation. Therefore, the first research question aims at studying the technical components and implemented security measures of EVA Skanning.

Second, an objective aims to assess the reliability and performance of the currently implemented error detection mechanisms in the Norwegian electoral system. According to the official website of the Directorate of Elections, *valg.no*, there are implemented error detection mechanisms in the electoral system to ensure result integrity:

> *In addition to securing the administrative IT system EVA, there are additional control mechanisms in the conduction of the election that ensures that compromise of the IT system itself is not sufficient to affect the result - the control mechanisms are not bound to if or which IT solutions are in use - valg.no* [Val17].

Which mechanisms or how they are implemented are not described. Therefore, the second research question aims at studying which error detection mechanisms are implemented and how they are enforced. Based on the acquired information, an assessment of the reliability and performance of the mechanisms, may be conducted.

Third, the thesis aims at analysing if, and how, risk-limiting audits should be applied to the Norwegian electoral system. Whether such an algorithm should be applied, depends on the results from the two previous research questions. How, on the other hand, may be addressed regardless of the results. The third research question therefore aims to analyse how risk-limiting audits may be applied to the Norwegian electoral system.

2.2 Mixed methods research

To embark on the research, clear strategies in order to address the research questions in a targeted and rigorous way are necessary, i.e., produce a research design. There are several ways to conduct research, but the question whether researchers should use quantitative or qualitative research approaches has been widely debated in the past years and has been characterised by two opposite camps. Recently, a historically less acknowledged and disputed research paradigm has accompanied the other two: the mixed methods research paradigm [JO04] [JOT07]. Mixed methods research is defined by Johnsen et al. as:

> *Mixed methods research is the type of research in which a researcher or a team of researchers combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the broad purposes of breadth and depth of understanding a corroboration* [JOT07].

Mixed research methods give the researcher the freedom to combine several methods to answer research questions in a most accurate manner. On one side, the researcher can exploit the benefits of quantitative research, e.g., make generalisations and predictions in a deductive way based on extensive data collecting [Yil13]. On the other side, the researcher can make use of the benefits of qualitative research, e.g., inductive in-depth studies to get an understanding of people's view or experience of a field of interest [Yil13]. Mixing these techniques provide a broader perspective of the research questions. The mixed methods process is illustrated in Figure 2.1.

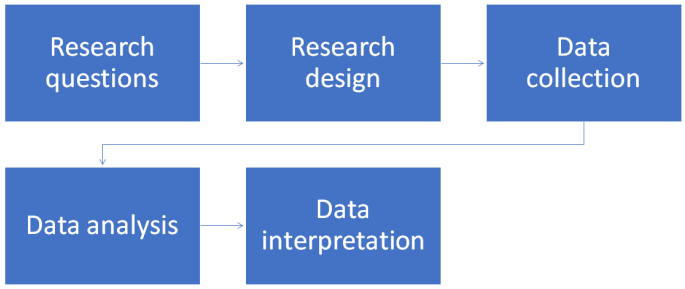


Figure 2.1: Illustration of mixed methods research

2.2.1 Qualitative vs. quantitative research

Qualitative research is concerned with understanding human behaviour from the informant's perspective and assumes a dynamic and negotiated reality. Data are collected through participant observation and interviews and analysed by themes from descriptions by informants [MAM90]. The technique involves conducting intensive individual interviews with a small number of respondents to explore their perspectives on a particular situation [BN06].¨

Quantitative research is empirical research where the data are in the form of numbers. Quantitative research is concerned with discovering facts about social phenomena and assumes a fixed and measurable reality. Data are collected through measuring things and analysed through numerical comparisons and statistical inferences. The result is often reported as statistical analysis [MAM90].

Traditionally in mixed methods research, qualitative research is first performed to research people's perception and understanding of a certain issue. Then quantitative research is applied to make generalisations and predictions based on extensive data collection on the same issue. This dissertation implements the mixed method research, however, not in its traditional form.

2.2.2 Mixed methods research applied to this master's thesis

To determine architecture and level of security of EVA Skanning, qualitative research in form of in-depth interviews with system engineers and the users themselves are appropriate. There exist few publicly available sources on EVA, therefore, interviews with developers and users are the primary source of information. In addition, an experimental test of the system may provide a quantitative foundation for further evaluation of how the modules communicate and their behaviour.

In-depth interviews are also the preferred method to research error detection mechanisms. There has not previously been performed research on error detection in the Norwegian electoral system either, and therefore exists few sources available to the public on which error detection mechanisms are applied in general. In-depth interviews will give indications of how errors are detected in theory. In collaboration with in-depth interviews, an experimental setup of EVA Skanning may be useful to investigate error detection mechanisms in practice. The combination of methods gives a foundation to assess the reliability of the error detection mechanisms in the Norwegian electoral system.

Finally, qualitative research is applied to evaluate risk-limiting audits algorithms and determine how they can be applied to the Norwegian electoral system. Initially, a quantitative study where each algorithm is tested in practice, was preferable. Unfortunately, such an experiment was not possible to conduct, due to that the inquiry to borrow document scanners and ballot paper from two municipals was denied. Therefore, a qualitative analysis of audit algorithms is performed. Based on the information obtained from the two previous research questions, a foundation to evaluate risk-limiting audits as error-detection mechanisms for the Norwegian electoral system is provided.

Collectively, these operations conform the research design of this master's thesis. In the following sections, the specific methods are further elaborated.

2.3 In-depth interviews

In this study, semi-structured interviews are used as qualitative research. Semi-structured interviews consist of a series pre-determined questions to be answered by

all interviewees. Additional questions may be asked during the interviews to clarify and/or further expand certain issues [VT14]. Advantages and disadvantages with semi-structured interviews are listed in Table 2.1.

Table 2.1: Advantages and disadvantages of semi-structured interviews [VT14]

Advantages	**Disadvantages**
Facilitates collecting detailed information about the research question	Time-consuming process
The interviewer has direct control over the process flow and can clarify issues during the data collection process	Difficult to arrange appropriate time with the interviewees

Three groups are relevant to interview:

1. the Ministry of Local Government and Modernisation
2. the Directorate of Elections
3. election officials

First, the Ministry of Local Government and Modernisation is relevant. The Ministry has the overall responsibility for implementation of elections.

Second, the Directorate of Elections is of interest. The Directorate is a subject to the Ministry and is responsible for the operative conduction of elections on a national level. The Directorate is also responsible for the technological system used in elections, EVA, and hold information on system description and documentation.

Third, election officials are responsible for conducting the election in their municipal according to the regulations statutory in the Election Act. The election official together with the electoral committee decide how to perform counting in their municipal, are responsible for securing election infrastructure, and ensuring that counting is performed according to the guidelines defined by the Directorate of Elections.

2.3.1 Ethical considerations

In order to collect personal data and record the interviews, an inquiry had to be issued to, and approved by, the Norwegian Centre of Research Data (NSD). Upon approving such an inquiry, NSD requires that the interviewees are informed about

the details regarding recording, how the information is used, and date of deletion of the acquired material. Hence, a request for a declaration of consent was sent to all the candidates, informing about associated details related to the research.

The representatives from the Ministry and the Directorate did not wish to sign the declaration due to not participating as individuals, but rather on behalf of the Ministry and the Directorate. They did not wish to be recognised by name or position, and approval from NSD was therefore not necessary. The representatives accepted that the interviews were recorded for memory purposes and correct rendering, and ensured they were anonymous. During the course of writing, it was found beneficial to transcribe the interviews and add them as appendix to the thesis, to better document the foundation for the conclusions. After discussing the matter with the representatives from the Ministry and the Directorate, the representatives stated that they did not wish to have the transcripts included due to not being informed of the matter prior to the interviews. The transcripts are therefore not added as appendix. The questions, on the other hand, are included, see Appendices C and E.

All participating election officials consented and signed the declaration. During the course of writing, it was decided that it was beneficial to anonymous the election officials as well, and the thesis does therefore not contain any personal data related to the participating election officials. The transcribed interviews are not included as appendices, due to the comprehensive task of transcribing 18 one-hour long interviews.

Upon completion of this project, all associated personal data have been deleted, including the recordings.

2.3.2 Interview with the Ministry of Local Government and Modernisation and the Directorate of Elections

Initially, there were planned two separate interviews with the Ministry of Local Government and Modernisation and the Directorate of Elections. However, the Ministry and the Directorate found it expedient to perform the interviews in collaboration. This was accepted.

The objectives of the interview were to gather system documentation, information related to which guidelines and procedures are implemented to detect errors when using EVA Skanning, and general information on development and security. In addition, an objective was to research if the answers provided by the Ministry and the Directorate correlated with the responses provided by the election officials. The results are presented in Chapter 3 and Chapter 4.

A representative from the Ministry of Local Government and Modernisation was

contacted via email in February 2018, with an invitation to and a description of the study. The representative was positive and arranged a meeting. 11 October, three representatives from the Ministry and two representatives from the Directorate attended the interview in Oslo. The interview guide may be found in Appendix C.

2.3.3 Interviews with election officials

18 election officials from a representative selection of municipals are interviewed in this study. The objectives of these interviews were to research how ballot counting is performed in different municipals and which error detection mechanisms are implemented. It was also of interest to study whether the error detection and correction methods are similar in all municipals. Finally, an objective was to study whether the responses correlated with the Ministry and the Directorate's answers.

There are 422 municipals in Norway (2018[1]), whereas 128 municipals were planning to use EVA Skanning during the parliament election in 2017, see Appendix F. An email with an invitation to and a description of the study was sent to election officials in 112 out of the 422 municipals. This was due to not knowing which municipals were planning to use EVA Skanning. Contact information to the election officials was provided by the Ministry.

62 election officials replied. Many of the responses were replies explaining that their municipal did not use EVA Skanning, hence these municipals were not of interest for the study. Others replied that they were not able to participate in the study due to full work schedule. 22 election officials replied that they would like to participate, and 18 of them were chosen based on size and location in the country to create a representative selection. The statistics are presented in Table 2.2 and 2.3.

Table 2.2: Contacted municipals

Municipals	**Contacted municipals**	**Municipals using EVA Skanning**	**Municipals using EVA Skanning in the study**
422	112	128	18
100%	27%	100%	14%

[1] in 2017, the government proposed a reform to merge municipals from 428 to 358 municipals, https://www.regjeringen.no/no/dokument/dep/kmd/sak/saksgang-kommunereformen/id2607187/

Table 2.3: Participating municipals

	South	West	East	Central	North	Sum
Small		1	2			3
Medium	1	1	6	3		11
Large		1	2	1		4
Sum	1	3	10	4	0	18

In Table 2.2, 27% of all municipals have been contacted, and 14% of the municipals using EVA Skanning are participating in the study. Table 2.3 presents an overview of size and location of the municipals participating.

A small municipal is defined as a municipal with less than 15,000 inhabitants. A medium municipal is defined as a municipal with more than 15,000 inhabitants and less than 100,000 inhabitants. A large municipal is defined as a municipal with more than 100,000 inhabitants. A clarification that must be noted is that a small municipal seldom is characterised by less than 15,000 inhabitants. The explanation is that municipals with less than 10,000 inhabitants seldom implements EVA Skanning. This because the equipment is expensive and may not simplify the counting process is small municipals. A small municipal is therefore here defined as a municipal with less than 15,000 inhabitants.

To create a representative selection, the country is here divided into five geographical areas: south, west, east, central, and northern part of Norway, see Table 2.3.

18 municipals were defined as a limit due to time restriction. Each interview was given a time frame of two hours. The majority of the interviews were performed via Skype or telephone, however two of the interviews were conducted in person at the municipals' city hall, all of them were conducted during a two weeks period from 10 September to 21 September. The interview guide may be found in Appendix H. The results from the interviews are presented in Chapter 4.

In retrospect, conducting these interviews as a questionnaire might have been more appropriate. This is because such a method would have obtained more data in less time. However, due to limited information on the electoral system, semi-structured interviews were considered the best option at the time. This because semi-structured interviews allow the interviewee to elaborate and explain certain issues.

2.4 Information day at the Directorate of Elections

2.4.1 Introduction

During the interview with the Ministry and the Directorate, the Directorate suggested an "information day" in Tønsberg. The questions of technical character were difficult to answer outside their offices. In addition, the request to set up a simulation of EVA Skanning at the university was denied, however, the Directorate offered to demonstrate EVA Skanning at their offices. The representatives from the Directorate therefore suggested to arrange an information day in Tønsberg, specifically to benefit this master's thesis.

The information day took place 23 October. The information day was divided into three sections. First, a review of elections and election law. This was to build context and provide the background for the technical systems. Second, a conversation about existing system documentation and architecture. The objective of the conversation was more insight and clarification of system architecture. Third, a demonstration of EVA Skanning. The objective was to observe how the modules communicate and to research error detection mechanisms in practice.

The first part of the information day is not further described, as the information is not directly relevant for this study. The two last parts of the information day are further explained in the following sections.

2.4.2 Conversation regarding system architecture

According to the Directorate, there does not exist any system documentation for EVA Skanning used in 2017. There were no guidelines requiring such documentation at the time of development, see Appendix C. Recently, the Directorate has started documenting the modules of EVA towards the 2019 election. The documentation is registered on *confluence*[2]. The objective of the conversation was to obtain information and understand the modules and their corresponding protocols. The conversation consisted of going through the pages on confluence and discussing figures, definitions, and security protocols. Occasionally, questions were asked to further explain and elaborate. An exemplification of a possible attack for result manipulation was also proposed.

Although the conversation was recorded, the Directorate was not informed that the conversation would be transcribed. Therefore, the Directorate requested that the transcript of the conversation was not to be published as an appendix. The questions

[2]a common work space for companies, https://www.atlassian.com/software/confluence/why-wiki-collaboration-software

asked during the conversation are added instead, see Appendix E. The results and discussions are presented in Chapter 3 and Chapter 4.

2.4.3 Experimental setup of EVA Skanning

The last part of the information day consisted of an experimental test of EVA Skanning, and is considered to be the quantitative part of the study.

Setup

According to the Directorate of Elections, the EVA Skanning version used in 2017 was not available for testing. The Directorate offered to test the version currently under development with reservations of an incomplete software. The primary difference between the 2017 and the 2019 model, is the ballot interpretation software. In 2017, the commercial software ReadSoft FORMS was used to interpret the paper ballots, now the Directorate is developing an open source interpretation software.

The experimental setup is illustrated in Figure 2.2. The setup consisted of a document scanner (Canon DR-G1130) connected to a laptop (Windows operating system) via USB cable. The laptop was installed with the EVA Skanning applications (EVA Jobbstyring, EVA Skann, and EVA Verifiser) and the database server (SQL LocalDB). A card reader was also connected to the laptop. This is used to scan the BuyPass card for authentication, authorisation, and signing of the result. The laptop was not connected to the Internet (transferring the result to EVA Admin was not part of the experiment).

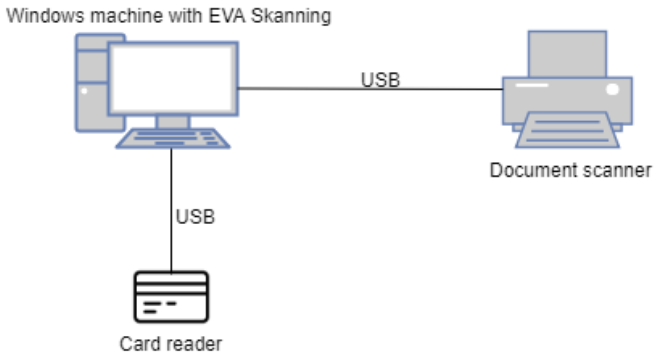


Figure 2.2: Experimental setup of EVA Skanning

Earlier, the same day, the Directorate had tested the setup. Despite the module being in development, the Directorate considered it to be a functional system. In the tests prior to the experiment, 8 ballots were scanned and interpreted.

Experiment

The objective of the experiment was twofold: 1) Identify communication protocols and behaviour of EVA Skanning to evaluate level of security and 2) research how possible software errors were detected in practice when scanning ballots, and thereby creating a foundation for evaluating the reliability and performance of the error detection mechanisms.

The experiment consisted of using EVA Skanning to interpret and count 15 paper ballots. 12 of the ballots were stamped, whereas 3 were not. This was to check if correct number of ballots were sent to EVA Verification. All ballots were placed in and run through the scanner 3 times. In the fourth round, only 8 ballots were scanned. The approach is described in the following section, and the results are presented in Chapter 4.

Approach

The Window client, the document scanner, and the card reader were activated. EVA Jobbstyring was started on the computer and the alternative log in method *nødmodus* was used to authenticate the user for the experiment. Vestfold and Horten were selected as county and municipal. When a municipal and county are selected, all precincts (polling stations) for the selected municipal are listed in EVA Jobbstyring, see Figure 2.3. Furthermore, the advance votes tab and preliminary count were selected, see Figure 2.4 and 2.5, respectively.

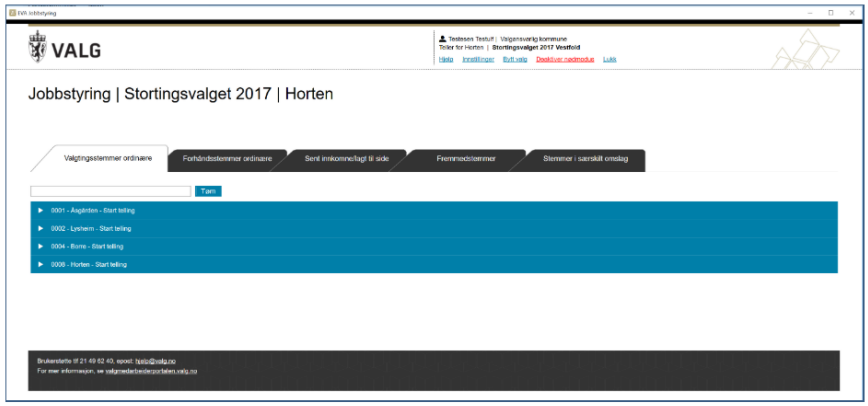


Figure 2.3: Select county and municipal, EVA Jobbstyring

Figure 2.4: Select votes to count, EVA Jobbstyring

Figure 2.5: Select type of count, EVA Jobbstyring

Next, EVA Skann was opened and authenticated in similar manner. The first view of EVA Skann is illustrated in Figure 2.6. Normally, in an election, the barcode on a box of ballots for the given precinct is scanned with the barcode reader, and the fields are automatically filled. In this experiment, there were no boxes with barcodes, the barcodes therefore had to be generated manually in EVA Jobbstyring. After generating the barcodes, they were copied and pasted into EVA Skann.

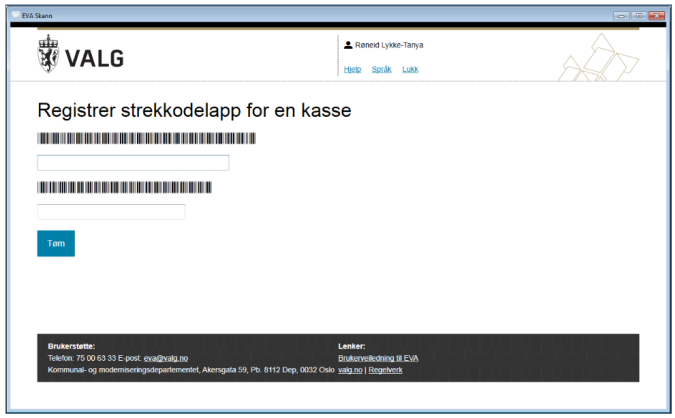


Figure 2.6: First view, EVA Skann

Next, information related to the barcode is presented in EVA Skann, see Figure 2.7. The ballots were then placed in the scanner, and "Start Skanning" was pressed in EVA Skann. While the ballots were scanned, the ballots were presented in the right corner of the EVA Skann application, see Figure 2.8. The ballots disappeared quite quickly, and the software was lagging.

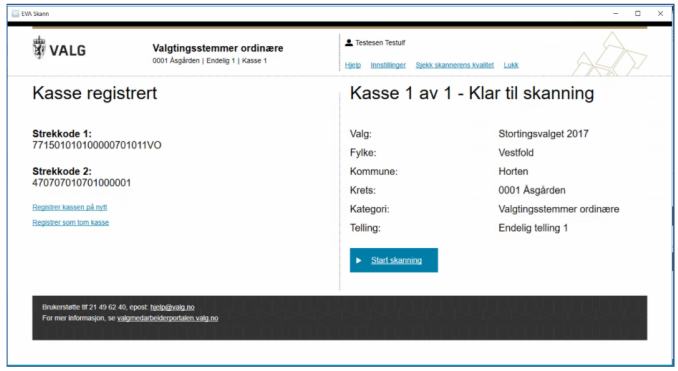


Figure 2.7: Box is registered, EVA Skann

Figure 2.8: Skanning ballots, EVA Skann

When all ballots had been scanned, EVA Skann presented three alternatives, see Figure 2.9. The alternative that was chosen in all three rounds was "Alle sedlene i kassen er skannet".

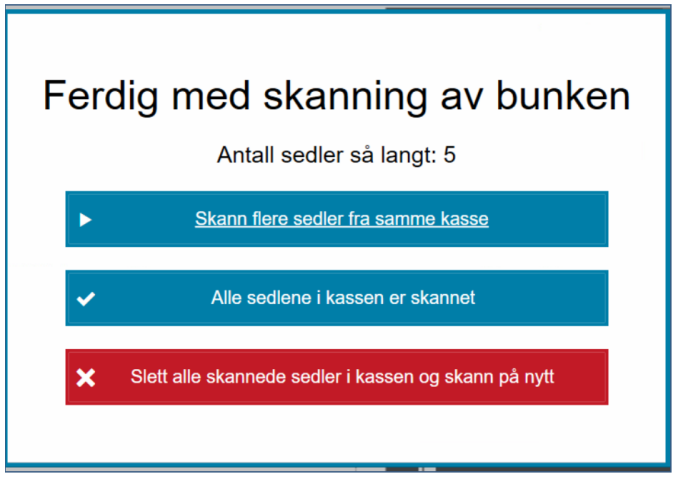


Figure 2.9: Skanning finished, EVA Skann

When the scanning was finished, EVA Verifiser was opened, see Figure 2.10. All ballots that are not unambiguously interpreted by EVA Skann, are sent to EVA Verifiser. In this experiment the only factor that was tested was whether the ballots without stamps were sent to EVA Verifiser, see Figure 2.11.

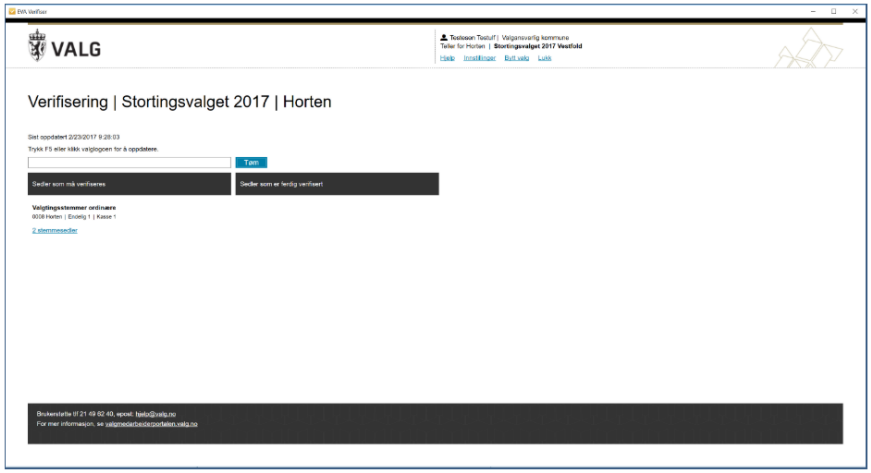


Figure 2.10: First view, EVA Verifiser

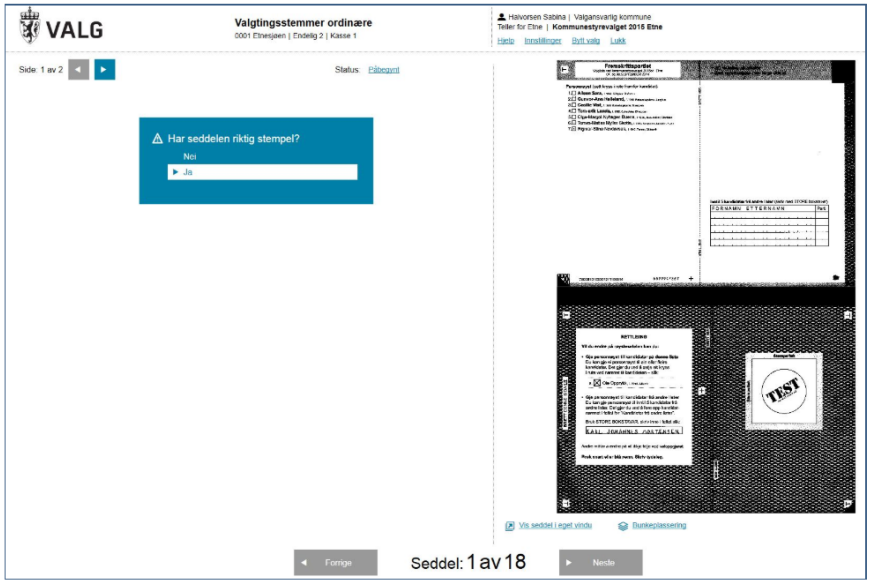


Figure 2.11: Verify if correct stamp, EVA Verifiser

Results and discussion

The results from the experiment and the corresponding discussion are presented in Chapter 4.

2.5 Analysis of risk-limiting audits and application to the Norwegian electoral system

The third research question addresses risk-limiting audits and its applicability to the Norwegian electoral system. The objective of a risk-limiting audit is to define a risk limit such that there is a high probability of detecting errors if the result were to be wrong. Primarily, a presentation of two algorithms are given: *ballot-polling audits* and *comparison audits*. These are "simple" calculations, meaning observers can easily check the auditors work. The algorithms are discussed in a vote-for-one contest, making it relevant for the Norwegian election.

A qualitative research approach is applied to evaluate risk-limiting audits algorithms and determine how they can be applied to the Norwegian electoral system. Based on the information obtained from the two previous research questions, a foundation to evaluate risk-limiting audits as error detection mechanisms is given. Which algorithms and how they may be applicable to the Norwegian electoral system is further analysed in Chapter 5.

An alternative research approach that was discussed, was to perform the risk-limiting audit analysis quantitatively. By first scanning the ballots, and then apply both algorithms to determine degree of applicability and simplicity, the audit algorithms would be analysed based on quantitative data. Unfortunately, such an experiment was not possible. An inquiry to lend a document scanner and ballot paper was denied by two municipals. Therefore, a qualitative analysis of the two algorithms are the foundation for the conclusion.

2.6 Analysing and interpreting the collected data

Following the mixed methods research model, the collected data must be analysed. An issue that emerges from mixed methods research is how and when the collected data from the different methods should be combined [CC17].

The research questions to be answered are threefold: 1) how the ballot counting system is architecturally structured, 2) how software and hardware errors are currently detected, and 3) how risk-limiting audits can be applied in the Norwegian electoral system.

These research questions divide the results chapters into three parts, and similarly each part is discussed and analysed separately. In Chapter 3, the EVA Skanning architecture and security is presented and discussed. Furthermore, in Chapter 4, implemented error detection mechanisms are described and their reliability is analysed. Finally, in Chapter 5, two risk-limiting audit algorithms are depicted, and their

applicability to the Norwegian electoral system is discussed.

Although the acquired information is analysed separately, each chapter provides foundation for the subsequent chapters.

Chapter 3
EVA Skanning

Chapter 2 provided the methodology used to study the research questions. This chapter aims to study the first research question: how EVA Skanning is architecturally structured and secured.

The methodology used to research the EVA Skanning module is to interview system engineers, operators, and managers, and study the experimental setup described in Chapter 2.4.3.

First, a high-level illustration of the EVA Skanning architecture is presented. Second, security vulnerabilities within the module are discussed. Finally, recommendations for improved level of security are provided.

3.1 Architecture of EVA Skanning

3.1.1 Introduction

To research the architecture and the level of security within EVA Skanning, proper system documentation is necessary. Unfortunately, there exists few publicly available sources that provides insight to the functionality and design of the system. There exists one document, *Boken om EVA Skanning* [Val15], which provides a thorough understanding of the EVA Skanning module used in 2015. According to the Directorate of Elections, the book was developed as an internal document for the handover of the system from the Ministry to the Directorate when the Directorate was established in 2016. Unfortunately, the majority of the document is redacted due to security reasons. However, the Directorate also claims the book to be outdated, and according to them, the module has been further developed since 2015, see Appendix C.

According to the Directorate, there does not exist complete architecture or system documentation on EVA Skanning used in 2017. This is due to lack of guidelines and routines requiring such documentation, see Appendix C. Why system documentation

for 2015 was developed, but the routines were not continued in 2017, is peculiar. The Directorate further stated that they do indeed have system documentation for the 2017 module, but that it does not exist in a publishable form. Currently, the Directorate is working on system documentation for the module to be used in 2019. Due to lack of proper system documentation, defining system requirements, capabilities, and level of security within the module is challenging.

3.1.2 Architecture

Due to no publicly available architectural description of EVA Skanning used in 2017, the architecture presented is based on dialogue with the Directorate of Elections. The Directorate did not wish to specify specific configurations due to security measures. Therefore, the architecture presented is a high-level illustration of EVA Skanning, see Figure 3.1 and Figure 3.2.

The figures illustrate the "common counting station", usually located at the city hall in the largest municipality in the county. All municipals that used EVA Skanning in 2017, implemented one of these configurations to perform the final count. There are two possible configurations of EVA Skanning: *small installation* and *large installation*.

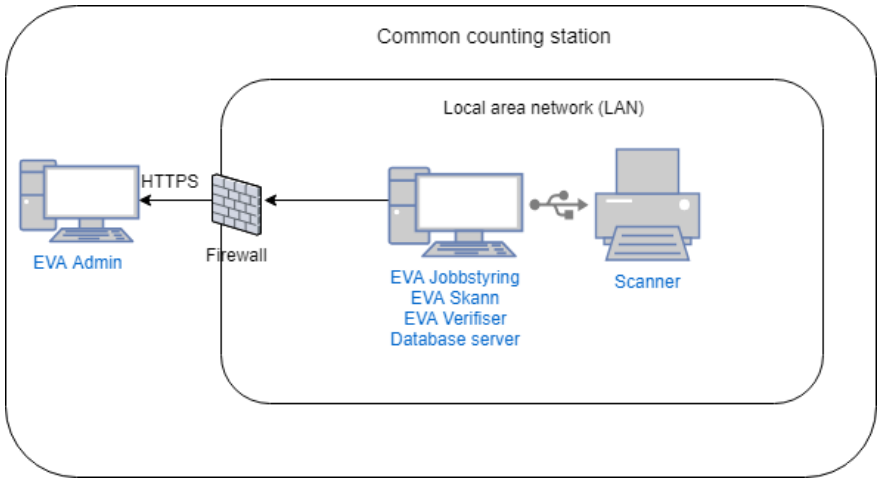


Figure 3.1: EVA Skanning architecture (small installation)

A small installation is configured in a local area network (LAN) at the common counting station, see Figure 3.1. A small installation consists of one Windows client and one document scanner. An example of a common document scanner is Canon DR-G1130 [Val15]. The Windows client is installed with all three EVA Skanning applications: EVA Jobbstying, EVA Skann, and EVA Verifiser (see Chapter 1.4).

In addition, the client has the datbase server installed. In a small installation, the database server edition is a Microsoft SQL LocalDB. The document scanner is connected to the client with a USB cable. EVA Jobbstyring communicates with EVA Admin for transferring the result over the Internet using HTTPS, see Appendix E. The Directorate further specified that the client does not necessarily need to be connected to the Internet during the scanning process, but can run in *nødmodus*, and be connected only when transferring the result, see Appendix D. Whether the municipals implement such a security measure is not known.

A similar LAN is configured for a large installation. Similar to a small installation, the scanners in a large installation are connected to EVA Skann clients with USB cables. In a large installation, EVA Jobbstyring and EVA Verifiser are installed on separate Windows clients. The same applies for the database server. Unlike a small installation, the database server edition installed may be Enterprise, Standard, or Express, see Appendix D. A large installation may be configured differently depending on the size of the municipal: the larger the municipal the more scanners and EVA Skann clients are necessary. The scanner-client ratio is 1-1. In the example in Figure 3.2, three clients and three scanners are used. Similar to a small installation, EVA Jobbstyring communicates with EVA Admin over HTTPS.

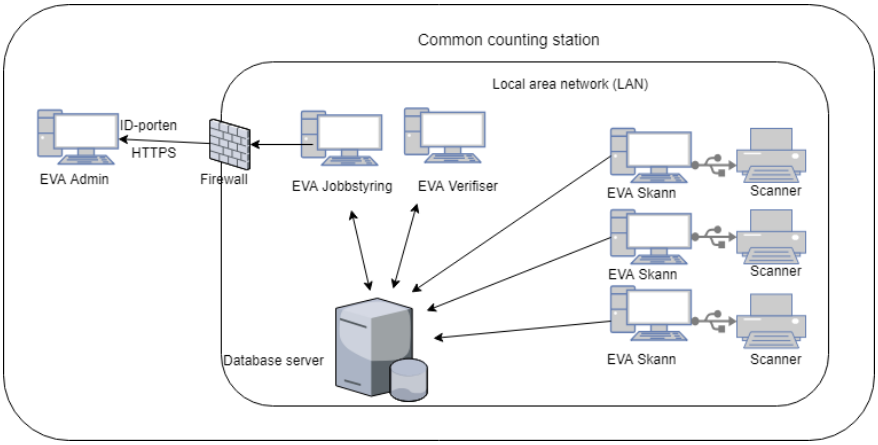


Figure 3.2: EVA Skanning architecture (large installation)

3.1.3 Sequence diagram

A high-level architecture may not be sufficient to fully understand the complexity and functionality of EVA Skanning. To demonstrate the components' interaction, a sequence diagram is presented, see Figure 3.3. A sequence diagram illustrates object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to

carry out the functionality of the scenario. The sequence diagram is based on the dialogue with the Directorate. Screenshots of the modules in use are included in the approach of the experimental setup, see Chapter 2.4.3.

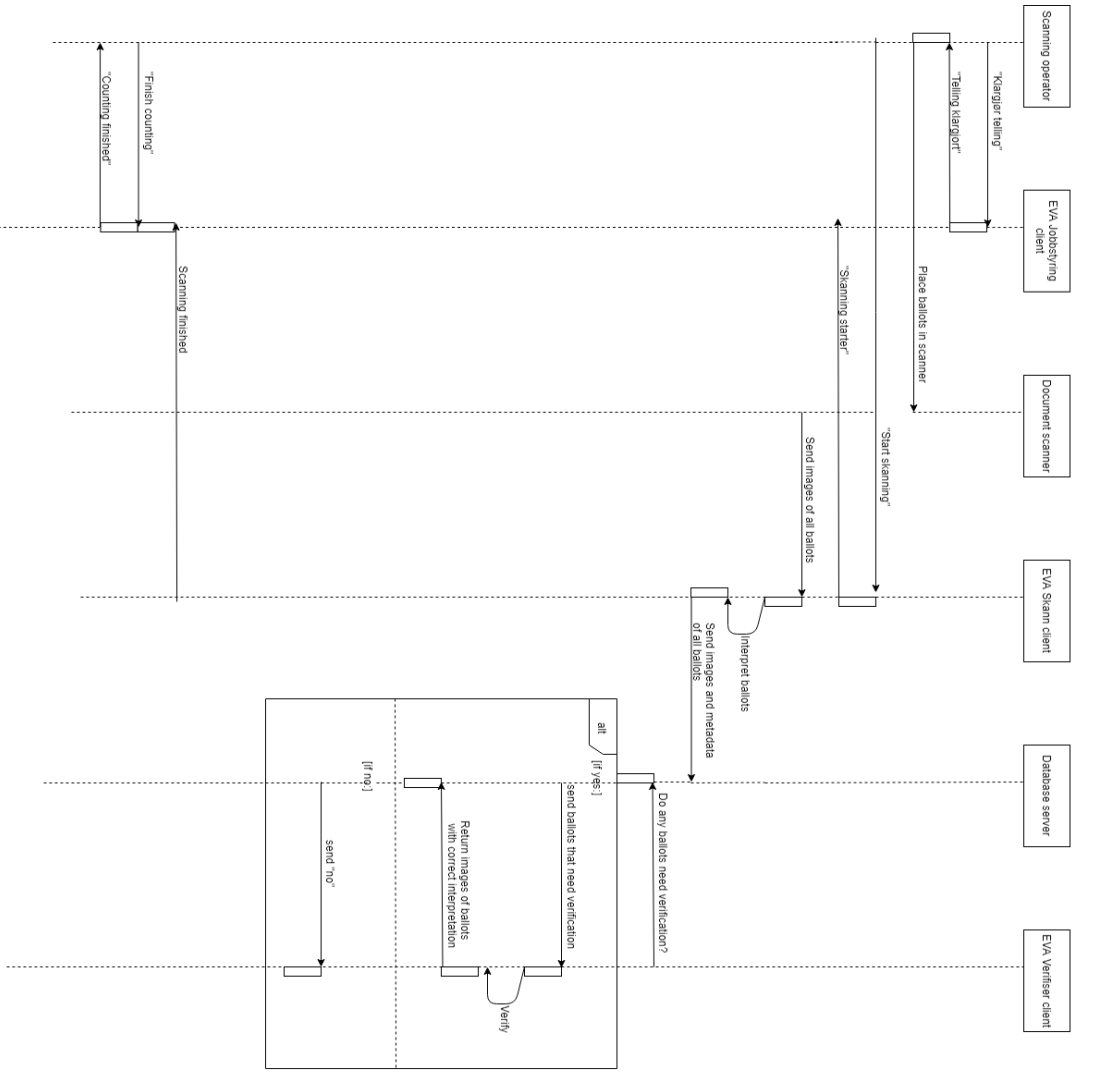


Figure 3.3: Sequence diagram of EVA Skanning

To start scanning ballots, the scanning operator opens the EVA Jobbstyring application, and selects "Klargjør skanning". The operator selects a box containing ballots from a given precinct and scans the barcode on the box with a barcode reader. Then, the operator places the ballots from the box in the document scanner.

Normally, batches of 1,000 ballots are used. The operator then opens the EVA Skann application and presses "Start scanning".

The document scanner scans the ballots and transfer images of the ballots to EVA Skann. EVA Skann then interprets all the images and sends the images together with associated metadata describing which information the ballot holds, such as ballot number, party, and stamp to the database. The image and metadata are stored in the database. In 2017, EVA Skann was dependent on the software application ReadSoft FORMS for interpretation. The Directorate is currently working on substituting ReadSoft with an open source application. The counting itself is based on the information stored in the database.

When a batch of ballots is finished, EVA Verifiser asks the database if any ballots need verification. The ballots that cannot be interpreted unambiguously by EVA Skann are sent to EVA Verifiser. These are often ballots with no stamps or ballots with manual changes (danglers). The ballots are demonstrated on a separate screen and interpreted by qualified election workers. The correct interpretation is registered, and the image with the metadata is sent back to the database.

When all ballots' images and metadata for a given precinct are stored in the database, the counting may be finalised. The operator opens EVA Jobbstying and presses "Finish counting", and the result is transferred to EVA Admin. Before the result is transferred, it is cryptographically signed with a BuyPass card.

3.1.4 Database configurations

The Directorate did not wish to further specify database configurations due to security measures, see Appendix G.2. In order to provide a security analysis, standard configuration of Microsoft SQL Server is assumed:

- At the simplest level, a SQL Server client can reside on the same machine as an instance of SQL Server, such as in a small installation. Typically, however, a client connects to one or more remote servers over a network. The client/server architecture of SQL Server allows it to seamlessly manage multiple clients and servers on a network, such as in a large installation [Mic16]. According to the Directorate, LocalDB is used in small installations and Enterprise, Standard or Express is used in large installations, see Appendix D.
- LocalDB supports two kinds of instances: *automatic instances* and *named instances*. Automatic instances of LocalDB are public and can be used by any application and provide seamless instance management. There is no need to create the instance; it just works [Mic16]. This allows for easy application installation and migration to a different computer. Automatic instances of

LocalDB have a special pattern for the instance name that belongs to a reserved namespace. The name for the automatic instance is MSSQLLocalDB [Mic16].

Named instances of LocalDB are private. They are owned by a single application that is responsible for creating and managing the instance. Named instances provide isolation from other instances and can improve performance by reducing resource contention with other database users. Named instances must be created explicitly by the user through the LocalDB management API or implicitly via the app.config file for a managed application [Mic16]. According to an email sent from the Directorate in January 2019, named instances are used in small installations. Named instances provide more control and better security in regard to which clients are connected to the database.

– In a standard LocalDB configuration, authentication between the client and server is usually approved with a default username and password. These fields are often stored in plaintext on the client. One can assume this is the case for the EVA Skanning application. The Directorate commented that in 2019, authentication details are stored using Data Protection API, see Appendix D.

Upon completion of the master's thesis, the thesis was sent to the Directorate of Elections for an evaluation. The Directorate was able to comment on the content and clarify any misunderstandings. The feedback from the Directorate may be found in Appendix D. In the feedback, the Directorate clarified that named instances and integrated security are used in small installations. Configuration of large installation was not mentioned.

3.1.5 Firewall configurations

The Directorate did not wish to specify any firewall configurations:

> *We cannot provide access to concrete network configurations. But we note that the principles are well illustrated in the provided information and through the conversation in Tønsberg* - E-mail from the Directorate of Elections, see Appendix G.2.

The firewall configurations are subject to the election committees in the municipals, each municipal is responsible for their own security of the election infrastructure. In the interviews with the election officials, the officials did not want to elaborate on specific configuration details. This was considered a security measure. Some also referred to the Directorate of Elections, and stated that the Directorate is responsible for firewall configuration, see Appendix H. According to the Directorate, the municipals are responsible for firewall configuration, but the Directorate will

in 2019 provide additional documentation for configuration and automated script where applicable, see Appendix D. How the firewalls that connect the local area networks and the Internet (see Figure 3.1 and Figure 3.2) are configured, is therefore not possible to further analyse.

An interesting remark to be made is that there seems to be confusion related to who is in fact responsible for security of the election infrastructure. The Directorate states that the municipals themselves have the responsibility to secure the configuration of the firewall, whereas some election officials are under the impression that the recommendations provided by the Directorate are sufficient for a secure installation. Such a disclaimer on both ends may lead to additional security vulnerabilities.

3.2 Development not motivated by security

Boken om EVA Skanning discusses the choice of relational database. According to the book, the primary argument for selecting this type of architecture is to maintain a simple system which is easy to implement. Futhermore, *Boken om EVA Skanning* addresses that the data could be stored advantageously in a document database, but continues to justify the choice of relational database:

> *One cannot only take data structure into consideration, one must also consider operating conditions, level of knowledge, and what is implementable in small municipals. The choice of relational database is not selected because relational model and SQL servers are the best solutions for all imaginable purposes, but because of pragmatism and the desire to keep the system relatively simple* - Page 13, *Boken om EVA Skanning* [Val15].

Although, the Directorate claims that *Boken om EVA Skanning* is outdated, the research shows that the architecture currently implemented in the municipals, implements the same database server as in 2015. Therefore, the quote is of relevance. Such commentary in an internal document is quite peculiar. An election system is the most important instance in a democratic society, and the need for the system to be secure is imperative. When the development of the system is not entirely motivated by security, but rather practical elements, there is a need for public auditing and verification.

Upon completion of the thesis, the Directorate commented that the choice of relational database is not related to security but rather related to choice of technology and architecture, see Appendix D. The fact that the Directorate does not understand the connection between choice of technology and level of security is quite surprising and alarming.

Furthermore, both the interview in Oslo and the conversation in Tønsberg provided the impression that there are in fact several security vulnerabilities related to the EVA Skanning module and that the development is not entirely motivated by security. During the conversation in Tønsberg, an exemplification of an attack was presented by the interviewer. Due to no authentication between client and database server, other than a username and password, any client with access to the local area network and knowledge of the credentials, may access the database and possibly alter the result. When discussing the attack, the representative from the Directorate agreed that such an attack would in fact be possible, although the attacker would have to break some barriers to perform the attack, see Appendix E.

In addition, during the conversation in Tønsberg, the representative from the Directorate stated that the electoral system is a complex picture, and that not everything necessarily is motivated by security, see Appendix E. In retrospect, the Directorate commented that this statement was a misunderstanding, and that the statement was rather related to the organisation of ballot counting (i.e. scanning of barcodes and boxes with ballots), and that an attack would have to be consistent to avoid deviations that would lead to investigations. *These* measures were not entirely motivated by security, but, nonetheless, contribute to increased level of security.

3.3 Possible technical vulnerabilities

The information acquired through the interviews is unfortunately not sufficient to determine level of security within EVA Skanning. The Directorate has not provided specific network configurations, and there is not enough data to conclude. However, there are indications of technical vulnerabilities within the system:

1. **Data traffic within the LAN is not encrypted:** The Directorate was asked if the data transfer within the LAN at the common counting stations is encrypted. The Directorate responded that they recommend the municipals to encrypt the connection from client to database within the LAN. The recommendation includes to use certificates, Active Directory, and replace username/password with NTLM/Kerberos/Windows authentication, see Question 1, Appendix I. Encryption is, however, not mandatory.

   The response is quite alarming. Based on the response, the municipals are free to decide whether they wish to encrypt the traffic or not. One can assume, due to simplicity (see the previous section), that encryption of data is not implemented. If EVA Skanning is installed and configured without any form of encryption in the local area network, anyone with access to the network can intercept the communication and obtain the information (e.g. man-in-the-middle attack).

2. **Username and password are stored in plaintext on the Windows clients:** The Directorate was asked how and where username and password for the database authentication are stored on the clients for the installation. According to the Directorate, username and password exist in "configuration files". For the election in 2019, username and password will be encrypted in a standard configuration by Data protection API (built-in in Windows), see Question 2, Appendix I.

   The reply indicates that until now, username and password have been stored in plaintext on the Windows clients. That allows anyone with access to the configuration file or to a configured client, to obtain the username and password without difficulty. Next, the attacker can connect to the database, and may alter the result without difficulties.

3. **In a small installation, the client (with database server installed) is connected to the Internet:** The EVA Jobbstyring client must be connected to the Internet to transfer the result to EVA Admin, and in a small installation the client which has EVA Jobbstyring installed has also the database server installed. In such a configuration, the client is subject to additional vulnerabilities from the Internet.

   The Directorate added that the client does not necessarily need to be connected to the Internet during scanning and verification, see Question 4, Appendix I. The client can run in *nødmodus*, and only be connected when the result needs to be transferred. Even though the client does not necessarily needs to be connected, it is unlikely that the municipals have configured the clients accordingly.

4. **The scanning providers have access to perform remote support:** According to a document published on Mimes Brønn[1], the scanning providers have access to perform support remotely. If this is the case, the scanning providers have access to EVA Skanning (and thereby the database) remotely.

   The response from the Directorate indicates that the municipals are responsible:

   > *The municipals and county councils are responsible for the practical conduction of the elections, including installation and configuration of the scanning solution, and the conduction of electronic ballot counting. The Directorate of Elections offers software and guidance related to use of the software* - see Question 6, Appendix I.

   The responses from the election officials varied. The majority of the election officials responded that the scanning operators do not have access to perform

[1] a public site for access requests, https://www.mimesbronn.no/nn/request/405/response/2439/attach/3/Signert%20kontrakt%20Evry%20Sladdet.pdf

remote support. Some responded that they did not know which access the scanning providers had. However, some of the election officials stated that the scanning operators did in fact have access to perform support remotely. Such a configuration decreases the level of security within the module and questions the integrity of the result.

The fact that such access restriction is not mandatory for all municipals contributes to weak security of EVA Skanning. If the Directorate holds no responsibility to how the municipals implement their systems, there is no guarantee that all municipals can guarantee the necessary level of security.

The configuration is installed 2 to 4 weeks prior to the election: According to the election officials, the EVA Skanning module is installed in the municipals 2 to 4 weeks prior to the election. This is to be able to perform training and testing according to the Election Regulations. During this period of time, access control and guards are implemented to secure the installation. Although access restriction is implemented, there will be opportunities to tamper with the hardware (e.g. cleaning personnel will have to enter). The system may therefore be exposed to an evil maid attack. An evil maid attack is a security exploit that physically targets an unattended computing device. An evil maid attack is an attack in which an attacker with physical access alters it in some undetectable way so that they can later access the device, or the data on it [Sch09].

Collectively, these bullet points indicate weak security within the EVA Skanning application, both in software and hardware. These indicators demonstrate that there is a need for auditing and verification of the system, in addition to emphasising the need of an open and transparent system.

3.4 Opaque electoral system

The Directorate claims the electoral system to be open and transparent. Information obtained throughout this study, indicate otherwise.

First, *Boken om EVA Skanning* is redacted due to security reasons (although the Directorate claims the information to be outdated). Second, the Directorate does not wish to share local area network configurations related to EVA Skanning, see Appendix G.2. Third, the Directorate denied the inquiry to test EVA Skanning at the university but offered instead a demonstration at their offices. In information security theory, such information is assumed public knowledge. According to Kerckhoffs's principle: *"a cryptosystem should be secure even if everything about the system, except the key, is public knowledge"* [Sha49]. This principle does not seem to apply for the Norwegian electoral system.

The lack of openness is problematic for many reasons. The electoral system is supposed to be transparent and open so that anyone can verify that the result is in fact correct. In order to verify a secure system, one must be granted access to research the system and corresponding infrastructure. Currently, the electoral system is transparent in the form of that anyone can attend the meetings of the electoral committee, and anyone can observe the ballot counting itself[2]. The electoral system is not transparent in the form of publishing system documentation, source code, and network configurations.

In a debate prior to the election in 2017, the managing director of the Directorate of Elections, Bjørn Berg, was asked if any third parties have evaluated or tested EVA Skanning prior to the election to ensure correct functionality and security. Berg replied:

> "*Our systems are penetration tested by the Norwegian National Security Authority (NSM). More specifically, the software is tested, but not the installation in the municipals. We (the Directorate) are responsible to assure quality of the system, in cooperation with the municipals, this is done by comprehensive testing prior to the election*". - Bjørn Berg on quality assurance of the EVA Skanning installation [Gun18].

This statement clarifies that there is no independent entity that controls the development or implementation of EVA Skanning. The Directorate of Elections are responsible for developing the system *and* controlling that it behaves according to the specifications. From a democratic perspective, such a role distribution is problematic and does not contribute to transparency or openness.

Furthermore, in the debate, Berg, stated that the source code and software implementation was fully open and available for anyone to verify. Berg said that after an election, the source code is published and available for all. This statement is not true. The most recent source code publicly available on the Internet is from 2013 [Gun18]. The source code from the election in 2017 is still not published, even though Berg stated specifically that it would be. When asked to further elaborate why the source code from 2017 is not published, the Directorate replied that no official request to publish the source code had been received. Therefore, the Directorate has prioritised to complete the source code for the election in 2019, see Question 9, Appendix I.

When asked what differences there are between a small and large installation, the Directorate responded that there were none in particular, other than that in a

[2]anyone can enter the common counting station and witness that the ballot counting is performed according to the regulations, however, there are cordons and guards to ensure security, https://www.regjeringen.no/contentassets/328b3cb156974d358f63319277a52837/valghandbok$_2$017$_b$*m.pdf*

small installation all components are installed on the same client, see Appendix C. When studying the architecture, quite significant difference appears. In a small installation, the client which is connected to the Internet, has all the components installed, including the database server. The counting itself is performed in the database, and when the client with the database server installed is connected to the Internet, specific security configurations must be activated to ensure security. In a large installation, on the other hand, it is only the computer which has EVA Jobbstyring installed that is connected to the Internet.

Nor the fact that in a large installation, the database must be configured to listen to external calls, was addressed. This may be considered a security vulnerability because anyone with the password can connect to the database if the database listens for external calls. Later, the Directorate specified that the comment stating that there are no differences in particular between small and large installation, was more directed toward the source code, and not the installation.

Nevertheless, the problem is that the system is not transparent and open for anyone to verify secure and correct implementation. These actions do not contribute to an open and transparent system, but rather justifies the assertion of an opaque electoral system. Although allowing qualified and non-qualified personnel to evaluate the technology used and degree of security may be viewed as a security risk, the important of such openness was demonstrated at DEFCON 2017 (see next section).

3.4.1 DEFCON 2017

DEFCON is one of the world's largest, longest-running, and best-known hacker conferences. In 2017, the conference featured a Voting Machine Hacking Village to demonstrate cyber vulnerabilities in the U.S. election infrastructure. The village contained over 25 pieces of election equipment infrastructure such as voting machines (electronic paperless voting machines), voter registration databases, and election office networks. The event was organised by several cyber, voting equipment, and national security experts, along with DEFCON founder Jeff Moss. The conference represented the first occasion where mainstream hackers were granted unrestricted access to explore and discover possible vulnerabilities in the electoral systems, previously there has been limited access to voting machine hardware. After the conference, a report describing the attacks and exploits was published, see Matt Blaze et al. [MB17].

The results from the conference were surprising. Every piece of equipment was effectively breached in some manner. Because of the previous limited access to test voter equipment vulnerabilities, there have been doubts if ordinary technologists have the knowledge and skills to discover and exploit the possible vulnerabilities. This conference demonstrated that participants with little prior knowledge and limited

tools were capable of breaching confidentiality, integrity, and availability of the systems [MB17].

In addition to providing voting equipment, the Village also implemented a mock virtual election official's office and network, called "cyber range", built in cooperation with a large U.S. election jurisdiction staff who ensured real-world likeness. The range provided a learning opportunity for regional and local leaders to better understand threats and vulnerabilities their systems are exposed for, in addition to how protect their networks best [MB17].

A limitation of the work performed in the village was that the Voting Village did not have access to any backend provisioning, counting, or voter registration systems. Such systems are generally difficult to acquire on the open market [MB17]. This limitation is quite significant, because the evidence from the 2016 election seems to indicate these machines were the primary target of Russian hacker attacks, not the voting machines themselves, see Appendix K.

Summarised, the most important findings were [MB17]:

- AVS WinVote model was the first voting machine to be breached, and that in matter of minutes. A vulnerability from 2003 let the machine to be controlled remotely, allowing changing of votes, observing who voters voted for, and shutting down the system. The vulnerability existed in the machine from 2003 - 2014.
- The same machine had default username and password of "admin" and "abcde". The authentication was universal, meaning it was found by a simple Google search, in addition to be unchangeable.
- Diebold Express 5000 was an electronic poll book used to check in voters at a polling station in Tennessee in 2008. The poll book was found to have been improperly decommissioned. The device was resold or recycled after the election, but the data stored - unencrypted files containing personal information, home residential addresses, and law enforcement officers - were not properly and securely removed.

The findings described above are not entirely new and ground-breaking as hackers and researchers have discovered similar vulnerabilities previously. The difference with this experiment, was allowing mainstream hackers more time and access to test a greater selection of election equipment than before.

First, the report concludes that voting systems may be hacked even with limited resources, time, and information. The participants had little or no previous experience

with voting machines and learned to find and exploit vulnerabilities in the matter of minutes and hours. The participants were not provided with proper documentation or tools but were still able to hack into the systems using mainstream tools and practices.

Second, the report concludes with a need for new policies. Although election security advocates have been arguing for such a change for a long time, the Village helped demonstrate the need for implementation of measures to secure U.S. election infrastructure.

Finally, previously, voting machine manufacturers have denied claims of insecure machines, some also claimed that the Voting Village did not simulate a "true" election setting. There is also a misconception that Internet is required for a successful hacking of a voting machine. Although creating an unprotected local network, demonstrates Internet as a vulnerability (WinVote), many of the systems' software and hardware components can be used to connect a device to the Internet, either prior to or after the election. These results show that one cannot take for granted statements from the voting equipment manufacturers [MB17].

3.4.2 Relevance to the Norwegian electoral system

Similarly, to the U.S election infrastructure, the Norwegian computer system used in elections have not been tested by ordinary technologists in a secure and controlled environment. Being that every piece of equipment gathered for DEFCON 2017 was effectively breached in some manner, indicate that other complex electoral system also may be vulnerable to attacks. Although the Norwegian election does not implement voting machines, election infrastructure such as electronic poll books and counting machines, are also vulnerable for attacks.

Based on these revelations, it would appear natural that the Directorate would release source code and system documentation for an independent evaluation of the system. A simple test of EVA Skanning software used in 2017, was not possible to conduct either, the inquiry to do so was denied by the Directorate.

According to Valg.no, system documentation and source code for the solution that will be used in 2019, will be published sometime during spring of 2019. However, the announcement specifies that part of the source code will be omitted from the publication due to security measures. If parts of the code are omitted, controlling the system is still not possible.

3.5 Recommendations for increased level of security of the EVA Skanning installation

Based on the findings presented in this chapter, there are indications of security vulnerabilities within EVA Skanning. Simple security measures may increase the level of security. Some recommendations that should be implemented are:

- Implement routines for developing system documentation to better verify that the system acts according to the specifications. System documentation will also be useful when testing the system, and allowing independent entities control the functionality and security.
- Allow an independent third party to study the source code and evaluate the level of security. An independent third party will analyse the code from a different perspective and may provide an objective view on the system.
- Penetration test the installation when the components are installed in the municipals. The municipals are responsible for securing the local area network and configuring the firewall, and the guidelines provided by the Directorate may not be detailed enough to secure the installation.
- Encrypt the traffic in the local area network. Encryption will help to avoid man-in-the-middle attacks, these attacks are useless if the attacker cannot read the information sent. Recommended encryption is asymmetric encryption for key exchange, such as RSA, and symmetric encryption for message transfer, such as AES. RSA is considered best practice for key exchange but is not efficient for transferring messages. When keys have been exchanged, symmetric message transfer with AES may be applied.
- Username and password for database authentication should be stored encrypted on the clients. SHA 256 is a secure hash function for storage of usernames and passwords.
- In a small installation, the database should be configured with named instances, and only listen for internal calls. In a small installation, the client connected to the firewall is installed with both EVA Skann and the database server. To secure the installation, measures such as named instances and internal calls are recommended.
- The database should be configured to only listen for a certain number of clients, the clients should be pre-determined. This is to avoid an attacker that has access to the local area network to send anything to the database. Such a measure strengthen the authentication beyond a username and password.

- The scanning providers (EVRY, Idox, and Indra) should not have access to perform remote support.
- The development of EVA Skanning should not be motivated by ease of implementation, but rather security. Although impossible to guarantee security, international standards of security must be fulfilled.

3.6 Summarised findings

To summarise, EVA Skanning is the Directorate's solution for electronic ballot counting. EVA Skanning consists of three Windows applications (EVA Jobbstyring, EVA Skann, and EVA Verifiser), a database server (Micosoft SQL Server), and a local area network. According to the Directorate of Election, there does not exist complete architecture or system description on EVA Skanning used in 2017. This is due to lack of guidelines and routines requiring such documentation. The information presented is therefore based on dialogue with representatives from the Directorate.

There are two possible configurations, small installation and large installation. A high-level illustration of the two configurations have been presented. The Directorate did not wish to further specify any specific database or firewall configurations. Standard Microsoft SQL database configurations have therefore been assumed. With regards to firewall configurations, according to the Directorate, these are subject to the municipals. The Directorate provides guidelines and recommendations, but the overall responsibility lies with the municipals. The election officials interviewed in the thesis did not wish to further elaborate on firewall configurations. Some officials added that they rely on the specifications provided by the Directorate to be sufficiently secure. These results may indicate confusion in relation to who is responsible for security of the implementation.

Furthermore, the findings show that the the development of the electoral system may not seem to be motivated by security, but rather by practical considerations. *Boken om EVA Skanning* discusses choice of technology, and justifies the selection of relational database due to ease of implementation in small municipals. The municipals are different in size, population, and level of knowledge, and requiring strict security measures would be inexpedient, according to the Directorate. Such commentary provides indications that security is not prioritised, and that there may be serious security vulnerabilities within the application. Security should not give way to ease of implementation. *Boken om EVA Skanning* and the responses provided by the Directorate, indicates that security is not prioritised when developing EVA Skanning.

Although, the acquired information is not sufficient to conclude, there are indicators of possible technical vulnerabilities within EVA Skanning. First, the data traffic

within the LAN is not encrypted, anyone with access to the network can easily intercept the communication and obtain the transmitted ballot information. Second, username and password for authentication between the clients and the database server may be stored in plaintext on the Windows clients. Anyone with access to the configuration file or a configured EVA client, may obtain the only authentication necessary to communicate with the database. Third, scanning providers may have access to EVA Skanning remotely to perform support.

Based on the publicly available information related to the technology used, the Norwegian electoral system may be considered non-transparent. Studying the technical requirements and capabilities of the Norwegian electoral system is challenging when there does not exist complete system documentation, and the Directorate has not published source code since 2013. The experiment at DEFCON showed serious vulnerabilities within the U.S electoral system. Although major differences must be noted in comparison to the Norwegian electoral system, there are remarks of relevance. Similarly, to the U.S there have been limited openness for mainstream hackers to test and research possible security vulnerabilities within the Norwegian electoral system. It is in everyone's interest that the system is as secure and possible, and public penetration testing under arranged circumstances is an optimal form of research. The Directorate denied such an inquiry.

Currently, the public cannot verify the level of security within the Norwegian electoral system. Publication of source code and system documentation will contribute to increased transparency and openness. The Directorate has stated that source code and system documentation for the 2019 election will be published in April 2019. Further work to research requirements and capabilities of EVA Skanning is recommended for future master's students in 2019.

Finally, recommendations for increased level of security of the EVA Skanning application have been presented. The Directorate should implement routines for developing system documentation, allow an independent third party to penetration test the installation, encrypt the data traffic within the LAN, store username and password encrypted, and not allow scanning providers access to perform support remotely.

Based on these findings, one must assume that reliable error detection mechanisms are implemented, to detect possible result manipulation. This is further discussed in the subsequent chapter.

Chapter 4
Error detection mechanisms

In the previous chapter, the level of security within EVA Skanning was discussed. Based on the findings, there are indications of weak security within the module and how it is installed. Therefore, mechanisms to detect errors are imperative for a democratic electoral system.

This chapter assesses the reliability and performance of the currently implemented error detection mechanisms in Norwegian electoral system. To assess the reliability and performance of the error detection mechanisms, qualitative research in form of interviews and quantitative research in form of experimental testing are performed.

First, a definition of a reliable error detection mechanism is introduced. Second a presentation and analysis of the currently implemented error detection mechanisms are provided. Finally, an assessment of the reliability of the mechanisms implemented to detect errors in the Norwegian electoral system is presented.

4.1 Reliable error detection mechanisms

4.1.1 Definition of reliability and performance

Eight dimensions of quality management can be used to analyse product characteristics. Some of the dimensions are mutually reinforcing, whereas others are not - improvement in one may be at the expense of others [Gar87]. The dimensions *performance* and *reliability* are very much mutually reinforced when discussing the product of error detection mechanisms. Performance refers to a product's primary operating characteristics, whereas reliability is the likelihood that a product will not fail within a specific time period [Gar87]. When discussing error detection mechanisms, reliability refers to *if* a mechanism detects errors, whereas performance refers to *how well* errors are detected. When discussing electoral systems, the term reliability is mostly used, due to that an error detection mechanism is either reliable (i.e. detects all errors) or is not reliable (i.e. does not detect all errors).

When technology is incorporated into an electoral system, reliable error detection mechanisms must be implemented to determine if any errors have occurred, and to ensure integrity of the result. According to Lindeman et al. (2012) [LS12], a reliable error detection mechanism for an electoral system is defined as a mechanism that enforces *software-independence*. Software-independence means that an undetected error in software must be incapable of causing an undetectable error in the election result. Such an error detection mechanism may take form as an independent comparable result. An independent comparable result in an electoral system may be obtained by counting ballots by hand or develop an independent computer system that performs the same operations as the original system.

4.1.2 Manual ballot counting versus electronic ballot counting

The question of whether manual or electronic ballot counting provides the most reliable result is widely discussed. Election officials interviewed in this master's thesis strongly believe that electronic ballot counting provides the most reliable result, see Appendix H. This assertion is based on their own experience with ballot counting. Their experience show that manual hand count is not as reliable as electronic ballot counting due to that the ballots are counted during the evening, after a long Election Day, and people may not be fully concentrated. There exists no empirical evidence of this assertion, but in their opinion, given correct implementation, the electronic result provided by EVA Skanning is more reliable than manual counting.

The assertion is supported by a study performed at Rice University in 2012, see Goggin et al. (2012) [GBG12]. The study showed empirically that hand counting of votes in post-election audit or recount procedures can result in error rates of up to 2%. 2% is a significantly high error rate, and could be able to influence the winner(s) of the election[1]. Therefore, given that the machines count correctly, electronic ballot counting provides a more reliable and correct result. One must note, however, that the study was conducted using U.S. ballots. These ballots are more difficult to count than Norwegian ballots due to the U.S ballots being more complex. There are several selections on one ballot, in Norway, the ballots are only sorted based on party (heading). Therefore, the results may not be applicable to the Norwegian electoral system.

Academics within the field of information security, on the other hand, often hold manual counting to be more reliable. This is justified by the fact that complex software systems are notoriously difficult to secure. One cannot guarantee that a system is perfectly secured [CYB17]. Furthermore, the consequences of software errors, hardware errors, or result manipulation are more severe than the consequences

[1] the selected government in Norway often depends on which parties pass or not pass the election threshold, 2% imbalance may affect the final result

of the occasional human error. Human errors will, given a sufficiently large selection, statistically distribute themselves equally to all parties, according to normal distribution [Zie02]. Software errors, hardware errors, or result manipulation, on the other hand, may consistently result in the same imbalance, and therefore the consequences of these types of errors are more severe than the consequences of human errors [GCJ+12]. Consequently, ballots cannot *only* be counted by machine. In fact, in the Election Manual used in 2017, the Ministry informs that:

> *The fact that ballot papers are scanned does not change the requirement for two rounds of counting. Errors may occur even when using this type of technical aid* [oLGM17].

In the discussion on manual versus electronic ballot counting, one might be tempted to analyse types of errors possible to obtain. In electronic ballot counting, errors may be classified as randomised errors (e.g. mechanical errors), systematic unintentional errors (e.g. software errors), and intentional errors or attacks (e.g. database manipulation). In manual ballot counting, two of the same categories applies: randomised errors (e.g. human errors) and intentional errors or attacks (e.g. manual manipulation). Although these errors may be classified differently, detection mechanisms are independent of error type. A reliable error detection mechanism provides an independent result that is compared to the original result to evaluate if an error has occurred. What type of error that may occur, is irrelevant.

There exists no empirical evidence of which method (manual or electronic ballot counting) is most reliable in Norway. Although, all errors and deviations between preliminary and final counts are protocolled by the election officials, these statistics cannot yet be used to determine reliability of the methods. Error rate of manual counting and error rate using EVA Skanning must first be empirically researched. Error rate of manual counting may be obtained by applying similar approach as Goggin et al., using Norwegian ballots. On the contrary, error rate of EVA Skanning is more difficult to obtain. A correctly configured system will have an error rate of zero. The problem arises when the software contains a systematic error in software or deliberate manipulation is applied. Therefore, when using EVA Skanning to count ballots, reliable error detection mechanisms must be implemented to ensure integrity of the result, nonetheless.

This master thesis aims at assessing the reliability and performance of the currently implemented error detection mechanisms in the Norwegian electoral system. The following section presents and analyses the implemented error detection mechanisms based on the definition provided in Chapter 4.1.1.

4.2 Implemented error detection mechanisms

4.2.1 Introduction

According to *valg.no*, the electoral system implements control mechanisms that ensure that compromise of EVA Skanning itself is not sufficient to affect the result:

> *In addition to securing the administrative IT system EVA, there are additional control mechanisms in the conduction of the election that ensures that compromise of the IT system itself is not sufficient to affect the result - the control mechanisms are not bound to if or which IT solutions are in use* [Val17].

Which mechanisms and how they are implemented are not described. Furthermore, in a debate prior to the election in 2017, the managing director of the Directorate of Elections, Bjørn Berg, stated:

> "*The system (EVA Skanning) may be hacked, our guarantee are the built-in control mechanisms (...) these are mechanisms that ensures that attacks are revealed when someone attempts to contact our systems*" - Bjørn Berg, Directorate of Elections [Gun18].

In this master's thesis, a review and discussion of the currently implemented error detection performance for potential counting system malpractice is performed. To research error detection mechanisms, in-depth interviews with relevant groups of people have been conducted.

First, the Ministry of Local Government and Modernisation and the Directorate of Elections were interviewed. The objective was to research how errors shall be detected in accordance to the Election Act and the Electoral Regulations. The interview guide may be found in Appendix C. Next, election officials in a representative selection of municipals were interviewed. This to research how error detection mechanisms are in fact implemented and whether they are similar in all municipals. The interview guide may be found in Appendix H. An excerpt of the questions and their corresponding answers are included in the following sections.

In addition to the interviews, an experimental setup has been tested to research how errors are detected in practice. The methodology in its entirety has been described in Chapter 2.

4.2.2 How ballot counting is performed

In an election, ballots are divided into two groups: 1) advance votes and 2) Election Day votes. The Election Act states that all ballots must be counted at least twice: a) one preliminary count and b) one final count. The Election Act, however, does not specify how to perform the counts. There are two options: i) manually or ii) electronically. Manual counting is defined as counting ballots by hand. Electronic counting is defined as using EVA Skanning. In addition, it is mandatory to perform an urn count on all votes. Urn count is not statutory in the Election Act, but mandatory prior to the preliminary count.

Question 5, Appendix H: How is ballot counting performed in your municipal?

All participating election officials were asked how they perform ballot counting in their municipal. In the 2017 election, it was mandatory to count all ballots manually at least once. This is reflected in the election officials' answers. All of the asked officials responded that in 2017, the preliminary count was performed manually, and the final count was performed electronically, see Figure 4.1. This was the case for both advance votes and Election Day votes.

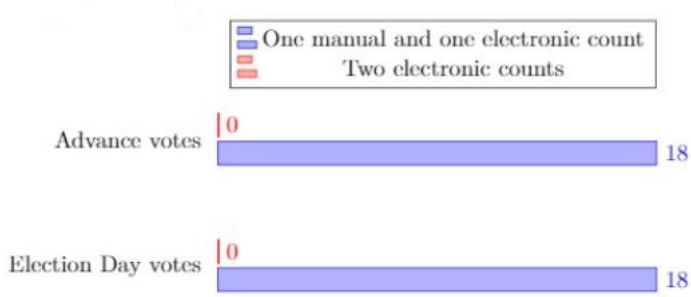


Figure 4.1: How ballot counting was performed in 2017

The majority of the election officials added that, normally, advance votes were counted twice electronically. Approximately half of the election officials added that Election Day votes normally were counted twice electronically as well, see Figure 4.2.

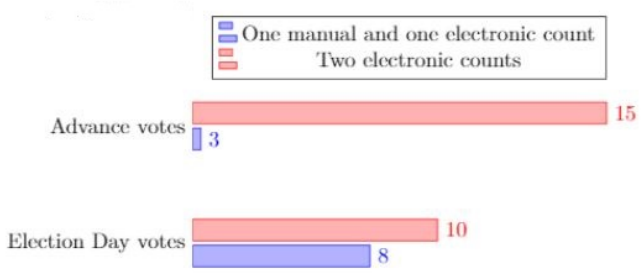


Figure 4.2: How ballot counting was performed before 2017

When asked how they expected to perform ballot counting in the future, the majority answered that they wished to continue to count advance votes electronically twice. Some added that two electronic counts of Election Day votes would be preferable in the future, while others stated that a manual preliminary count is efficient and will continue to do so. Three election officials mentioned the increasing threat of election manipulation and would therefore continue to count manually at least once. According to them, a manual count ensures a trustworthy and comparable result, and thereby serves as a control mechanism.

4.2.3 Consultation memorandum

Question 25, Appendix C: How shall counting be performed in the next elections - manually and/or electronically?

The representatives from the Ministry and the Directorate were also asked how ballot counting is to be performed in future elections. The requirement for manual preliminary counting only applied to the election in 2017 and ended 31 December 2017. The Election Act and the Electoral Regulations do not prevent both the preliminary and final counting from being performed by scanning. The municipalities can thus, according to the current regulations, choose to either perform both counts manually, both counts by machine, or combine manual and machine counting.

At the time of the interview, 11 October, the Ministry was still working on the evaluation from the previous election. The Ministry stated that they would decide how they would proceed with the regulation sometime during the fall of 2018.

1 November, the Ministry released a consultation memorandum, see Appendix B. The Ministry proposed to stipulate in the Electoral Regulations that the preliminary counting of both advance votes and electoral votes (votes cast on Election Day) must be handled manually. In addition, the Ministry proposed to regulate a routine for

deviations between preliminary counting and final counting, if final counting is done by machine scanning. Currently, there are no statutory or regulatory procedures for deviations between preliminary and final counting, see Appendix B. Below, an excerpt from the consultation memorandum is included:

> It is important to avoid uncertainty regarding implementation of key election tasks such as ballot counting. The Ministry therefore proposes to regulate a provision in the Electoral Regulations that the preliminary counting pursuant to sections 10-4 (5) and 10-5 of the Election Act must be done by manual counting. Manual counting means that counting is done by hand without the use of machines. That the Ministry proposes that the preliminary counting to be done manually, and not the final, is due to practical considerations, as the preliminary counting of electoral votes may take place at the polling stations. Final counting must take place under the supervision of the electoral committee and therefore does not take place at the polling stations.
>
> That the election is conducted in a correct and trustworthy manner is essential for democracy. To regulate a requirement that the preliminary counting should be done by manual counting will, to a greater extent than with the current regulations, help ensure two independent counts and give legitimacy to the election results.
>
> The Ministry proposes at the same time to determine a routine for deviations between preliminary counting and final counting, if final counting is performed electronically by scanning. The proposal implies that a recount will be performed given deviation between preliminary count and final count. The second machine count shall not be performed by the same persons who performed the final count originally. The Ministry does not consider it necessary to regulate a deviation routine if both counts occur manually.
>
> Security in the electoral process is an important prerequisite for the population to trust the administration and political institutions. The Directorate of Elections is working on attending to and strengthen the security of EVA Skanning towards the municipal and county council elections in 2019. The Directorate will provide municipals and counties with written instructions on the physical and technical security measures that should be implemented when using EVA Skanning. The Ministry recommends that the municipalities and county authorities follow the recommended measures.

In the consultation memorandum published by the Ministry of Local Government and Modernisation, the Ministry proposes two changes in the Electoral Regulation. New § 37a shall read:

> § 37a - Preliminary counting of ballot papers
>
> 1. The preliminary counting of ballot papers pursuant to section 10-4 (5) and section 10-5 of the Electoral Act shall be by manual counting.
> 2. In the event of a deviation between a preliminary and a final counting made by machine, the result shall be recounted. New machine count cannot be made by the same persons who performed final counting.

Evaluation of the proposal

At the time of the interview with the Ministry and Directorate, the Ministry had not yet decided if at least one manual count would be a requirement for future elections. Three weeks after the interview, a proposal was sent on hearing.

The first proposal (1), requires that all municipals must perform at least one manual count. This is considered an improved security measure. Requiring at least one manual count provides the municipals with a reliable comparable result as control mechanism. With two electronic counts, software-independence cannot be guaranteed.

The second proposal (2), however, contradicts the first one. The first sentence in the second proposal states that given deviation, there shall be a recount. The second sentence allows a second machine count, which undermines the legitimacy of the manual count. If the second machine count equals the first machine count, but differs from the manual count, the registered result will be, according to election officials, the result produced by the machine count, see Appendix H.

This is in direct contrast to the first proposal, where a manual count is introduced to control the machine count. In addition to contradicting the first proposal, the second sentence indicates that it is the machine operator's fault that the machine counts incorrectly. Stating that the recount must be performed by different personnel, suggests that the fault lies with the people, not the machine. This insinuation is quite alarming.

Based on this master's thesis, an official reply from the Norwegian University of Science and Technology, Department of Information Security and Communication Technology, was constructed. The reply may be found in Appendix J.

4.2.4 How software errors, hardware errors, and result manipulation are detected

Both the representatives from the Ministry and the Directorate and the election officials were asked to elaborate on how errors are currently detected in the Norwegian electoral system.

Question 15, Appendix C: If both counts are performed electronically, how are errors detected?

First, the Ministry emphasised that the municipals have a freedom of choice regarding how they wish to perform ballot counting. This is due to the municipals being quite different in both size and population. It would be inexpedient to decide one correct method. Every municipal is divided into precincts, each precinct has one polling station. Some are too small to count the ballots without compromising anonymity: if a precinct has less than 100 ballots, the election in that precinct is no longer anonymous. These ballots must then be transferred to another precinct for counting. Therefore, there is a need for local adjustments when counting ballots.

The most common procedure is to conduct the preliminary count locally at the polling station, and later conduct the final count for the entire municipal centrally at a common counting station. According to the Ministry, the idea with such a procedure is to provide a control mechanism. Prior to the 2017 election the Ministry saw a tendency that many municipalities would not perform the preliminary count at the polling station, but rather perform both counts centrally, and some also considered performing both counts electronically with EVA Skanning. The Ministry then observed that the control mechanism was weakened. The decision to implement minimum one manual count in the 2017 election was based on this tendency.

Furthermore, according to the Ministry, if both counts are performed electronically, the primary control mechanism is that the municipals are aware of the result from the preliminary count. The result exists both in the protocols and in EVA Admin. The municipals perform a comparison of both tallies and can make assessments depending on deviation. According to the Ministry, if the results are the same, the objective of the second count is fulfilled. Two equal results verify correct counting.

The Ministry continued by specifying other control mechanisms. First, there exist manual control mechanisms. An important job of the ballot counters is to pay attention when counting: when they scroll through ballots or when they see the scanner goes through a batch of ballots, they may observe if something seems out of proportion. Second, the testing and training prior to the election ensures that the public can trust the produced result. Third, all decisions and deviations are protocolled. These protocols are public. Finally, there are several control instances:

the counties control the municipals, the Ministry controls the counties, and the Parliament controls the Ministry.

Evaluation of the response

According to the Ministry, the most important control mechanisms is that the election implements two counts: preliminary and final count. Even though both counts are performed electronically, and provide equal results, the objective is reached: two equal results determine that the result is correct.

Such a statement is far from reassuring. According to the Ministry, result integrity is dependent on comparing two electronic results produced by the same software and hardware. Comparing two electronic results produced by the same software and hardware cannot be defined as a reliable error detection mechanism. According to Lindeman et al. (2012) [LS12], a reliable error detection mechanism is a mechanism that enforces software-independence. Comparing two electronic results performed with the same software does not guarantee software-independence. For this measure to be reliable, an independently developed system, which performs the same operations, should be deployed. The comparison of two results produced by two independently developed systems would, enforce software-independence. Comparing two results performed with the same software, does not guarantee software-independence.

Furthermore, the Ministry addresses manual control mechanisms. These cannot be considered reliable error detection mechanisms either. EVA Skanning interprets the ballots quickly, and as long as the deviations are not too different from previous years, errors are difficult to detect by only observing the scanner. The training and testing prior to the election is well-documented. The Directorate arranges training seminars in Oslo for all election officials, and all municipals are encouraged to participate in the trial elections ahead of the election to ensure correct installation. These seminars and the testing are important and contributes to a quality assured electoral system. However, according to the election officials, no testing is performed on Election Day itself. An attacker may be able to tamper with the machines (which is set up several weeks before the election) and activate the malware on the day of the election. Such an attack would not be detected by the error detection mechanisms described by the Ministry and the Directorate.

Question 18, Appendix H: How does your municipal detect errors?

The election officials were asked a similar question. When asked how errors are detected in their municipal, the responses varied. The question was in some cases vague and had to be clarified in regard to what type of error was in question. The interviewer clarified that all counting errors were of relevance, both errors resulted from manual mistakes and errors resulted from software or hardware configurations.

A summary of the responses from the election officials regarding implemented error detection mechanisms is illustrated in Figure 4.3.

All election officials replied that in 2017, the results from the manual count and the electronic count were compared to each other to check if they were equal. Based on the results, they decide if a recount is necessary. Each municipality defines a deviation limit such that if the deviation between the first and the second count is larger than the set deviation limit, a recount must be performed. The deviation limit varies from municipal to municipal, ranging from a deviation of 1 ballot to 3 ballots to 5 ballots per thousand ballot. One municipal had a deviation limit on 10 per thousand. When asked how the municipals perform the recount, all replied electronically.

The election officials were again challenged on how errors are detected if the final count and the recount (given sufficient deviation) are both performed electronically. First, one responded that the recount is performed with different machines to ensure correct result. If there exists an error on one of the scanners, this would be detected by using a different one. Second, if the result from the recount matched the original electronic result, they assumed the result was correct. They trust the software developed by the Directorate of Elections and does not consider it their job to detect if the system is flawed. Some election officials added that in their experience, humans were more likely to count incorrect than machines. This was explained by the challenge to concentrate under stress and after a long Election Day. In addition, in their experience, the electronic counting system was improved when the system became state-owned. Therefore, they viewed the result produced by the machine more likely to be correct than the result reported by humans. Third, many election officials replied that they use their previous election results to compare to the current one. If suddenly one party receives abnormally many votes (or opposite), they would detect and report it. However, according to the election officials, if the deviations were small, they would probably not detect it. Finally, all municipals described thorough and well-planed training and testing prior to the election to ensure the machines counted correctly. None of the election officials mentioned testing on Election Day itself.

To those who responded that they wanted to perform two electronic tallies in future elections, the same question as in the paragraph above was asked: How are errors detected if both tallies are performed electronically? Similar responses were provided: they trust the machines to count correctly, and if something abnormally were to happen with the result, they would report it. However, if there would be small deviations from previous elections many responded they would probably not detect errors.

Finally, two new error detection mechanisms were pointed out. First, the urn count prior to the preliminary count serves a comparable result to determine that the number of ballots cast, and the number of votes counted, are equal. The urn count is not party distributed but indicates how many people have voted. The urn count is performed manually. Second, the control count performed by the county electoral committee. Note that control count is only performed in county council and parliamentary elections, not in municipal elections. The control count is often done in the largest municipality in the county and is performed using the same hardware and software as in the final count performed by the municipality.

An overview of implemented error detection mechanisms can be seen in Figure 4.3.

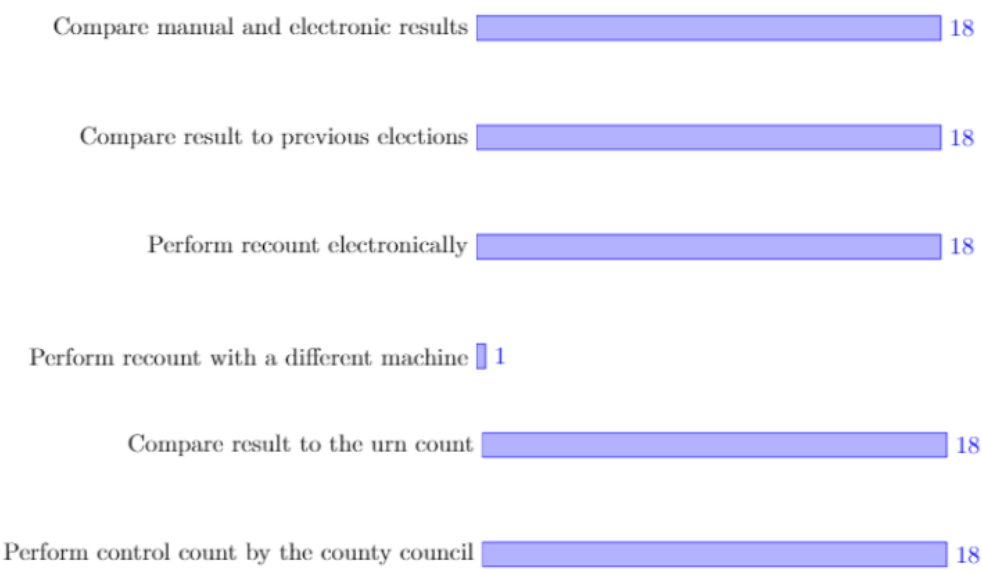


Figure 4.3: How software errors, hardware errors, and result manipulation are detected, according to the election officials

Evaluation of the responses

According to the election officials, there are several error detection mechanisms implemented. The reliability of these are further discussed:

- **Compare manual and electronic result:** The reliability of comparing the manual and electronic results depends on the subsequent actions. If there

exists a deviation larger than the set deviation limit, a recount is performed. According to the majority of the election officials, the recount is often performed electronically. If so, the manual result has no value, and the comparison is not a reliable error detection mechanism (see the following bullet point).

– **Electronic recount:** To demonstrate why electronic recount are not reliable for error detection, a numerical example is provided.

  When counting ballots, the ballots are divided into batches to simplify manual counting. Normally one batch equals 1,000 ballots. Let the result from a manual count be $Venstre = 1,000$ votes. Given an error in software, hardware, or deliberate manipulation, the result from the electronic count is $Venstre = 1,010$ votes. The election committee observes the deviation, and performs a recount. Electronically. The result is once again $Venstre = 1,010$ votes. Based on the responses from the interviews with election officials and representatives from the Ministry of Local Government and Modernisation and the Directorate of Elections, the result $Venstre = 1,010$ is registered. If the same error is propagated equally at all common counting stations, such an error can alter the final result. The error may contribute to a party passing not passing the election threshold. In a Norwegian election, which parties are passing the election threshold is a determining factor for choice of government.

  A common argument for electronic ballot counting is that humans are more likely to make errors when counting ballots than machines. The ballots are counted during the evening, after a long Election Day, and people may not be fully concentrated. Therefore, given that the machines count correctly, electronic ballot counting provides a more reliable and correct result.

  An argument against electronic ballot counting is that the consequences of software errors are more serious than the consequences of human errors. Human errors will, given a sufficiently large selection, statistically distribute themselves equally to all parties, according to normal distribution [Zie02]. A software error exemplified in the paragraph above, a hardware error, or result manipulation, on the other hand, will continue to count incorrect for that one party, and possibly alter the election result. An error detection mechanism that does not provide an independent, comparable result cannot be considered reliable.

– **Compare final result to previous elections:** If the deviation from the final result differs abnormally (one or several parties receive significantly more or less votes than normal) from the results from previous elections, the final result is reported and recounted, electronically.

  Many election officials mentioned experience and knowledge of election history in their municipal as important factors when working with ballot counting. However, if there are small deviations, these will not be detected based on previous elections.

This error detection mechanism helps to detect major imbalances, but cannot be considered reliable to detect smaller deviations.

- **Perform recount with a different machine:** One election official replied that the recount is performed with a different machine. This is to detect if there is a hardware error in the scanner used for the final count. This argument is problematic as well. If there is a hardware vulnerability in a machine, the vulnerability is in many cases propagated onto all machines of the same production cycle. In addition, such a measure will not detect errors resulting from other stages in the scanning process. Scanning the ballots with a different scanner is not likely to detect errors because the same errors will most likely be propagated onto all scanners at the counting station, or the result manipulation may be performed in a later stage within the process (e.g. within the database).
- **Compare final result to urn count:** A common argument for electronic recount is that the result of the final count is also compared to the original urn count. The urn count provides a comparable result (meaning an independent secondary tally) to number of people who have cast a vote, but does not provide a comparable party distribution. Unfortunately, such a comparison no longer relevant if the electronic count is still prioritised. Therefore, the urn count error detection mechanism may be considered not reliable (see the second bullet point).
- **The county councils perform a control count:** In county council and parliamentary elections, the county council performs control counts. These counts cannot be assessed as reliable detection mechanisms, due to that the control counts are often performed in the same counting station and with the same equipment as in the final count. Such a recount does not provide an independent and comparable result.

To summarise, none of the error detection mechanisms mentioned by the Ministry, the Directorate, or the election officials can be considered reliable error detection mechanisms, following the definition from Section 4.1.1.

Question 20, Appendix C: In Appendix A, "routines for random sampling of ballots" is listed to explain how errors are detected. How is this implemented?

In a document provided by the Directorate of Elections, see Appendix A, random sampling is listed to explain how counting errors are detected. Further specification of which algorithm is used or how this is implemented is not included.

According to the Directorate, random sampling of ballots is a guideline they wish to provide, but is not yet implemented. When asked what the routine consists of,

the Directorate explained that they wish to make a selection of scanned ballots and count manually to investigate correctness of the result. They had not yet defined which statistical algorithm to use to select the ballots for random sampling. These specifications will be a part of the documentation that will be published in 2019, according to the Directorate.

When asked if the Directorate has knowledge of risk-limiting audits, the answer was no.

Evaluation of the response

Although, the Directorate is not aware of the term *risk-limiting audit*, the answer indicates that the concept is known. The fact that the Directorate seeks to implement a risk-limiting audit algorithm is positive for future error detection in the Norwegian electoral system. Nevertheless, random sampling of ballots cannot be considered a currently implemented error detection mechanism.

4.3 Experimental testing of EVA Skanning

4.3.1 Introduction

The objective of the experiment was to research how software errors, hardware errors, and result manipulation are detected in practice, when scanning ballots, and thereby creating a foundation for evaluating the reliability and performance of the implemented error detection mechanisms.

The experiment consisted of using EVA Skanning to interpret and count 15 ballot papers. 12 of the ballots were stamped, whereas 3 were not. This was to check if correct number of ballots were sent to EVA Verification. All ballots were placed in and run through the scanner 4 times. The experimental setup is illustrated in Figure 4.4. The corresponding results are presented in Table 4.1. The software used in the experiment, was in the developing phase, hence errors were to be expected. How an incorrect result was detected, was of interest.

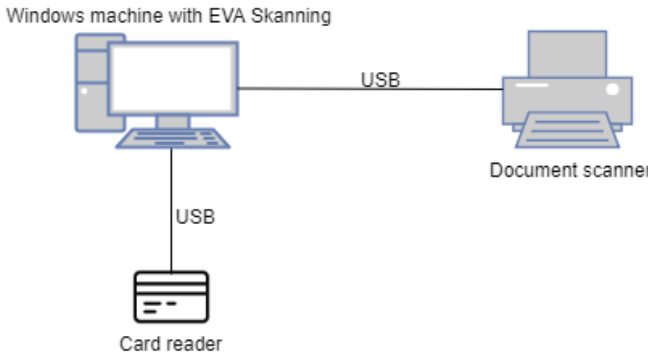


Figure 4.4: Experimental setup of EVA Skanning

4.3.2 Results

Table 4.1: Results from experimental setup

	Number of ballots scanned	**Expected number of ballots to verification**	**Result from EVA Skanning**	**Number of ballots to verification**
Round 1	15	3	13	2
Round 2	15	3	17	17
Round 3	15	3	14	3
Round 4	8	3	8	3

First round: The manual count showed 15 ballots, whereas 3 of them should be sent to verification (3 ballots did not have stamp). The first round in EVA Skanning showed 13 ballots in total, whereas 2 of them were sent to verification. The result was not correct.

Second round: The second time, the result showed 17 ballots, whereas all 17 were sent to verification. This was quite a surprise. Still, only 15 ballots were scanned and only 3 were supposed to be sent to verification.

Third round: The third time, 14 ballots were counted by EVA Skanning, whereas 3 were sent to verification. Still, the result from the system turned out incorrect.

Fourth round: Earlier in the day, the system had counted correctly when 8 ballots had been scanned. In the fourth round, only 8 ballots were scanned, whereas 3 should be sent to verification. Now, EVA Skanning counted correctly, and sent the correct

number to verification. The Directorate concluded that the software was not able to interpret too many ballots in one round.

4.3.3 Discussion

All ballots were counted manually prior to the scanning. This provided a foundation to determine if the scanner counted correctly or not. The manual count may be viewed as a preliminary count. After the ballot scanning, the two results were compared (as they would be in an election). The mean deviation from all four rounds was 1.25 ballots difference (83 ballots per thousand). Such a deviation would normally lead to a recount. In this experiment, two recounts (electronically) were performed with the same number of ballots. None of the recounts provided equal results. Therefore, a manual count was performed to ensure that there was in fact 15 ballots in the batch.

One must note that the software was in a developing phase during the experiment, and that such errors are not normal to obtain during testing prior to an election. The Directorate stated "*we can almost guarantee that this would not happen on Election Day. The system undergoes intensive testing: unit tests, integration tests, and acceptance test*". Nevertheless, the interesting result to notice, is that the preliminary manual count helped to determine that the result was incorrect. Furthermore, a recount was performed manually to determine if the preliminary count was indeed correct. EVA Skanning was not trustworthy to determine the correct result.

It is understandable that in batches of 1000 ballots, it is more difficult to determine if the manual count is in fact correct. However, the consequences of these manual errors are less than the consequences of major or minor computerised errors. The manual errors will statistically distribute themselves equally to all parties, given that the selection is sufficiently large. It is impossible to guarantee that the electronic ballot counting result is correct without a manual comparable result. If the recount is performed electronically as well, the manual control result is irrelevant.

The conclusive remarks indicate that a manual preliminary result is important to obtain a reliable comparable result. In addition, a recount cannot only be performed electronically. Such an action undermines the preliminary manual result and contributes to increase the risk of result manipulation. A post-election risk-limiting audits may be applied to determine probability of incorrect result and provide a reliable comparable result.

4.4 Assessment of reliability of implemented error detection mechanisms in the Norwegian electoral system

According to academics within the field of information security, a reliable error detection mechanism is defined as a mechanism that ensures software-independence. That involves producing a reliable comparable result such as a manual ballot count or a result produced from an independently developed system that performs the same operations.

The official website of the Directorate of Elections state that the electoral system does implement control mechanism to ensure that the compromise of EVA Skanning is not sufficient in itself to compromise the election result. Based on the findings from the interviews, the currently implemented error detection mechanisms cannot be considered reliable.

The primary error detection mechanisms is to compare the preliminary and final result. If both counts are performed electronically, software-independence is not fulfilled. In the consultation memorandum, the Ministry suggests making a preliminary manual count mandatory. This is to produce a reliable comparable result to the result produced by EVA Skanning. Such a measure may improve the error detection performance, but only if the recount is performed manually. The second proposal in the consultation memorandum suggests, however, that the recount may be performed electronically. If this were to be implemented, the preliminary count holds no value.

Alternative error detection mechanisms were introduced by the election officials, such as compare the results to previous elections, compare the results to the urn count, and perform control count by the county council. However, none of these measures ensure software-integrity or a reliable comparable result. The experimental test of EVA Skanning showed that in practice, one cannot guarantee that EVA Skanning has counted correctly without performing a manual control count. In consequence, the reliability of the currently implemented error detection mechanisms is low.

Based on the results, the Norwegian electoral system should implement a more reliable error detection mechanism. The subsequent chapter suggests implementation of risk-limiting audits to provide an "intelligent" reliable comparable result. According to related literature, the most reliable and practical method to achieve reliable error detection is through an approach called risk-limiting audits [GCJ+12] [CYB17] [LS12]. The effect of risk-limiting audits is not to eliminate software vulnerabilities, but to ensure that the integrity of the election outcome does not depend on the herculean task of securing every software component in the system.

Chapter 5
Risk-limiting audits

Chapter 4 presents an assessment of the currently implemented error detection mechanisms in the Norwegian electoral system. The assessment shows that the reliability of the error detection mechanisms is low. The currently implemented mechanisms cannot unambiguously guarantee that the final result is correct. Therefore, the Norwegian electoral system requires implementation of a reliable error detection mechanism.

A reliable error detection may take many forms, however, one concept is analysed and discussed in this thesis: risk-limiting audits. Risk-limiting audits are considered to be best-practice for reliable error detection, but are currently not implemented in the Norwegian electoral system. This chapter analyses the concept's degree of applicability to the Norwegian electoral system. The analysis is based on a qualitative study of the characteristics of the algorithms. A quantitative experiment would have been preferable; however, ballot scanners and ballots were not possible to obtain during the study.

First the concept's definition is introduced, then two algorithms that may be appropriate for the Norwegian electoral system are discussed, and finally, an analysis of the risk-limiting audits' degree of applicability.

5.1 What is a risk-limiting audit?

5.1.1 Definition

Risk-limiting audits are used in elections where ballots are counted electronically. They provide statistical assurance that election outcomes are correct by manually examining portions of the audit trail, either paper ballots or voter-verifiable paper records. Risk-limiting audits do not guarantee correct electoral result, but have a high probability of detecting an incorrect result [LS12]. Risk-limiting audits are based on manual counts of statistical samples of paper ballots, which are stored from

election day to the time of the audit. It tests whether the election result identified the correct winner(s). Specifically, if the samples show few discrepancies, the public knows that there is a limited risk of the initial result being wrong. If the samples find substantial discrepancies, the risk-limiting audit requires a 100% recount by hand, to identify the correct winner(s) [Far12]. According to Goodman et al. (2012), risk-limiting audits must be conducted even if both manual and electronic counts are performed [GCJ+12].

The simplest form of a risk-limiting audit is an accurate full hand tally of a reliable audit trail. A full hand tally will reveal the correct result (assuming no human errors). However, such a count is resource demanding: examining fewer ballots can provide strong evidence for a correct result, given that the ballots are chosen at random by suitable means. Such a method is described as an "intelligent" incremental recount that stops when the audit yields sufficiently strong evidence of correct result. As long as the audit does not provide sufficiently strong evidence, more ballots are manually inspected, potentially progressing to a full hand tally [LS12].

"Sufficiently strong" is defined by the *risk limit*, the largest probability that the audit will stop when the original outcome is in fact wrong [LS12]. A smaller risk limit requires stronger evidence that the outcome is correct: the audit examines more ballots if the risk limit (margin) is 1% than if it is 10%. The risk limit is *not* the probability that the result after auditing is wrong. If the original result is wrong, the risk limit is the probability of not correcting it. Risk-limiting audits improve the outcome if and only if it leads to a full hand tally that disagrees with the original outcome.

5.1.2 Random sampling

A prerequisite for risk-limiting audits is random sampling with replacements. Random sampling is a concept that requires further clarification.

A requirement to obtain public confidence in a random selection, is ensuring that observers can verify the selection is fair, meaning all ballots are equally likely to be selected in each draw. Methods such as an "arbitrary" selection of paper ballots (little chance of confirming that each ballot is only represented once and that they are adequately mixed), proprietary software such as Excel, or any source of commonly believed randomness (cannot readily be checked) are not trustworthy for a random selection. An optimal random number generator often has two features: a physical source of randomness (e.g. dice rolls) and inputs form multiple parties represented in the contest [LS12]. *Pseudo-random number generator* (PRNG) is an efficient an transparent method to generate "pseudo-random" numbers. PRNG can generate arbitrarily many pseudo-random numbers from a "seed" generated by a mechanical method (such as dice roll) [CWD06]. PRNG has a deterministic output given the seed,

but the numbers generated by a good PRNG have properties of random sequences. The method is transparent in which an observer who has knowledge of the seed and the PRNG can control the output [LS12].

5.2 Risk-limiting audit algorithms

There are two types of election audits: process audits and results audits. Process audits determine whether appropriate procedures were followed, and results audits determine whether votes were counted accurately [For09]. Risk-limiting audits are one form of a results audit.

There are three types of risk-limiting audits [GCJ+12]:

1. **Ballot polling:** Know computer total for the election, count a random sample of ballots, report differences between computer and manual percentages
2. **Ballot level comparison:** Know how computers counted each ballot ("cast vote record"), compare the computer and manual interpretations of a random sample of ballots, count and report differences in these interpretations
3. **Batch comparison:** Know computer total for each batch of ballots (e.g. one precinct), hand-count all ballots in a random sample of batches, report any differences between computer and manual totals for each batch

Two algorithms are proposed and discussed in relation to the Norwegian electoral system: *ballot-polling audits* and *ballot level comparison audits*. These are "simple" calculations, meaning observers can easily check the auditor's work, an important requirement for an open and transparent election [LS12]. This master's thesis discusses a vote-for-one contest.

5.2.1 *Ballot-polling audits*

Ballot-polling audits examine a random sample of ballots (see random sampling above). The audit ends when the vote shares in the sample give sufficiently strong evidence that the reported winner really won. An advantage of *ballot-polling audit* is that the audit requires little information from the vote tabulation system: the reported winner must be known, however, the audit requires no additional data. Disadvantages such as that the audit generally requires examining more ballots than *comparison audits* (described below) and that the workload is disproportionately higher for contests with smaller margins, makes it a resource demanding audit [LS12].

In the following paragraph an example with risk limit of 10% is demonstrated. If the reported winner did in fact not win, there is at least a 90% chance it will require a

full hand tally. The audit applies to contests that require a super-majority, in this example it assumes that the winner's reported share s of valid votes is greater than 50% [LS12].

1. Let s be the winner's share according to the vote tabulation system (requires $s > 50\%$). Let t be a positive *tolerance* small enough that when t is subtracted from the winner's vote share s, the difference is still greater than 50%. Set $T = 1$.
2. Select a ballot at random, a ballot can be selected more than once.
3. If the ballot does not show a valid vote, return to step 2.
4. If the ballot shows a valid vote for the winner, multiply T by
$$(s - t)/50\%$$
5. If the ballot shows a valid vote for anyone else, multiply T by
$$(1 - (s - t))/50\%$$
6. If $T > 9.9$, the audit has provided strong evidence that the reported result is correct. The audit can stop.
7. If $T < 0.011$, perform a full hand count to determine who won. Otherwise return to step 2.

Numerically, a candidate reportedly received $s = 60\%$ of the votes. Set $t = 1\%$, so that if the reported winner received $s - t = 59\%$ of the votes, there is at most 1% chance the procedure will lead to a full hand count. Note that $1 - (s - t) = 1 - 59\% = 41\%$. Repeat steps 2-7 to perform the audit, until either $T > 9.9$ or $T < 0.011$. The number of selected ballots depends on the shares and the ballots selected. If the first 14 ballots drawn all show votes for the winner, the audit stops:

$$T = (59\%/50\%) \times (59\%/50\%) \times \cdots \times (59\%/50\%)$$
$$= (59\%/50\%)^{14} = 10.15$$

A ballot-polling audit may not be suited for the Norwegian electoral system. First, the expected workload grows quickly as the margin shrinks. The result in the Norwegian election is rarely an overwhelming majority, therefore the number of ballots to be audited is most likely to be quite high. An example to demonstrate the exponential growth, is if the winner's reported share in the example above is 60%, the audit

is expected to examine 120 ballots, a 55% share expects to examine 480 ballots, whereas for a 52% share, 3,860 ballots are expected to be audited.

Second, the ballot-polling applies to contests with super-majority, meaning that the winner's reported share is greater than 50%. Such a result is not likely to obtain in a Norwegian election.

Although impractical for the Norwegian election, ballot-polling audits are a realistic option for large contests as they do not require data from the vote tabulation system. According to Lindeman et al. (2012), *all* statewide contests could be confirmed with a single ballot-polling audit expected to analyse 3,860 ballots if the winner's smallest vote share was 52% [LS12].

5.2.2 *Ballot level comparison audits*

In ballot level comparison audits, each batch (see definition in Section 5.2) is one ballot. Imagine two phases [LS12]:

1. Check whether the reported subtotals for every cluster of ballots sum to the contest totals for every candidate. If not, the reported result is inconsistent and the cannot continue.

2. "Spot-check" the voting system subtotals against hand counts for randomly selected clusters, to assess whether the subtotals are sufficiently accurate to determine who won. If not, the audit has a high probability of requiring a full hand count.

Comparison audits generally involves fewer ballots than ballot-polling audits, but require more information from the vote tabulation system. The audit compares a manual interpretation of ballots selected at random to the system's interpretation. This assumes we know how the vote tabulation system interpreted every ballot. This is possible in EVA Skanning, as each ballot is stored as an image in the database. The audit continues until there is strong evidence of correct result or the audit requires a full hand count [LS12].

There are two alternatives if the manual interpretation disagrees with the system interpretation: "understatement" and "overstatement". If changing the system interpretation to the manual interpretation of the ballot *increases* the vote share for the winner, the ballot has an understatement. Understatements do not call the result into question, because correcting them benefits the winner. Overstatements, however, occurs when correcting the system interpretation to the manual interpretation *decreases* the margin between the winner and any loser [LS12]. The ballot then has

an "overstatement" equal to the maximum number of votes by which any margin would decrease:

- If the system interpretation of a ballot identifies an undervote but the manual interpretation finds a vote for one of the losers, the ballot has an overstatement of one vote.
- If the system interprets a vote for the winner, while the manual interpretation finds an overvote, the ballot has an overstatement of one vote.
- If the system interprets a ballot as a vote for the winner and the manual interpretation finds a vote for one of the losers, the ballot has an overstatement of two votes.

Similar to the ballot-polling audit example, an example of ballot-level comparison audit with risk limit of 10% is demonstrated. The example is based on the "super-simple" ballot-level risk-limiting comparison audit presented in Stark (2010) [Sta10]. The rule depends on the "diluted margin" m, the smallest reported margin in votes, divided by the number of ballots cast. Suppose the audit has inspected n ballots. Let u_1 and o_1 be the number of 1-vote understatements and overstatements, and similarly, let u_2 and o_2 be the number of 2-vote understatements and overstatements. The audit stops when

$$n \geq \frac{4.8 + 1.4(o_1 + 5o_2 - 0.6u_1 - 4.4u_2)}{m}. \tag{5.1}$$

This follows from equation [9] of [Sta10] with risk limit $\alpha = 10\%$ and $\gamma = 1.03905$ [LS12].

Numerically, we can suppose that a contest received 10,000 ballots. The reported winner, according to the vote tabulation system, received 4,000 votes, while the runner-up received 3,500 votes. The diluted margin is then $m = (4000 - 3500)/10000 = 5\%$. There are two options for sampling the ballots: 1) incrementally or 2) in stages.

1. *Sampling incrementally:* The auditor draws a ballot at random and checks manually if the system interpreter is correct or not. If there is one 1-vote understatement an no other misstatements among the first 80 ballots examined, $u_1 = 1$ and o_1, u_2, and o_2 are all zero and the audit may end, because

$$80 \geq \frac{4.8 - 1.4 \times 0.6 \times 1}{5\%}. \tag{5.2}$$

2. *Sampling in stages:* An auditor may draw many ballots at once to simplify logistics, then compare each ballot to the system interpretation. If a condition (described below) is not met, the auditor draws another set of ballots. Each set of draws and comparisons is one *stage*. The condition that must be met to end the audit, is that a 1-vote understatement offsets 60% of a 1-vote overstatement and a 2-vote understatement offsets 88% of a 2-vote overstatement [Sta10] [LS12]. We assume the auditor expects one 1-vote overstatement and one 1-vote understatement per thousand ballots (0.001 per ballot), and expects 2-vote misstatements to be negligibly rare. With diluted margin m of at least 5%, an initial sample of $4.8/m$ ballots is 96 ballots or fewer.

Although comparison audits require more information from the vote tabulation system and may seem more complex than ballot-polling audits, the audit may be suitable for the Norwegian electoral system. The first results based on the preliminary count and forecasts are published already 9 p.m. on the election day. In addition, the audit requires fewer ballots to be counted, even if the vote shares for the winner and runner-up are minimally different.

5.2.3 Degree of applicability in the Norwegian electoral system

To be able to determine which algorithm is appropriate to the Norwegian electoral system, and if any of them are in fact applicable, a quantitative experiment where a certain number of ballots would be scanned using a document scanner, and both algorithms were applied in turn to determine probability of correct result, would have been optimal. Unfortunately, such an experiment was not possible. An inquiry to lend a document scanner and ballot paper was denied by two municipals. Therefore, a qualitative analysis of the two algorithms is the foundation for the conclusion.

The advantages and disadvantages of the two algorithms are presented in Table 5.1. The disadvantages of ballot-level audit are quite significant. Due to the fact that the Norwegian electoral result is normally only separated by few percent, and is not a contest that requires super-majority, ballot-level audit is not applicable for the Norwegian election.

Based on the characteristics, comparison audits are more appropriate for the Norwegian electoral system. Comparison audits apply to contests with small margins as well. The disadvantage is that the audit requires more information form the vote tabulation system, however, is not relevant for the Norwegian electoral system. Each ballot is interpreted and stored in the database server along with associate metadata. Comparison audit requires information on how each ballot is interpreted, and the information may be located easily in the database.

Table 5.1: Comparison of ballot-level audit and comparison audit

	Advantages	**Disadvantages**
Ballot-level audit	Requires little information from the vote tabulation system	– the expected workload grows exponentially as the margin shrinks – applies to contests with super-majority
Comparison audit	Require fewer ballots, although few percent separates the candidates	Require more information from the vote tabulation system

5.3 Summarised findings and recommendations for the Norwegian electoral system

From the two previous chapters, indications of security vulnerabilities within EVA Skanning and non-reliable error detection mechanisms have been researched and concluded. The Norwegian electoral system is therefore in need of implementing a reliable error detection mechanism. Risk-limiting audits are considered best-practice and have therefore been analysed to determine degree of applicability in the Norwegian electoral system. Risk-limiting audits examine portions of the audit trail by hand until there is sufficiently strong evidence of correct result or until there has been a full hand count. Risk-limiting audits guarantee that if the vote tabulation system found the wrong winner, there is a high probability of a full hand count to correct the result. A requirement for such an audit is a voter-verifiable paper records, audit trail, and that the audit trail remains complete and accurate throughout the audit.

Risk-limiting audits require random sampling. The samples must be drawn properly, in a way that precludes manipulation, and in a way that the public can verify the outcome. A pseudo-random number generator with a seed generated by auditors satisfies these requirements. The mathematics may seem complex, but the examples provided are "simple" (can easily be performed with pen and paper or a calculator) which improves transparency.

Ballot-polling audits and comparison audits are two types of risk-limiting audits. For both methods, the sample size depends on the margin between winner and losers, and the ballots drawn in the audit. The size of the contest is rarely a factor.

Ballot-polling audit requires only the reported winner and the audit trail, whereas comparison audit requires detailed information from the vote tabulation system (the interpretation of each ballot). However, comparison audits examine fewer ballots than ballot-polling audits when the margin is small and the reported result is correct.

Of the two, comparison audits is analysed to be more appropriate for the Norwegian election. In ballot-polling audits, the expected workload grows quickly, exponentially, as the margin between the candidates shrinks, in addition to requiring super-majority. In a Norwegian election, the margin between the blocks is rarely large, and super-majority us rarely obtained. Although comparison audits require more information from the vote tabulation system, the system does record how each ballot is interpreted, and the audit may be performed post-election.

In conclusion, from a qualitative perspective, risk-limiting audits, in form of comparison audits, may be applied to the Norwegian electoral system. However, to determine degree of applicability, a quantitative experiment with ballots and the EVA Skanning installation is recommended.

Chapter 6
Conclusion

6.1 Introduction

An electoral system is the most important instance in a democratic society. When technology is incorporated into an electoral system, information security must be prioritised to ensure integrity of the result. Although one cannot guarantee a perfectly secure software system, there are measures that may be implemented to prevent mainstream attacks, such as man-in-the-middle and denial-of-service. Furthermore, reliable error detection mechanisms must be enforced to detect if any counting malpractice or result manipulation have occurred. If an attack were to occur, mechanisms to detect such an attack must be well-functioning and reliable.

This master's thesis has aimed to research the level of security within EVA Skanning, assess the reliability and performance of the currently implemented error detection mechanisms in the Norwegian electoral system, and analyse if, and how, risk-limiting audits should be applied as a reliable error detection mechanism.

This chapter summarises the results and corresponding discussions provided by the research. First, the findings from the security analysis of EVA Skanning are presented. Second, the reliability and performance of the implemented error detection mechanisms in the Norwegian electoral systems are accounted for. Third, the analysis of risk-limiting audit is discussed and summarised. Finally, recommendations for future work is presented.

6.2 Security within EVA Skanning

This master's thesis has aimed at researching the level of security within EVA Skanning. The methodology used is varied: in-depth interviews, dialogue with the Directorate of Elections, and a study of protocols and communication through an experimental setup of EVA Skanning.

The findings conclude that there is not sufficient information to determine the level of security within EVA Skanning. According to the Directorate of Elections, there does not exist complete system architecture or documentation for EVA Skanning used in 2017. This is due to lack of guidelines and routines requiring such documentation. The high-level system architecture illustrated in Chapter 3, is therefore not sufficient to determine the level of security within EVA Skanning. The illustration is based on publicly available information and interviews with the Directorate, but significant information related to database and firewall configurations have been omitted, due to security measures.

Similar to system documentation, the source code of the module used in 2017 is not publicly available either. The latest source code of EVA Skanning published, is the source code from the module used in 2013. The Directorate stated in an interview that source code of the module is to be published after the election, but has not yet published the source code for 2017. The Directorate later stated in an e-mail that they have not received an official request for the publication of the source code, and has therefore rather spent time on finalising the documentation for the 2019 module. Due to these limitations, studying system architecture and level of security has been challenging. There is not sufficient information to conclude degree of security within EVA Skanning.

Although, the information provided is not sufficient to determine level of security within EVA Skanning, the findings indicate that there are serious security vulnerabilities related to EVA Skanning:

1. **Developing complex software without documentation is a security vulnerability:** According to the Directorate of Elections, there does not exist system documentation for EVA Skanning used in 2017. This is due to lack of guidelines and routines requiring such information. It is difficult to comprehend how the Directorate can develop a complex software system without defining system requirements or architecture in writing. How can one verify that the system acts according to the specifications without documentation of expected behaviour? The lack of system documentation is considered security vulnerability.

2. **Development not entirely motivated by security:** *Boken om EVA Skanning* is considered to provide a thorough understanding of the EVA Skanning module used in 2015. Although the Directorate claims the document to be outdated, the research shows that the architecture remained similar in 2017. Therefore, the information provided is of relevance. The majority of the document is redacted due to security reasons. However, one chapter remains public

and provides arguments for the chosen architecture within the module. The document states that:

> *the choice of relational database is not selected because relational model and SQL servers are considered the best solutions for all imaginable purposes, but because of pragmatism and the desire to keep the system relatively simple - Boken om EVA Skanning.*

The Directorate later added in an e-mail that the choice of technology is not related to security. Such a statement is far from reassuring, as choice of technology is very much related to the level of security within an application. When the development of an electoral system software is not entirely motivated by security, but rather by simplicity, there are indications of security vulnerabilities within EVA Skanning.

3. **Possible technical vulnerabilities within EVA Skanning:** Based on the information provided, there has not been possible to determine level of security within EVA Skanning. Nevertheless, the results indicate several technical vulnerabilities:

   a) **Data traffic not encrypted:** There is no requirement that data traffic within the local area network must be encrypted. The municipalities themselves are responsible for ensuring the security of the EVA Skanning installation. The fact that encryption within the local area network is not a requirement, may indicate that anyone with access to the network can intercept the communication and obtain the information sent between the clients and database (man-in-the-middle attack). Furthermore, the attacker can alter the ballots, and thereby alter the final result. None of the interviewed election officials specified any local area network configurations, due to security reasons.

   b) **Username and password for database authentication may be stored in plaintext on the clients used in the 2017 module:** Username and password for authentication between the clients and the database are stored in the configuration file. The responses obtained during this study, indicate that these fields were stored in plaintext on the clients. Anyone with access to the configuration file or the local area network may therefore have obtained the username and password and could have connected to the database. The Directorate has later commented that in the 2019 version, the credentials will be stored encrypted by Data Protection API.

   c) **The database server is vulnerable in a small installation:** In a small installation, the client is installed with all EVA applications and the

database server. The client needs to communicate over the Internet from EVA Jobbstyring to EVA Admin, and the database server is therefore vulnerable for attacks from the Internet, in addition to attacks from the local area network.

d) **Scanning providers have access to provide support remotely:** The scanning providers (EVRY, Idox, and Indra) have in some municipalities remote access to EVA Skanning to perform support remotely.

Collectively, these bullet points indicate weak security within the EVA Skanning application, both in software and hardware. The fact that there is uncertainty of whether the municipals or the Directorate is responsible for securing the election infrastructure, contributes to further security vulnerabilities.

4. **Opaque electoral system:** Although the Directorate has been graciously answering questions throughout this study, there is not full openness or transparency of the electoral system.

   First, the majority of *Boken om EVA Skanning* is redacted due to security reasons (although the Directorate claims the information to be outdated). Second, a request to set up an experimental lab of EVA Skanning at the university was denied. The Directorate offered instead to demonstrate the software at their office. During this demonstration, specific security issues were not possible to study. Third, when asked to explain configuration details of the local area network and the database, the request was again denied. Due to these security measures, the Directorate could not provide this information.

   In information security theory, such information is assumed public knowledge. Kerckhoff's principle state that: *a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.* The fact that information related to network and firewall configurations are withheld from the public, may indicate that the system is not well enough secured.

   One of the problems with lack of openness and transparency is that the system is not available for anyone to verify correct implementation. In an interview, the managing director of the Directorate of Elections, Bjørn Berg, stated that the Directorate itself is responsible for developing the system and controlling that it behaves according to the specifications. When the developer is the same entity that is responsible for controlling the development, the public may have difficulties in trusting the system.

5. **Confusion related to who is responsible for infrastructure security:** Whilst interviewing representatives from the Ministry and the Directorate, the representatives emphasised that the responsibility of securing the election infrastructure lies with the municipals. The Directorate provides guidelines and recommendations, but the municipals themselves are responsible for securing

the installation. According to the election officials, the municipals follow the guidelines provided by the Directorate, and assume that the software provided is correct. Such a disclaimer on both ends leads to confusion to which entity is in fact responsible for that the result produced by EVA Skanning is correct.

Based on these findings, reliable error detection mechanisms are a requirement to determine if a compromise of the result has occurred. The following section discusses the reliability of the currently implemented error detection mechanisms in the Norwegian electoral system.

6.3 Reliability of implemented error detection mechanisms

An objective of this master's thesis was to assess the reliability and performance of the currently implemented error detection mechanisms in the Norwegian electoral system. Error detection mechanisms are necessary to ensure that compromise of the technology is not sufficient to compromise the result. A reliable error detection mechanism is defined as a mechanism that enforces software-independence. Software-independence may be enforced by producing an independent and comparable result, such as a full hand count or an independently developed software system that performs the same operations as the original system.

On the official website of the Directorate of Elections, *valg.no*, it is stated that: *In addition to securing the administrative IT system EVA, there are additional control mechanisms in the conduction of the election that ensures that compromise of the IT system itself is not sufficient to affect the result - the control mechanisms are not bound to if or which IT solutions are in use.* Which mechanisms and how they are implemented are not further described.

The methodology used to research the error detection performance in the Norwegian electoral system was to perform in-depth interviews with representatives from the Directorate and the Ministry and election officials from a representative selection of municipals, and study error detection in practice from the experimental setup of EVA Skanning. The results show that the reliability of the currently implemented error detection mechanisms is low:

1. **Comparison of preliminary and final counts:** The primary error detection mechanism is to compare the preliminary count and final count. Given a deviation, a recount shall be performed.

   Until the election in 2017, there were no regulations specifying how the counts should be performed: the municipals could choose to count manually and/or electronically. In 2017, the Ministry of Local Government and Modernisation

imposed the municipals to perform the preliminary count manually. This was to ensure a reliable comparable result to the result produced by EVA Skanning. Whether this measure will be implemented in future elections, is currently on hearing.

If both counts are performed electronically, the comparison of the two results is not a reliable error detection mechanism. Any error present in the preliminary count will most likely be present in the final count.

If the preliminary count is performed manually, as in 2017, this provides a reliable comparable result to the result produced by EVA Skanning. Given deviation, the recount should be performed manually. If the recount is performed electronically, the manual comparable result has no value. Currently, the recount is performed electronically, making the comparison of the preliminary and final count a not reliable error detection mechanism.

2. **Routines for random sampling of ballots:** A document provided by the Directorate, lists "routines for random sampling of ballots" as an error detection mechanism in the Norwegian electoral system. When asked to further explain the routine, the Directorate replied that this is a mechanism they wish to provide in future elections. They had not yet defined an appropriate algorithm, nor how to perform correct random sampling of ballots. Therefore, random sampling cannot be considered an implemented error detection mechanism.

3. **Compare final count to the urn count, the control count performed by the county council, and previous election results:** Error detection mechanisms mentioned by the election officials were to compare the final electronic result to the urn count, control count, and previous election results.

   Comparing the final result to the urn count is a reliable error detection mechanism if and only if the recount is performed manually. Normally, according to the election officials, the recount is performed electronically.

   The control count performed by the county council cannot be considered a reliable error detection mechanism because the control count is often performed with the same equipment as in the final count.

   Comparing the final count to previous election results will detect deviations out of proportion, but cannot be considered a reliable detection mechanisms for minor deviations.

4. **Error detection in practice through experimental setup of EVA Skanning:** The inquiry to set up a simulation of ballot counting using EVA Skanning at the university was denied by the Directorate, however, an invitation to test the system in Tønsberg was offered instead. The objective of the experiment was to research how errors are detected in practice. 15 ballots where scanned 3 times.

The results showed that a manual preliminary count provided a reliable comparable result when the machine counted incorrectly. The machine counted incorrect all three times (note that the software was under development). To verify that there were in fact 15 ballots in the scanner, a manual control count was performed.

According to the current regulations, a manual preliminary count is not yet specified, nor is a manual recount given deviation. Lack of such specifications contribute to low reliability of the error detection mechanisms.

5. **Consultation memorandum:** 1 November, a consultation memorandum was released by the Ministry. The memorandum suggests that the preliminary count of all votes (advance votes and Election day votes) must be counted manually. The Ministry argues that this will, to a greater extent than the current regulations, help ensure two independent counts and give legitimacy to the election result. This suggestion is a positive contribution to increase the reliability of error detection.

   Furthermore, the memorandum states that:

   > *In the event of a deviation between the preliminary and the final count, there shall be a recount. The recount cannot be performed by the same persons that performed the final count originally.*

   This phrasing is highly contradictory. First of all, similar to previous bullet points, this proposal undermines the legitimacy of the manual count. If the recount may be performed electronically, the result from the manual count has no value. Second of all, stating that the recount must be performed by different personnel, suggests that the fault lies with the people, not the machine. This insinuation is quite alarming.

Summarised these findings indicate that the reliability of error detection in the Norwegian electoral system is low. None of the error detection mechanisms enforce software-independence, therefore cannot be considered reliable. This thesis concludes with absence of reliable error detection mechanisms. Although the Ministry recommends to implement mandatory manual preliminary count, the measure holds no value as long as the electronic result is favoured. The measure may increase its value if risk-limiting audits were to be implemented. Risk-limiting audits are considered best-practice for error detection in electoral systems, and should be implemented to ensure integrity of the final result.

6.4 Risk-limiting audits as error detection mechanism in the Norwegian electoral system

The final objective of this master's thesis was to analyse if, and how, risk-limiting audits should be applied to the Norwegian electoral system.

Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of the audit trail, either paper ballots or voter-verifiable paper records, to verify correct result. Risk-limiting audits do not guarantee correct electoral result, but have a high probability of detecting if the result were to be wrong, and thereby enforce software-independence.

Based on the results from the two previous research questions, risk-limiting audits should be applied as a reliable error detection mechanism. There are technical vulnerabilities within EVA Skanning and, currently, there are no reliable error detection mechanisms implemented in the Norwegian electoral system. The electoral system needs to ensure integrity of the result, and risk-limiting audits may enforce an independent and comparable result. The methodology applied to research how risk-limiting audits may be implemented is a qualitative analysis of the concept. A quantitative experiment with EVA Skanning and ballots would have been preferable, but scanners nor the EVA Skanning software, were possible to obtain during the study.

Two risk-limiting audit algorithms are analysed qualitatively in the thesis: *ballot-polling audits* and *comparison audits*. The results in Chapter 5 show that *comparison audits* may be more appropriate for the Norwegian election. In *ballot-polling audit*, the expected workload grows quickly, exponentially, as the margin between the candidates shrinks, and is more suitable for contests with super-majority. In a Norwegian election, the margin between the blocks is rarely greater than a few percent. *Comparison audits*, on the other hand, requires fewer ballots to be checked even if the margin is low. The fact that comparison audits require more information from the vote tabulation system, is not considered problematic. The information on how each ballot is interpreted is available in the database server.

Although the term risk-limiting audit is not known by the Directorate, the concept seems to be known. The Directorate stated during the interview that in the election in 2019, routines for random sampling of ballots would be implemented to ensure integrity of the result. Which algorithm to be used had not yet been evaluated. Based on the findings from this study, comparison audit seems to be an appropriate algorithm for the Norwegian electoral system.

6.5 Future work

There has previously not been performed research on the technology used for the Norwegian electoral system, or more specifically, EVA Skanning. Therefore, there are several opportunities for future work:

1. **Penetration test EVA Skanning:** The request to simulate an election at the university, and penetration test EVA Skanning, was denied by the Directorate of Elections. Future master's thesis students should continue to request such access. More accurate results are likely to be found when penetration testing EVA Skanning.

2. **Simulate an election with risk-limiting audit algorithms:** In this research, a qualitative analysis of risk-limiting audits and their applicability to the Norwegian electoral system is performed. Future work may perform quantitative research in form of simulating an audit in practice with different algorithms.

3. **Test reliability of manual ballot counting vs EVA Skanning:** The question of whether manual ballot counting or electronic ballot counting provides the most reliable result is widely discussed. However, there exists no empirical evidence of error rate or consequence estimation on either one in Norway. Conducting an experiment with this objective is recommended as future work.

6.6 Conclusion

Unfortunately, there is not sufficient information to determine the level of security within EVA Skanning. However, the results indicate that there exist security vulnerabilities within the module. The software is developed without proper documentation, the development is not entirely motivated by security, and the system may be regarded as opaque. In the EVA Skanning configuration installed by the municipalities in 2017, encryption of the data traffic within the local area network was not a mandatory requirement. In addition, username and password for database authentication may have been stored in plaintext on the clients. Anyone with access to the local area network could therefore easily have intercepted the communication and altered the final result (man-in-the-middle attack). Collectively, these vulnerabilities gives an impression that security is not prioritised.

Furthermore, any technology-dependent electoral system requires reliable error detection mechanisms to identify potential counting malpractice and result manipulation. According to the results produced by this master's thesis, the currently implemented error detection mechanisms in the Norwegian electoral system are not reliable. A

reliable error detection mechanism must provide an independent and comparable result to determine if the produced outcome is correct. Given deviation, a manual recount should be performed. Currently, the municipalities may perform both the preliminary and final count electronically, using the same software and hardware for both counts. Given deviation, a recount is performed electronically. This approach yields no independent and comparable result, and cannot be considered reliable to detect result manipulation.

A reliable error detection mechanism may take many forms. One approach has been discussed in this master's thesis: risk-limiting audits. Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of the audit trail, either paper ballots or voter-verifiable paper records. Two algorithms have been analysed in the context of the Norwegian electoral system: *ballot-polling audits* and *comparison audits*. Based on the characteristics, comparison audit is considered to be the most appropriate algorithm for error detection in the Norwegian electoral system.

Finally, this master's thesis recommends at least one mandatory manual count of all ballots, as proposed in the consultation memorandum. Given deviation between the manual and electronic count, a manual recount should be performed. Furthermore, to ensure result integrity, risk-limiting audits are recommended implemented to provide statistical assurance of correct election outcome.

References

[BN06] Carolyn Boyce and Palena Neale. Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input. 2006.

[CC17] John W Creswell and J David Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017.

[CWD06] Arel Cordero, David Wagner, and David Dill. The role of dice in election audits—extended abstract. In *IAVoSS Workshop on Trustworthy Elections*, 2006.

[CYB17] HEARING ON CYBERSECURITY. University of pennsylvania us house of representatives committee on oversight and government reform subcommittee on information technology and subcommittee on intergovernmental affairs. 2017.

[Far12] Cyrus Farivar. Saving throw: securing democracy with stats, spreadsheets, and 10-sided dice, 2012.

[For09] Election Audits Task Force. Report on election auditing. 2009.

[Gar87] David Garvin. Competing on the eight dimensions of quality. *Harv. Bus. Rev.*, pages 101–109, 1987.

[GBG12] Stephen N Goggin, Michael D Byrne, and Juan E Gilbert. Post-election auditing: effects of procedure and ballot type on manual counting accuracy, efficiency, and auditor satisfaction and confidence. *Election Law Journal: Rules, Politics, and Policy*, 11(1):36–51, 2012.

[GCJ+12] Susannah Goodman, Common Cause, Roger Johnston, Mark Lindeman, Ronald L Rivest, Pam Smith, and Philip B Stark. Risk-limiting post-election audits: Why and how. 2012.

[Gun18] Martin Gundersen. Stortingsvalget 2017: Hver tredje stemme risikerte å aldri bli sjekket av et menneske. *NRK*, 2018.

[HCE17] Vilde Helljesen Helge Carlsen Hans Cosson-Eide, Peter Svaar. Krever manuell stemmetelling i alle kommuner. *NRK*, 2017.

[JO04] R Burke Johnson and Anthony J Onwuegbuzie. Mixed methods research: A research paradigm whose time has come. *Educational researcher*, 33(7):14–26, 2004.

[JOT07] R Burke Johnson, Anthony J Onwuegbuzie, and Lisa A Turner. Toward a definition of mixed methods research. *Journal of mixed methods research*, 1(2):112–133, 2007.

[LS12] Mark Lindeman and Philip B Stark. A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, 10(5):42–49, 2012.

[MAM90] Victor Minichiello, Rosalie Aroni, and Victor Minichiello. *In-depth interviewing: Researching people*. Longman Cheshire, 1990.

[MB17] Harri Hursti Joseph Lorenzo Hall Margaret MacAlpine Jeff Moss Matt Blaze, Jake Braun. Voting machine hacking village - report on cyber vulnerabilities in U.S. election equipment, databases, and infrastructure. *DEFCON*, 2017.

[Mic16] Microsoft. SQL Server 2016 Express LocalDB. 2016.

[oLGM17] Norwegian Ministry of Local Government and Modernisation. Election manuel - overview of election rules. 2017.

[Riv08] Ronald L Rivest. On the notion of 'software independence'in voting systems. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 366(1881):3759–3767, 2008.

[RM16] Colin Robson and Kieran McCartan. *Real world research*. John Wiley & Sons, 2016.

[SCFS14] Signe Bock Segaard, Dag Arne Christensen, Bjarte Folkestad, and Jo Saglie. Internettvalg: Hva gjør og mener velgerne. 2014.

[Sch09] B Schneier. Evil maid attacks on encrypted hard drives. *Crypto-Gram Newsletter*, 2009.

[Sha49] Claude E Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[SS12] Signe Bock Segaard and Jo Saglie. *Evaluering av forsøket med e-valg 2011: Tilgjengelighet for velgere, tillit, hemmelig valg og valgdeltagelse*. 2012.

[Sta10] Philip B Stark. Super-simple simultaneous single-ballot risk-limiting audits. In *EVT/WOTE*, 2010.

[Val15] Valgdirektoratet. Boken om EVA Skanning. 2015.

[Val17] Valgdirektoratet. Hva er elektronisk valgadministrasjonssystem – EVA? 2017.

[VT14] Edwin Van Teijlingen. Semi-structured interviews. *Retrieved from*, 2014.

[Yil13] Kaya Yilmaz. Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, 48(2):311–325, 2013.

[Zie02] Eric R Ziegel. Statistical inference, 2002.

[SC17a] Øyvind Bye Skille and Helge Carlsen. Sensitive valg-filer for tre kommuner var tilgjengelig for hele verden. *NRK*, 2017.

[SC17b] Henrik Lied Øyvind Bye Skille, Ola Mjaaland and Helge Carlsen. Teller opp stemmer i valget på datamaskiner tilkoblet internett. *NRK*, 2017.

Chapter A

Elektronisk valgadministrasjonssystem

Elektronisk valgadministrasjonssystem

EVA Admin

EVA Admin er den sentrale applikasjonen som behandler alle grunndata, og sammenstiller resultatene når stemmene er talt opp og overføres fra kommunene og fylkeskommune. Valgdirektoratet oppretter hvert enkelt valg i EVA basert på lovpålagte krav, før kommuner og fylkeskommuner legger inn informasjon om hvordan valgstyret ønsker å gjennomføre valget innenfor sitt ansvarsområde.

EVA Admin inneholder en oversikt og informasjon om manntallsførte velgere, og benyttes til å registrere stemmegivninger på velger. Stemmegivningene vurderes manuelt, men forkastes eller godkjennes i EVA, eventuelt mot et papirmanntall for de kommunene som registrerer stemmegivninger i et papirmanntall på valgdagen(e).

Når kommunene fordeler stemmene på parti og fortar opptelling av stemmesedlene, legges tall og rettelser gjort på stemmeseddelen inn i EVA før de blir godkjent og rapportert. Når alle stemmesedlene er talt opp i et valgdistrikt gjennomføres et valgoppgjør med mandatfordeling og kandidatkåring.

Underveis og avslutningsvis er ulike rapporter tilgjengelig i EVA Admin.

Bruksområder

Valggjennomføringen kan deles i fire faser, og EVA Admin gir systemstøtte i alle disse fasene.

Forberedelsesfasen

- Grunnlagsdata - målform, opptellingsadministrative forhold, forhånds- og valgtingsstemmesteder, samt valgkortinformasjon relatert til disse
- Listeforslag - administrasjon av listeforslag og stemmeseddelgrunnlag
- Manntall - som del av grunnlag for listeforslag

Stemmegivningsfasen

- Stemmegivninger i tidlig- og forhåndsstemmeperioden
- Administrasjon av forhåndsstemmer mottatt i annen kommune / krets / bydel
- Stemmegivninger for valgting
- Administrasjon av valgtingsstemmer mottatt i annen kommune / krets / bydel

Opptellingsfasen

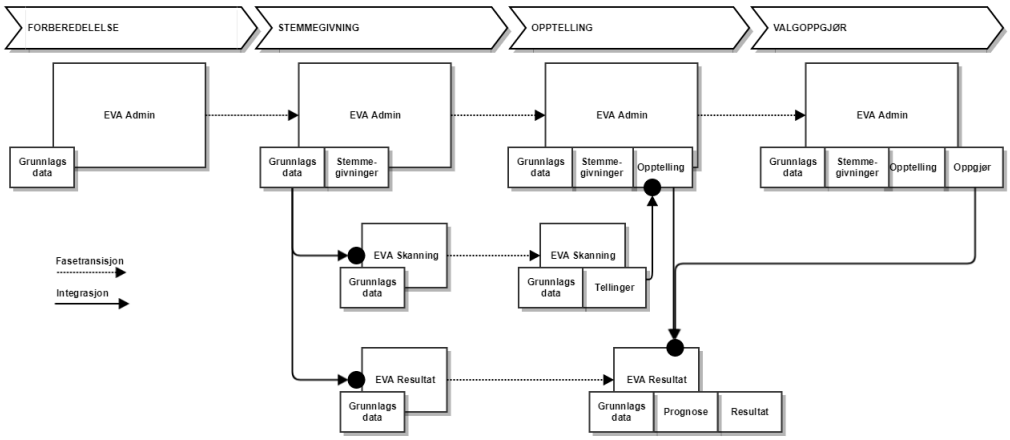
- Manuell opptelling av
    - Forhåndsstemmer
    - Valgtingsstemmer
    - Stemmer mottatt i annen kommune / krets / bydel
- Mottak av maskinelle telleresultater for
    - Forhåndsstemmer
    - Valgtingsstemmer
    - Stemmer mottatt i annen kommune / krets / bydel
- Protkollføring av valggjennomføring for aktuell valggjennomføringsinstans
    - Stemmestyrer

- Valgstyre
- Fylkesvalgstyre
- Bydelsutvalg

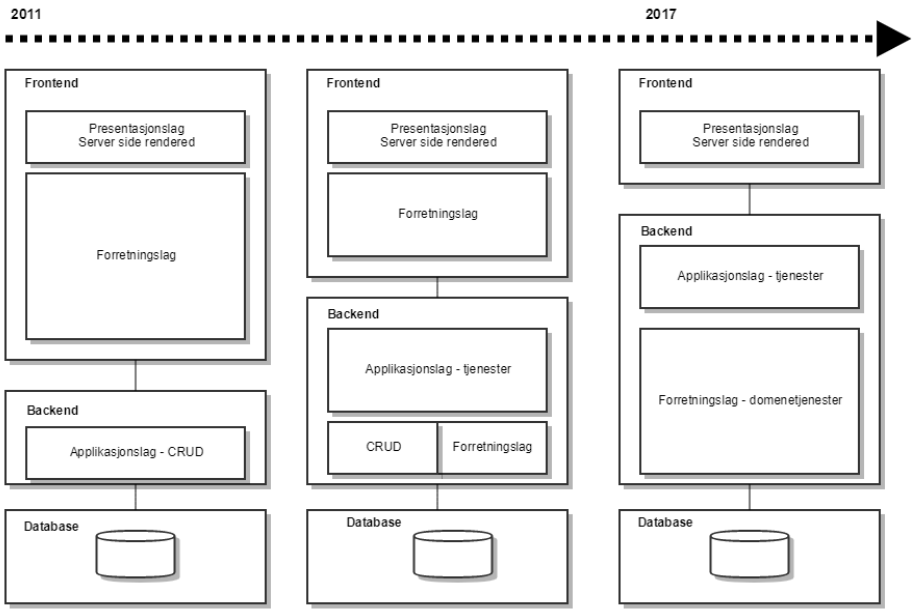
Valgoppgjørsfasen

- Endelig valgoppgjør
- Beregning av mandatfordeling
- Beregning av kandidatkåringer

I alle faser gir EVA tilgang til relevant rapportering til sluttbrukere og valgmyndigheter



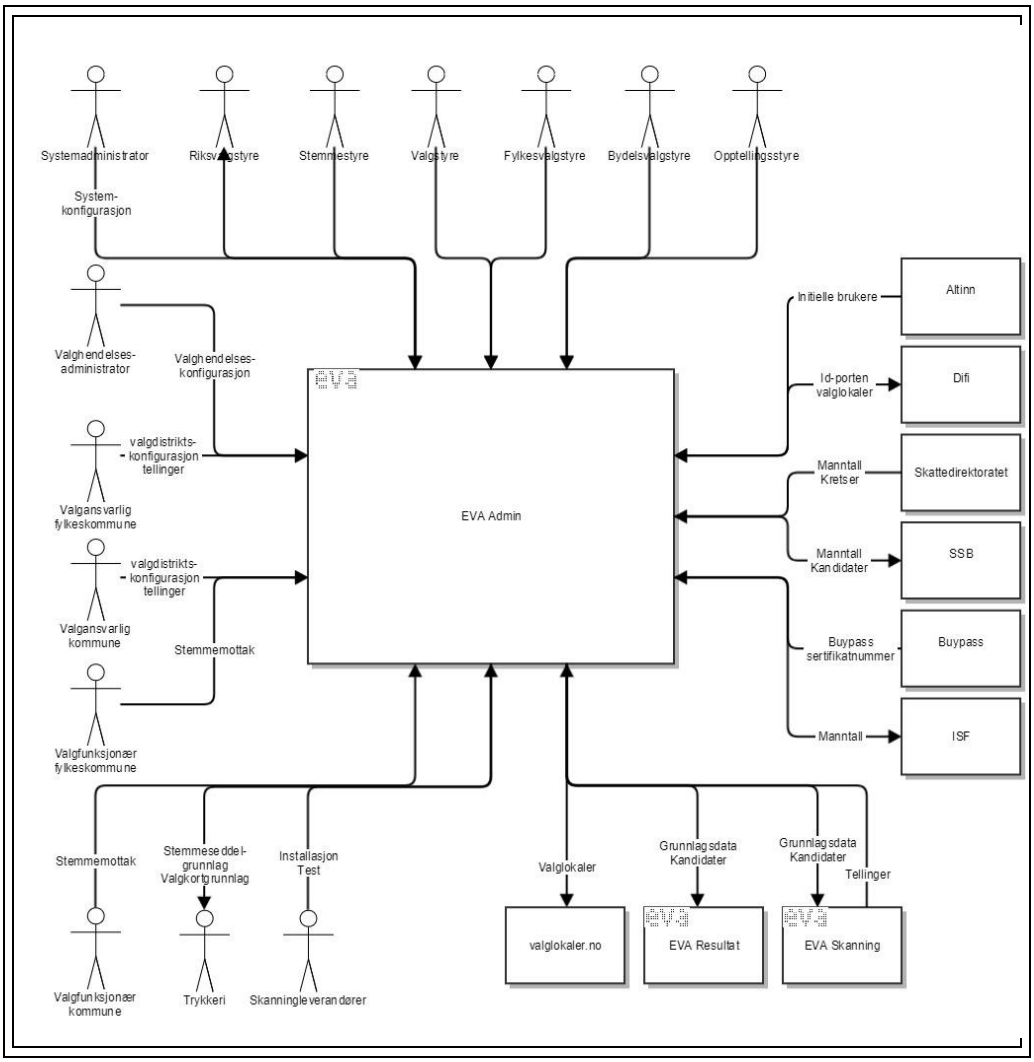
Diagrammet viser i hvilken fase av valggjennomføringen applikasjonen brukes



Diagrammet illustrerer lagdelingen i applikasjonen

Kontekstdiagram EVA Admin

Kontekstdiagrammet beskriver de aktører og systemer som bruker EVA Admin.



For å kunne kommunisere med EVA Admin må man først ha et klientsertifikat utstedt av Valgdirektoratet. Deretter må man identifisere seg ved å logge inn med ID-porten. Når man har logget inn er den enkelte bruker tildelt roller basert på hvilken tilgangsnivå de skal ha basert på de oppgavene de skal utføre i valggjennomføringen.
Forbindelsen til EVA Admin er kryptert.
Arkitekturen i EVA Admin er en splittet arkitektur med «frontend», «backend» og «database». Frontend er der valgmedarbeidere logger inn og benytter applikasjonen. Alle data som behandles gjøres i backend og alle data lagres i databasen. Det er kun frontend som kan kommunisere med

backend og det er kun backend som kan kommunisere med databasen. Arkitekturen har også utviklet seg over tid med tanke på risikobildet og best practice rundt utvikling av web applikasjoner.

EVA Skanning

EVA Skanning er applikasjonen som benyttes som systemstøtte for maskinell lesing og gjenkjenning av stemmesedler ved opptelling av stemmesedler i kommunene og fylkeskommunene.

EVA Skanning benyttes av de kommuner og fylkeskommuner som ønsker å lese stemmesedlene maskinelt, kombinert med å telle manuelt. Kommunene og fylkeskommunene kan selv vurdere om de finner det hensiktsmessig å benytte skanningløsningen. Vurderingene bygger på risiko, kostnader og effektivitet. Cirka halvparten av kommunene og alle fylkeskommunene benyttet EVA Skanning i forrige valggjennomføring (2017). Det er mindre kommuner som velger å ikke benytte skanningløsningen, da effektiviseringen ikke veier opp for kostnadene ved en installasjon. Disse kommunene benytter EVA Admin for en manuell registrering av opptellingene.

EVA Skanning installeres på lokale maskiner ute i kommune. Kommunene kan velge å benytte tredjepartsaktører til leie eller kjøp av utsyr og bistand til installasjon og support. Disse leverandørene er kvalifisert av Valgdirektoratet gjennom en egen rammeavtale.

Bruksområde

EVA Skanning brukes i opptellingsfasen av valgavviklingen til maskinell lesing og gjenkjenning av stemmesedler. Applikasjonen dekker tre hovedfunksjoner for dette området og er tilsvarende delt inn i tre moduler:

Jobbstyring

- Styring og oversikt over hvilke bunker / kasser som skannes på gitte tidspunkt
- Ferdigstilling av telling og overføring av telleresultater til EVA Admin

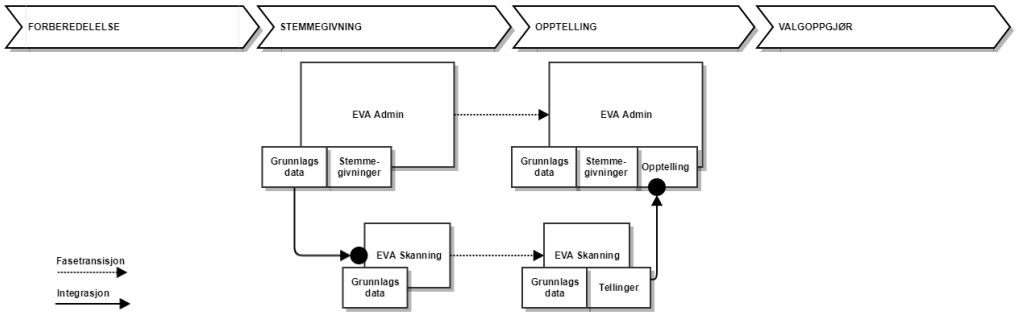
Skanning

Skanning og tolkning av stemmesedler for et gitt valg der:

- Parti identifiseres
- Endringer på stemmesedler identifiseres
- Stemmesedler akkumuleres opp i et telleresultat

Verifisering

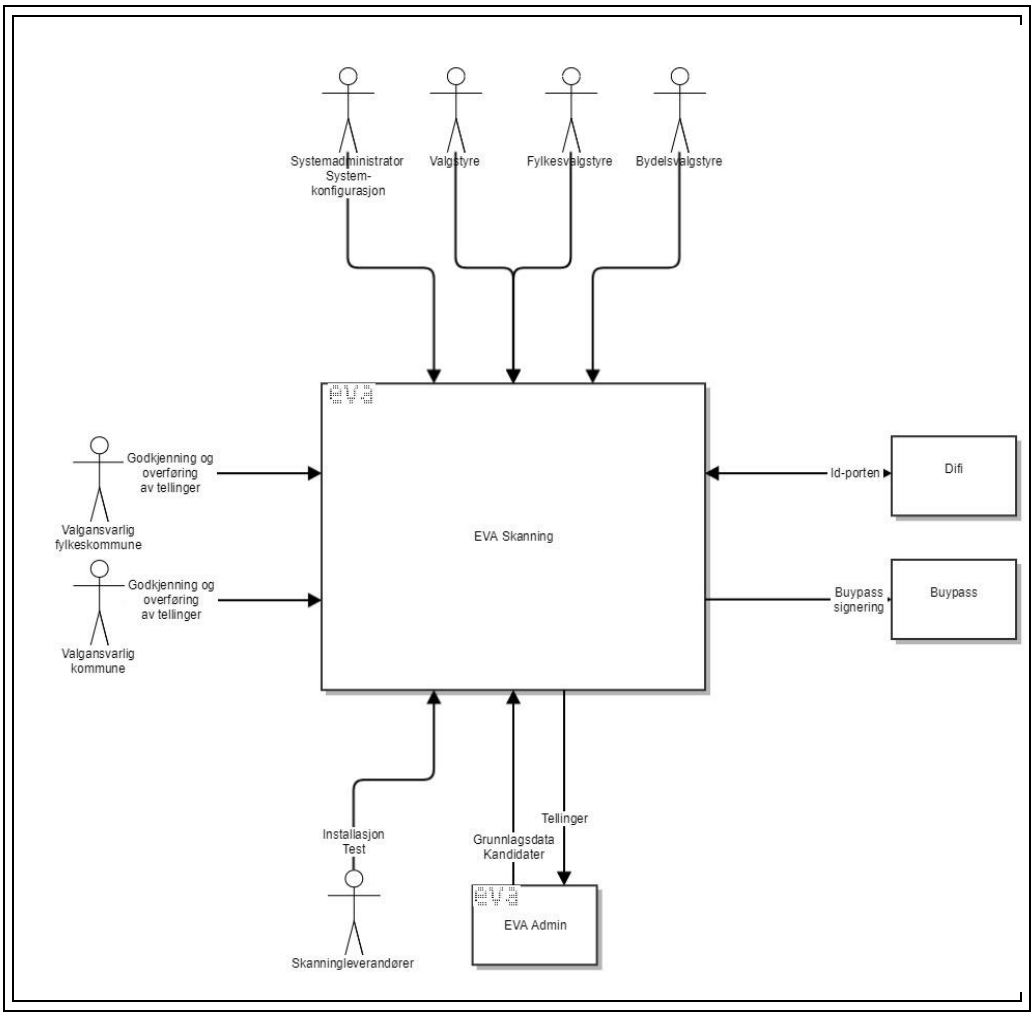
- Funksjonalitet for visuell verifikasjon og tolkning av stemmesedler som ikke er maskinelt lesbare, eller der resultatet av den maskinelle lesingen er usikkert



Diagrammet viser i hvilken fase av valggjennomføringen applikasjonen brukes

Kontekstdiagram EVA Skanning

Kontekstdiagrammet beskriver de aktører og systemer som bruker EVA Skanning



Datamaskinene som brukes for å skanne stemmesedler er sikret. Programvaren er utviklet av Valgdirektoratet, og krever et bestemt oppsett på maskinen som brukes. Maskinene har ikke tilgang til vanlig Internett, og skal ikke ha vært benyttet til andre formål tidligere.
Det stilles også krav til fysisk sikring av lokaler der EVA Skanning benyttes, og at kun autorisert personell har tilgang.
Det stilles også krav til hvordan applikasjonen skal installeres, og det følger en installasjonsveileder med programvaren. Installasjon i h.h.t. veileder innebærer at klienten blir låst, og valgmedarbeidere kan ikke bruke datamaskinen til andre formål.
For at eventuelle feil skal oppdages blir flere rutiner fulgt rundt stikkprøver, manuell verifisering av stemmesedler og rullering av tellestasjoner.
Datamaskinene og programvaren som benyttes til maskinell opptelling blir overvåket av Valgdirektoratet.

EVA Resultat

EVA Resultat er applikasjonen for beregning og eksponering av valgprognoser samt foreløpig og endelig valgresultat.

Når en opptelling er godkjent i EVA Admin, rapporterer kommunene og fylkeskommunene dette videre til EVA Resultat. I EVA Resultat ligger prognosemodellen som beregner valgprognoser basert på anerkjente beregningsmetoder som er utarbeidet i samarbeid med fagmiljøer på dette området. Medieaktører kan inngå avtale med Valgdirektoratet som gir tilgang til valgresultater og valgprognoser i tråd med gjeldende lover og regelverk.

Valgdirektoratet formidler også valgresultater og prognoser via nettstedet valgresultat.no. Her presenteres resultatene i tall på en nøytral måte. Tallene hentes direkte fra EVA Resultat, og er de samme tallene som medieaktørene får tilgang til. Valgdirektoratet publiserer sin prognose klokken 21.00 på valgdagen i h.h.t. sperrefrist som også gjelder for medieaktørene.

Kommunene og fylkeskommunene benytter kun EVA Admin og EVA Skanning. EVA Resultat er en intern applikasjon i Valgdirektoratet som mottar valgresultater fra EVA Admin og formidler valgresultater og prognoser.

Bruksområde

EVA Resultat er applikasjonen for beregning og eksponering av valgprognoser samt foreløpig og endelig valgresultat:

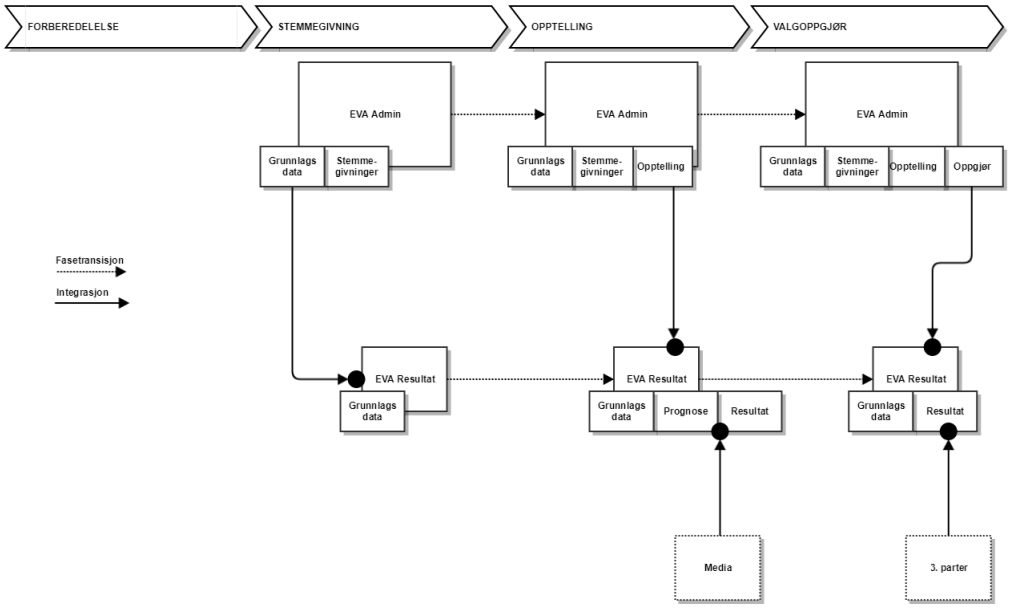
Opptellingsfasen

- Prognose beregnes etter at valglokalene stenger og frem til ca 01:00 - 02:00 påfølgende natt, når faktisk opptalte resultater erstatter prognosen
- Prognosen baserer seg på forhåndsstemmer og innkommende resultater underveis i opptellingen
- Prognosen gir antatt partifordeling og mandatberegning
- Når grunnlaget er komplett presenteres det faktiske valgresultatet og den antatte mandatfordelingen

Valgoppgjørsfasen

- Når valgoppgjør er gjennomført og endelig valgresultat foreligger med mandatkåringer presenteres det endelige valgresultatet med mandatfordeling

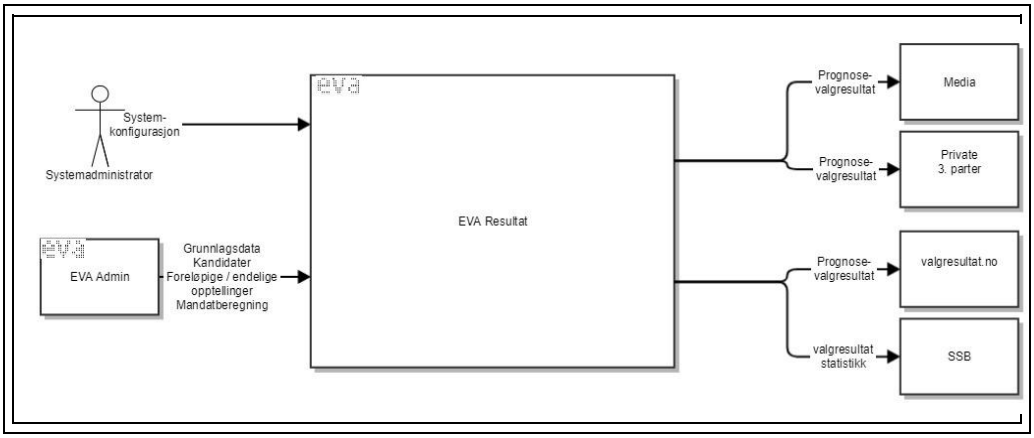
EVA Resultat eksponerer historiske valgresultater og statistikk og er eneste applikasjonen i EVA porteføljen som også er aktivt utover valggjennomføringen.



Diagrammet viser i hvilken fase av valggjennomføringen applikasjonen brukes

Kontekstdiagram - EVA Resultat

Kontekstdiagrammet beskriver de aktører og systemer som bruker EVA Resultat



EVA Resultat har også en delt arkitektur i likhet med Admin. Backend produserer prognoser og resultater og publiserer disse til frontend. Frontend kan ikke kommunisere tilbake med backend.

De som har tilgang til API for uthenting av valgdata (JSON APIet) i EVA Resultat er forhåndsgodkjent av Valgdirektoratet, og må benytte en API nøkkel for å identifisere seg ved pålogging.

Andre som ønsker tilgang til valgresultatet har tilgang til dette på nettsidene i valgresultat.no. Dataoverføringen gjøres over en kryptert forbindelse for å sikre at resultatet er korrekt.

Chapter B

Høringsnotat - Forslag til endringer i valgforskriften og forskrift om direkte valg til kommunedelsutvalg

Høringsnotat – Forslag til endringer i valgforskriften og forskrift om direkte valg til kommunedelsutvalg

Innhold

1. Bakgrunn

I dette høringsnotatet foreslås endringer i forskrift 2. januar 2003 nr. 5 om valg til Stortinget, fylkesting og kommunestyrer (valgforskriften). Forskriften er gitt med hjemmel i lov av 28. juni 2002 nr. 57 om valg til Stortinget, fylkesting og kommunestyrer.

Endringene er delvis en oppfølging av endringene i valgloven som ble vedtatt i Stortinget den 15. juni 2018 i tråd med forslaget som ble fremmet i Prop. 76 L (2017–2018). Dette gjelder forslaget om å oppheve valgforskriften § 16 og forslaget til endringer i § 25a.

Den 31. august 2017 fastsatte departementet en forskrift med krav om at den foreløpige opptellingen av alle stemmesedler ved valget i 2017 skulle skje manuelt. Forskriften opphørte 31. desember 2017. Departementet foreslår nå å fastsette i valgforskriften at den foreløpige opptellingen av både forhåndsstemmer og valgtingsstemmer skal foregå manuelt. I tillegg foreslår departementet å forskriftsfeste en rutine ved avvik mellom foreløpig opptelling og endelig opptelling, dersom endelig opptelling er foretatt maskinelt ved skanning.

I 2019 skal det gjennomføres kommunestyre- og fylkestingsvalg. Det foreslås enkelte endringer i bestemmelsen om utformingen av stemmesedlene til kommunestyrevalg og fylkestingsvalg, blant annet som følge av at det i forbindelse med kommunesammenslåinger er kommuner og fylkeskommuner som skal velge flere representanter til kommunestyret og fylkestinget enn det er plass til på dagens stemmesedler. Departementet foreslår også en endring i plasseringen av stempelfeltet på stemmesedlene til kommunestyre- og fylkestingsvalg, lik den som ble gjort for stemmeseddelen til stortingsvalg i 2017.

Som følge av at A- og B-post er slått sammen til én felles brevstrøm fra 1. januar 2018, foreslår departementet også en endring i bestemmelsen om forsendelse av forhåndsstemmer.

Departementet foreslår i tillegg en mindre endring i forskrift 3. januar 2003 nr. 8 om direkte valg til kommunedelsutvalg, slik at det framgår eksplisitt at også valgforskriftens bestemmelser om kommunestyrevalg gjelder tilsvarende så langt de passer.

Departementet vil komme tilbake med forslag til nødvendige endringer i forskrift 19. desember 2008 nr. 1480 om valg til Sametinget i forkant av sametingsvalget i 2021.

2. Manuell foreløpig opptelling av stemmesedler

2.1 Bakgrunn

Kommunal- og moderniseringsdepartementet (KMD) har det overordnede nasjonale ansvaret for gjennomføring av valg til Stortinget, fylkesting og kommunestyrer. Kommunene har ansvaret for den praktiske valgavviklingen, herunder opptellingen av stemmesedlene. Alle kommuner og fylkeskommuner har siden 2013 benyttet det elektroniske valgadministrasjonssystemet EVA i valggjennomføringen. Om lag halvparten av kommunene og alle fylkeskommunene har valgt å benytte seg av skanningmodulen i EVA til maskinell opptelling av stemmesedler.

I forkant av valget i 2017 var det økende aktivitet og oppmerksomhet om de tekniske løsningene. For å skjerpe sikkerheten i valggjennomføringen ytterligere fastsatte departementet med hjemmel i valgloven forskrift om opptelling av stemmesedler ved valg til Storting og kommunestyre i 2017. Det framgikk av forskriften § 2 at den foreløpige opptellingen etter valgloven § 10-4 femte ledd og § 10-5 skulle skje ved manuell telling. Bakgrunnen var stor oppmerksomhet i mediene og offentligheten for øvrig om sikkerheten i skanningløsningen og mulige svakheter i løsningen. Departementet la til grunn at et krav om at den foreløpige opptellingen skulle skje manuelt, ville sørge for at velgernes tillit til valggjennomføringen ikke ble svekket.

2.2 Gjeldende rett

I valgloven § 10-4 er det lovfestet prinsipper for opptelling av stemmesedler. Valgloven § 10-4 første ledd fastsetter at valgstyret er ansvarlig for opptellingen og at opptellingen foretas av de personer og på den måten valgstyret har bestemt. Valgloven § 10-4 femte ledd fastsetter prinsippet om at stemmesedlene skal telles opp i to omganger, ved en foreløpig og en endelig opptelling. Det gjelder både stemmesedler avgitt på forhånd og stemmesedler avgitt på valgting. Valgloven §§ 10-5 og 10-6 gir nærmere regler for henholdsvis den foreløpige og den endelige opptellingen. Alle stemmesedler det er tvil om kan godkjennes, skal legges til side og holdes utenfor den foreløpige opptellingen. Endelig opptelling må skje under valgstyrets tilsyn. Valgstyret avgjør om stemmesedlene som ble lagt til side ved den foreløpige opptellingen skal godkjennes. Stemmesedlene som blir godkjent, telles sammen med de øvrige stemmesedlene i den endelige opptellingen. Ved den endelige opptellingen blir også rettinger velgerne har gjort på stemmesedlene registrert.

Forskriften med krav om manuell foreløpig opptelling gjaldt kun ved valget i 2017 og opphørte 31. desember 2017. Valgloven og valgforskriften er ikke til hinder for at både den foreløpige og endelige opptellingen foregår maskinelt ved skanning. Kommunene kan dermed etter dagens regelverk selv velge å gjennomføre begge opptellingene manuelt, begge opptellingene maskinelt eller kombinere manuell opptelling og maskinell opptelling.

Valgloven har regler om føring av protokoller (møtebøker) ved valg for å sikre valgets notoritet, mulighet for kontroll og godkjenning. I henhold til valgloven § 10-7 skal stemmestyret, valgstyret og fylkesvalgstyret føre protokoll i forbindelse med gjennomføringen av valget. Av valgforskriften § 41 følger det at departementet fastsetter formularer om blant annet opptelling som valgmyndighetene er forpliktet til å benytte ved protokollering. Departementet har delegert myndigheten til å fastsette formularer til Valgdirektoratet. Det er imidlertid ikke lovfestet eller forskriftsfestet rutiner ved avvik mellom endelig og foreløpig opptelling.

2.3 Departementets vurdering

2.3.1 Forskriftsfeste krav om foreløpig manuell opptelling

Det er viktig å unngå usikkerhet rundt gjennomføringen av sentrale valgoppgaver som opptelling av stemmesedler. Departementet foreslår derfor å forskriftsfeste en bestemmelse i valgforskriften om at den foreløpige opptellingen etter valgloven §§ 10-4 femte ledd og 10-5

skal skje ved manuell telling. Med manuell opptelling menes at opptellingen skjer for hånd uten bruk av maskiner. At departementet foreslår at det er den foreløpige opptellingen som skal skje manuelt, og ikke den endelige, skyldes praktiske hensyn, da den foreløpige opptellingen av valgtingsstemmer kan foregå på stemmestedene. Endelig opptelling må skje under valgstyrets tilsyn og foregår derfor ikke på stemmestedene.

At valget gjennomføres på en korrekt og tillitvekkende måte er avgjørende for demokratiet. Å forskriftsfeste et krav om at den foreløpige opptellingen skal skje ved manuell telling vil i større grad enn med dagens regelverk bidra til å sikre to uavhengige opptellinger og gi legitimitet til valgresultatet.

Evalueringer av stortingsvalget i 2017 viser at kommunene gjennomførte den foreløpige manuelle opptellingen på en tilfredsstillende måte uten større utfordringer, selv om endringen ble fastsatt kort tid for valgdagen. Den manuelle opptellingen førte ikke til forsinkelser i opptellingsresultatene. Krav til manuell foreløpig opptelling er etter departementets vurdering gjennomførbart for alle kommuner og et krav som er forståelig for velgerne.

Departementet foreslår samtidig å forskriftsfeste en rutine ved avvik mellom foreløpig opptelling og endelig opptelling, dersom endelig opptelling er foretatt maskinelt ved skanning. Forslaget innebærer at det skal telles på nytt ved avvik mellom foreløpig opptelling og endelig opptelling. Ny maskinell opptelling skal ikke foretas av de samme personene som foretok den endelige opptellingen opprinnelig. Departementet vurderer det ikke som nødvendig å forskriftsfeste en rutine for avvik dersom begge tellinger skjer manuelt.

Forskrift om direkte valg til kommunedelsutvalg § 8 fastslår at valglovens bestemmelser om kommunestyrevalg gjelder tilsvarende så langt de passer. Det er ikke presisert nærmere hvilke bestemmelser dette er. Reglene i valgloven kapittel 10 foruten §§ 10-8 og 10-9 gjelder ved kommunestyrevalg, og vil dermed gjelde "så langt de passer" ved direkte valg til kommunedelsutvalg. Valglovens bestemmelser om opptelling i §§ 10-4 og 10-5 må ses i sammenheng med de regler om opptelling som er fastsatt i valgforskriften. Forslaget om at den foreløpige opptellingen etter §§ 10-4 og 10-5 skal skje ved manuell telling vil dermed også gjelde opptelling av stemmesedler for direkte valg til kommunedelsutvalg. Departementet foreslår å tydeliggjøre bestemmelsen i forskrift om direkte valg til kommunedelsutvalg § 8, slik at det framkommer direkte at også valgforskriftens bestemmelser om kommunestyrevalg gjelder tilsvarende så langt de passer.

2.3.2 Vurdering av forskriftshjemmel

Valgloven § 10-10 inneholder en forskriftshjemmel. Ordlyden i bestemmelsen er generell, og fastslår at departementet kan gi forskrift om blant annet «opptelling av stemmesedler». Det framgår av Ot.prp. nr. 45 (2001–2002) på s. 215 at detaljer om fremgangsmåten ved opptellingen kan reguleres i forskrift. Forarbeidene trekker utover dette ikke opp noen konkrete begrensninger for hva slags regler for opptellingen som kan fastsettes i forskrift.

Med dette som bakgrunn vurderer departementet at forskriftshjemmelen i valgloven § 10-10 gir hjemmel til å gi bestemmelser i forskriften om at den foreløpige opptellingen skal skje manuelt, samt bestemmelser om rutiner for håndteringen av avvik mellom manuell og

maskinell opptelling. Bestemmelsene anses som detaljregler av praktisk betydning for en reell opptelling i to omganger, og anses ellers i tråd med de prinsipper og rutiner ved opptelling som følger av valgloven.

2.3.3 Anbefalte sikkerhetstiltak ved bruk av EVA Skanning

Sikkerhet i valggjennomføringen er en viktig forutsetning for at befolkningen skal ha tillit til forvaltningen og politiske institusjoner. Valgdirektoratet arbeider med å ivareta og styrke sikkerheten i EVA Skanning fram mot kommunestyre- og fylkestingsvalget i 2019. Direktoratet vil gi kommuner og fylkeskommuner skriftlige veiledninger om hvilke fysiske og tekniske sikkerhetstiltak som bør iverksettes ved bruk av EVA Skanning. Departementet anbefaler kommunene og fylkeskommunene å følge de anbefalte tiltakene.

3. Stemmeseddelens utforming

3.1 Bakgrunn

Valgforskriften § 19c omhandler krav til stemmesedlenes utforming ved kommunestyre- og fylkestingsvalg. Bestemmelsen fastsetter blant annet krav til farge og størrelse på stemmesedlene og til veiledningstekst og stempelfelt på stemmesedlene.

I forbindelse med sammenslåingen av kommuner og fylkeskommuner, er det flere kommuner og fylkeskommuner som skal velge flere representanter til kommunestyret og fylkestinget enn stemmesedlene i valgforskriften legger opp til. Det er derfor nødvendig med enkelte endringer i utformingen av stemmesedlene til kommunestyrevalg og fylkestingsvalg.

3.2 Krav til stemmesedler med kandidatnavn

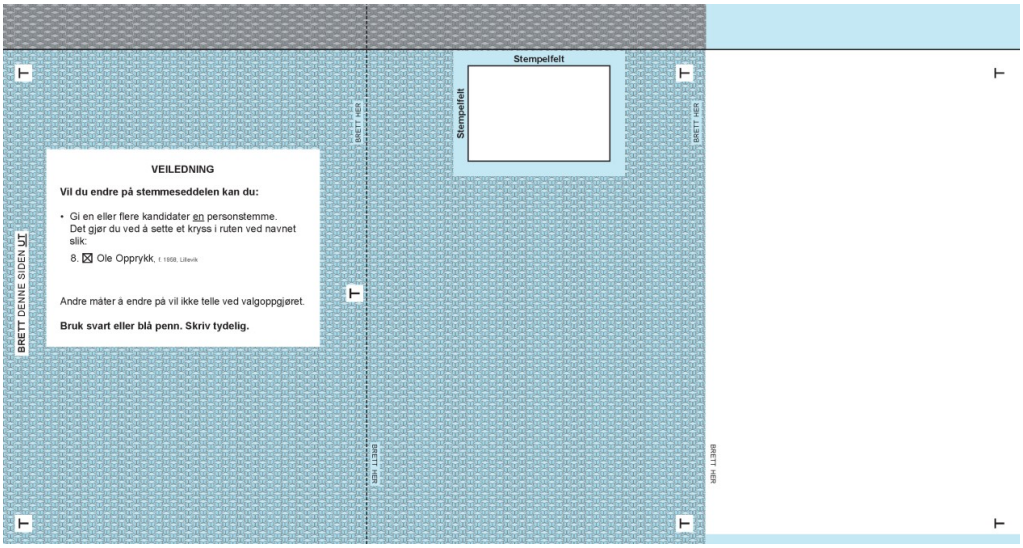
Det foreslås at kommuner som skal velge mer enn 43 og inntil 67 representanter til kommunestyret skal benytte stemmeseddel med to falser. For kommuner som skal velge mer enn 67 representanter til kommunestyret foreslås det at feltet der velgeren kan skrive navnet på kandidater fra andre lister (såkalte slengere) trykkes på utsiden av stemmeseddelen. Det er markert på stemmeseddelen at siden med veiledningsteksten skal brettes ut. Siden med feltet der velgeren kan skrive navnet på kandidater fra andre lister skal brettes inn. Det vil dermed ikke være mulig for andre i valglokalet å få kjennskap til om velgeren har ført opp kandidater fra andre lister på stemmeseddelen og hvem disse eventuelt er når stemmeseddelen er sammenbrettet. Velgeren skal foreta sammenbrettingen i "enerom og usett" jf. valgloven § 9-5 tredje ledd. Dersom velgeren bretter stemmeseddelen feil, skal en valgfunksjonær veilede velgeren i hvordan denne brettes riktig, og be velgeren gå tilbake til avlukket.

Det foreslås videre at fylkeskommuner som skal velge mer enn 57 representanter til fylkestinget skal benytte stemmeseddel med to falser.

3.3 Stempelfelt

Departementet viser til endringene i valgforskriften som ble vedtatt 27. februar 2017, der stempelfeltet på stemmesedlene for stortingsvalg ble forminsket og flyttet opp. Bakgrunnen for endringen var evalueringen etter valget i 2015, der departementet fikk tilbakemeldinger

Utside (mønsterside)



§ 25a andre punktum skal lyde:
Kandidat som er oppført på valgliste ved stortingsvalget eller fylkestingsvalget, kan ikke oppnevnes til valgfunksjonær i valglokalene ved forhåndsstemmegivningen i kommunene i vedkommende *valgdistrikt*.

§ 27 niende ledd oppheves.

Ny § 37a skal lyde:
§ 37a *Foreløpig opptelling av stemmesedler*
(1) Den foreløpige opptellingen av stemmesedler etter valgloven § 10-4 femte ledd og § 10-5 skal skje ved manuell telling.
(2) Ved avvik mellom en foreløpig og en endelig opptelling som er foretatt maskinelt, skal opptelling foretas på nytt. Ny maskinell opptelling kan ikke foretas av de samme personer som foretok endelig opptelling første gang.

I forskrift 3. januar 2003 nr. 8 om direkte valg til kommunedelsutvalg gjøres følgende endringer:

§ 8 skal lyde:
§ 8 Forholdet til valgloven *og valgforskriften*
Valglovens *og valgforskriftens* bestemmelser om kommunestyrevalg gjelder tilsvarende så langt de passer.

Chapter C

Interview guide - The Ministry of Municipal and Modernisation and the Directorate of Elections

Intervjuguide: KMD og Valgdirektoratet

a) Systemdokumentasjon

1) Jeg har fått skummet litt gjennom den dokumentasjonen dere sendte i går, men jeg savner fortsatt litt informasjon.
    - Når det står beskrevet at de ulike delene snakker med hverandre, er det illustrert med en pil. Jeg lurer litt på hvordan den kommunikasjonen tar form?
        - Hvem kommuniserer med hverandre og den sentrale serveren.
        - Dersom det er en stor installasjon – hvordan kommuniserer EVA Jobbstyring med EVA Admin? Hvordan rapporterer EVA Admin til EVA Resultat?

2) Hvordan kommuniserer PCene i valglokalene med den sentrale serveren? Er de koblet til Internett? Det står i det dokumentet at maskinene ikke er koblet til «vanlig» internett. Hva vil det si? Hvordan blir resultatet sendt videre?
    - Samme når man må laste ned valgkonfigurasjonen fra distribusjonssiden. Da må man vel ha internettilgang?
    - Liten installasjon – da er alt på en PC. Denne må vel da også ha tilgang til internett?
        - Ser dere noen større risikoer ved at stor eller liten installasjon?
    - Er det en sentral server og en sentral database? Hvordan er den sentrale databasen konstruert?
3) Hvilke elektroniske elementer består systemet av?
    - Elektronisk manntall – hvordan fungerer det?
    - EVA Admin, EVA Skanning og EVA Resultat – servere og databaser, det savner jeg litt i det dokumentet dere sendte.
    - PCer, servere, databaser, skanner
4) Skannere – hvordan skannes stemmeseddelen? Blir den lagret? Eller telles den bare?
    - Lagres det et bilde av seddelen når den skannes? Eller telles den bare?
    - Bildet sendes til databasen – telles det i skanneren eller databasen. Man in the middle attack.
    - Autorisering mellom PCen og SQL databasen – hvordan autoriserer de seg?

5) Da jeg snakket med valgansvarlige i kommuner, var de litt usikre på hva som faktisk lagres. Noen mener ingenting lokalt, mens andre mener de har en database som lagrer stemmesedlene. Hva vet dere?

6) Det står i det dokumentet dere sendte i går: at dataoverføring gjøres over en kryptert forbindelse. Kan dere si noe om hvilken kryptering som er brukt? Hvilke portokoller? Hvordan tas avgjørelser som dette?

7) Autentisering: foregår det med BuyPass og Min ID?
    - ID porten logg inn, signering av tellingen med buypass

8) Hvilke endringer gjør dere før valget 2019?

b) Administrasjon

9) Kan dere si litt om samspillet mellom Valgdirektoratet og KMD? Valgdir har ansvar for den operative gjennomføringen? Og med kommunene
10) Hvordan er samspillet med skanningsleverendørene?
    - Evry, Idox og Indra – hvordan er anbudsprosess. Risiko at det er utenlandske leverendør?
    - Hvilken rolle har de, hva har de ansvar for?
    - Hvor godt kjennskap har de til EVA Skanning og EVA generelt?
    - Hvilke krav stilles til skanningslevereandørene

11) Hvem har utviklet EVA slik det brukes i dag?
12) Hvem er Boken om EVA Skanning tiltenkt? Kommunene eller offentligheten? Er det et internt dokument? (Sluppet fra Valgdirektoratet etter Mimes Brønn requesten). Hvis det er ute av produksjon kan jeg få se på?)
13) Hvorfor er store deler av Boken om EVA Skanning sensurert?

14) Hvilke risikoer har systemet? Hvilke tiltak gjøres for å minke risikoene? Er det mulig å få tilgang til risikoanalysen som er nevnt i dette dokumentet: https://valg.no/globalassets/dokumenter/styrende-dokumenter/tildelingsbrev-valgdirektoratet-2018.pdf

c) Feilhåndtering

15) Frem til i fjor var det opp til kommunen hvordan de ønsket å telle, manuelt eller maskinelt. Hvordan oppdages feil dersom begge tellingene utføres maskinelt?
16) Hvem har ansvar for å oppdage feil? Kommunene eller Valgdirektoratet? Hvordan skal det gjøres?
17) Er det mulig å garantere programavareuavhengighet? En uoppdaget feil i programvaren skal ikke kunne føre til uoppdagede feil i resultatet – risk limiting audits
18) Noe som kom frem da jeg intervjuet valgansvarlige var at, mange valgmedarbeidere sier de stoler mer på maskiner enn på mennesker (menneskelige feil). De fleste feil som oppdages skjer på grunn av feil i manuell telling. Hvordan stiller dere dere til det?

19) Har dere vurdert å bruke risk-limiting audits i stedet for full manuell telling?

20) Det står i det dokumentet dere sendte i går, at det gjennomføres stikkprøver, det er i hvertfall rutiner på det. Det stemmer ikke helt overens med de kommunene jeg har snakket med. Er dette nye rutiner?

    - Måten de oppdager feil på er å sjekke om resultatet er noen lunde likt forrige valg, hvis ikke sjekk. De gjør tester i forkant av valget, men ikke på valgdagen.
    - Mener at Valgdir har ansvar for programvaresikkerheten.

21) Hvilke statistiske metoder bruker dere for stikkprøver?

d) Eksperiment

22) Så hyggelig at jeg ble invitert til Tønsberg, det ønsker jeg svært gjerne.
23) Jeg ønsker å sette opp en testlab med systemet EVA for å simulere et valg for å øke min forståelse av systemet og hvordan kommunikasjonen foregår. Dette var også noe jeg fikk anbefalt av enkelte valgansvarlige, at jeg burde være med på et valg. I og med at det ikke er valgår, lurer jeg på om jeg kan få tillatelse til å prøve ut systemet selv? Kan jeg få tilgang til å laste ned EVA programvare fra distribusjonssiden?
    - Forsøket vil foregå i kontrollerte omgivelser på NTNU Trondheim, eventuelt et rådhus dersom det er ønskelig.
    - Ting som når stemmene fordeles på parti, når endrede stemmesedler behandles er ting som er litt uklar for meg fortsatt. Samspillet mellom manuelle og elektroniske prosesser, slik som mantall, skanning osv.
    - Evt: hvorfor ikke?

e) Veien videre:

24) Ser dere for dere å ikke bruke manuell telling ved neste valg?
25) Hvordan skal tellingen gjennomføres ved neste valg- manuelt eller maskinelt

Chapter D
Feedback from the Directorate of Elections

Upon completion of the master's thesis, the thesis was sent to the Directorate of Elections for an evaluation. The Directorate was able to comment on the content, and clarify any misunderstandings. The evaluation resulted in the following appendix, and has been included to document the additional information that was presented.

Tilbakemelding på masteroppgave

Side 4 (1.4 Introduction of EVA Skanning):

Vedrørende boken EVA Skanning - Valgdirektoratet anser ikke dette dokumentet som komplett systemdokumentasjon for EVA Skanning benyttet i 2015. Dokumentet er et internt arbeidsdokument og var ikke tilstrekkelig kvalitetssikret til å anses som systemdokumentasjon.

Side 5 (1.4.1 – 3. punkt):

Vedrørende slengere – dette er avhengig av hvilken type valg. Slengere gjelder kun ved kommunestyrevalg. Ved stortingsvalg er det renummereing og stryking som gjelder.

Side 5 (Figur 1.1):

Skissen gir indikasjon av at det er flere klienter tilknyttet same database, men databaseutgaven er localdb. LocalDb er kun ved «liten utgave» der du gjør opptelling på en maskin. LocalDB er ikke designet for å benyttes av flere klienter. Da må du installere «stor utgave» og sette opp f.eks. Microsoft SQL Server enterprise, standard eller express.

Står noe om de ulike utgavene her https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017?view=sql-server-2017

Side 6 (1.4.2):

Kommentaren om figur 1.1 gjelder her også.

Vedrørende siste setning i delkapittelet – Klienten må være registrert i/ha tilgang til nettverket databasen star i. Dette er ikke unikt for EVA Skanning. Her benytter man anerkjente databaseprodukter med protokoller for håndtering av autentisering som de er avhengig av i en eller annen form. Dette er avhengig av kommunens oppsett. Den kan settes opp med windows autentisering og benytte kerberos, eller brukernavn og passord. Benytter man brukernavn og passord blir passordet lagret med Data Protection API (https://msdn.microsoft.com/en-us/library/ms995355.aspx).

Side 7 (1.5.1 – 2. punkt):
Refereringen til Kommunal- og moderniseringsdepartementet stemmer ikke. Det er den enkelte kommune som gjør egen kost/nytte-vurdering. Alle kan benytte EVA Skanning, uavhengig av størrelse. **OBS!** Dette gjentas også på side 18.

Side 7 (1.5.2 – 2. punkt):
Vedrørende penetrasjonstesten til NSM - Testen ble gjennomført på et oppsett satt opp av en kommune, oppsettet var ikke gjort av Valgdirektoratet.

Vedrørende boken om EVA Skanning – som nevnt, så anser ikke Valgdirektoratet dette dokumentet som komplett systemdokumentasjon for EVA Skanning benyttet I 2015. Dokumentet er et internt arbeidsdokument og var ikke tilstrekkelig kvalitetssikret til å anses som systemdokumentasjon.

Side 28:
Nederste avsnitt: Ved liten installasjon er det ikke nødvendig at klienten er tilkoblet nettverk. Det er mulig å kjøre i nødmodus og koble til nettverk og overføre resultatet når det er klart. Eller ta over den kryptografisk signerte telleresultatfila på en annen maskin tilkoblet nettverk og overføre i nettleseren.

Side 29 (figur):
"password" kan også være windows autentisering, og gjelder også for jobbstyring og verifiser.

Side 31:
Første avsnitt, siste setning: Det er mer korrekt å si at tellingen skjer basert på informasjonen som ligger i databasen.

Side 31 (3.1.4 – andre punkt):
Vi benytter named instance EvaSkanningSmall

Side 32 (3.1.4 – tredje punkt):
Vi benytter kun integrated security med localdb. Dvs at brukernavn og passord ikke er lagret i klartekst med konfigurasjonen.

Side 32 (3.1.5):
Direktoratet er ikke ansvarlig for brannmurkonfigurasjon, men til 2019 prøver vi å støtte kommunene ekstra med dokumentasjon og automatiserte skript der det er mulig.

Side 33 (3.2 – fjerde og nest siste avsnitt):
Som nevnt tidligere er dette avhengig om dette er liten eller stor installasjon. Dvs localdb eller annen utgave av microsoft sql server. Passord lagres nå kryptert i konfigurasjonsfilen ved hjelp av Data Protection API. Samt skript for å hjelpe kommunene å implementere SSL mellom klient og databasen. Dette er da funksjonalitet som allerede ligger i Microsoft SQL Server.

Når det gjelder setningen «When confronted with the assertion, the Directorate stated that this was a complex picture, and that not everything necessarily is motivated by security» er dette en misforståelse. Poenget var at om man har tilgang slik det skisseres er det fremdeles forhold i prosessen som ikke primært er motivert ut i fra sikkerhet som likevel kan gjøre det vanskelig å «treffe» med et angrep. Dette går på organiseringen av selve opptellingen med strekkodelapper og kasser og det at man ville måtte være i stand til å gjennomføre et angrep konsistent for samme sett med stemmesedler over potensielt flere tellinger for å unngå avvik som vil føre til undersøkelser.

Side 33 (3.3 – 1. punkt):
Som nevnt ovenfor, vi utleverer mer støtte/script for å hjelpe kommuene.

Side 34 (3.3 – 2. punkt):
Også som nevnt ovenfor, så hadde kommunene i 2017 muligheten til å bruke integrated security i stedet for brukernavn og passord. Nå krypteres passordet i konfigurasjonsfilen med Data Protection API hvis dette benyttes.

Side 34 (3.3 – 3. punkt):
Det er kun den ene brukeren som benytter EVA Skanning som har tilgang til databaseinstansen.

Side 35 (siste avsnitt):
Det er ikke noe usikkerhet rundt hvem som er ansvarlig for å sikre infrastrukturen som EVA Skanning kjører på – det er kommuenene og fylkeskommunene. Kommunal og moderniseringsdepartementet er rett instans for spørsmål rundt ansvar mellom direktoratet og kommuene.

Side 37 (to midterste avsnittene):
Vedrørende forskjellen mellom stor og liten installasjon - Dette var nok i en annen kontekst. Det er ikke store forskjeller i koden som kjøres på liten og stor installasjon.
Vedrørende eksterne kall – Dette er belyst tidligere. LocalDB lytter ikke til eksterne kall. Andre utgaver av SQL server er avhengig av kunne kommunisere med klientene og autentisere seg for å persistere data. Dette er ikke unikt for EVA Skanning.

Side 40 (3.5):
Flere av disse anbefalingene følges allerede, og bidrar dermed allerede til å sikre EVA Skanning.

Side 41-42 (oppsummering):
En del av innspillene gitt over, gjelder også her. Blant annet gjelder dette merknadene om LocalDB og avsnittet om dialogen med Valgdirektoratet.

Side 58 (testing av EVA Skanning):
Det er viktig at riktige forutsetninger ligger til grunn når man snakker om resultatene av testingen. Som nevnt var programvaren under utvikling og feil var å kunne forvente. Feilen i dette tilfellet var en uhåndtert feil i nye tolkningsmodulen, som ikke ble sendt på riktig måte til EVA Skanning. Årsaken til at man fikk ulikt antall mellom skanningøktene var at bildene blir ikke helt identiske hvis du skanner seddelen flere ganger pga fysiske påvirkninger som f.eks. inndragning i skanneren, som kan utløste feilscenarioet i noen tilfeller.

Side 71 (6.2 – 2. punkt):

Diskusjonen mellom relasjonsdatabase eller ei er ikke sikkerhetsrelatert, men valg av teknologi og arkitektur. Denne uttalelsen baserer seg altså på en misforståelse.

Side 71 (6.2 – 3. punkt):

Disse sårbarhetene er svart ut i tidligere kommentarer.

Chapter E

Information day - Questions

Informasjonsdag hos Valgdirektoratet

1) SPM: Er EVA Resultat ikke en del av EVA Admin?

2) SPM: Men er EVA Resultat noe som har blitt laget i ettertid? De stedene jeg har lest om EVA (bortsett fra i boken om EVA Skanning), står det at systemet består av 3 deler: EVA Admin, EVA Skanning og EVA internettstemming (som nå ikke lenger er i bruk). Jeg har ikke sett at EVA Resultat har vært en egen entitet.

3) SPM: men gjelder det da kommunikasjon mellom tellesentralen og dere (her i Tønsberg) eller innad i tellesentralen også?

4) Ja, det er egentlig det.

5) Bare fortsett slik du har planlagt å legge det opp. Så kommer jeg bare med spørsmål underveis.

6) SPM: Det er her jeg lurer på. Er det mulig for meg å sette opp min egen klient. La oss ta en stor kommune hvor det kreves flere skannere og skannerklienter. Hva er det som hindrer meg fra å sette opp min egen klient og feede inn stemmesedler til databasen?

7) Men det er hver klient, men ikke hver skanner?

8) Og de kommuniserer ikke over nettet?

9) Hvordan kommuniserer klientene med den databasen? Er det mulig for meg å sette opp min klient som feeder noe inn til databasen på det nettverket?

10) Det er ikke noe autentisering mot databasen?

11) Har ikke alle tilgang til å overse tellingen?

12) Det er et mulig alternativ.

13) Det som også gjør et slikt angrep teoretisk mulig er jo at nettopp det eneste som trengs å leses er en stemmeseddel, og den er kjent allerede.

14) Jeg er ikke helt sikker på hvordan dette ser ut, men la oss si det eksisterer et sperrebånd rundt tellesentralen. Hvis klientene kommuniserer med databasen over det lokale nettverket trådløst, og hvis jeg kommer meg inn på det lokale nettet og finner ut hvordan disse kommuniserer seg i mellom, så trenger jeg ikke å stå så langt unna for å få til å dytte noen ekstra stemmesedler inn i databasen

15) Men sjekker databasen dette? Alle ID ene osv? Eller er dette bare for å kunne skanne en seddel?

16) Ja, det er jo i tilfellet noe skjer, hvordan kan man oppdage det. Og da har jeg sett på hva er det som kan skje, fins det noen muligheter. Og det er vanskelig å garantere at det ikke kan skjer angrep, da er det viktig å ha en mekanisme som kan fange opp nettopp det.

17) Men da lurer jeg litt på hva er det som skjer, stemmesedlene telles i databasen, hvilken informasjon er det som blir overført fra skannerklienten til databasen?

18) Jeg skjønner ikke hvor den valgkonfigurasjonsfilen kommer inn i dette?

19) Så den har ikke noe i databasen å gjøre?

20) Liten pause (intervjuer er usikker på hva som blir forklart). Når du sier knyttes til databasen – hva mener du da?

21) Så dette er det som identifiserer stemmeseddelen?

22) Det jo bare å hente meg seg ekstra stemmesedler når man er inne og stemmer, så kommer man seg rundt det.

23) Men hvis du henter med deg et par mens du er inne og stemmer.

24) Det har jeg også tenkt på. Det er derfor jeg har spurt de valgansvarlige i kommunene om avvik mellom manuell og maskinell telling, og det er som oftest den maskinelle de stoler på.

25) Jeg er enig at det nok hadde vært vanskelig å få til et slikt angrep, men er nysgjerrig på om det ville latt seg gjøre og hvordan et eventuelt hadde blitt oppdaget. Og jeg ønsker også å prøve å forstå hvordan kommunikasjonen fungerer.

26) Kan du sende det til meg eller kan jeg ta et bilde?

27) Det jeg har tenkt da, noe som jeg må ha med i oppgaven, om det blir fra dere eller om det blir basert på det dere forteller, så må jeg ha en illustrasjon av arkitekturen. Jeg kan for så vidt lage den selv og sende til dere og høre om dere er enige, eller om jeg kan basere det på noe som dere har laget selv. For det blir vanskelig å skrive en oppgave uten å kunne…

28) Det er en god begynnelse i alle fall. Hvis jeg kunne ha fått den også, den forteller at det er lokalt nettverk. Den viser at det er en *liten installasjon*, sant?

29) Dette er da autentisering mellom EVA Admin og EVA Skanning, ikke mellom EVA Skanning klient og database på det lokale nettverket?

30) Dette gjelder for 2019 systemet eller for det som ble brukt i 2017?

31) Det står på valg.no (https://valg.no/om-valg/om-valg2/det-elektroniske-valgsystemet-eva/) at: *Selv om ikke all informasjon er hemmelig, er all informasjon sikret med de samme mekanismene*
Hvilke mekanismer er det snakk om og hvordan er det gjort?

32) På samme link står det*: I tillegg til sikring av IT-systemet EVA ligger det kontrollmekanismer i valggjennomføringen som sikrer at kompromittering av IT-systemer ikke i seg selv er tilstrekkelig til å påvirke valgresultat – kontrollmekanismene er ikke bundet til om, eller hvilken IT-løsning som brukes. Les mer om hvordan stemmer telles her.*

Hvilken kontrollmekanisme er det snakk om her? Manuell telling? Linken til "les mer om hvordan stemmer telles her" fungerer ikke. Hvor kan jeg finne det?

33) På valg.no (https://valg.no/om-valg/om-valg2/maskinell-opptelling-av-valg-i-norge/) står det: *Systemet EVA Skanning har flere lag med digitale signeringsmekanismer innebygd for å sikre integriteten til systemkoden, biblioteker og ikke minst til dataene. Vi kan derfor være trygge på at det sentrale valgsystemet kun vil snakke med en ekte utgave av EVA Skanning som kommer fra Valgdirektoratet selv.*

Hvilke signeringsmekanismer er det snakk om? Flere lag? Gjelder det mellom scanner og PC eller mellom PC og database?

34) Jeg ser at det er en del sikkerhetsmekanismer som gjør det vanskelig å prøve seg på å endre et resultat etter det er signert osv, men tenker vel mer på kommunikasjonen mellom klient og database.

35) Under møtet i Oslo ble det sagt at systemet er koblet til internett. Jeg lurer på om skannerne er koblet til internett for å kommunisere med PC en, eller om PCen er koblet til internett for å kommunisere med databasen.

36) Sist sa dere at resultatet var signert før det kom til EVA Admin, derfor kunne ikke noen komme og endre det på veien. Signeres resultatet i EVA Skanning eller i EVA Admin?

37) Ja, absolutt. Nå føler jeg har litt mer kontroll, i hvert fall på arkitekturen lokalt der det telles. Og det er vel det jeg fokuserer på. Og hvis jeg har noen spørsmål utover det, så kan jeg kanskje bare sende en mail. Jeg tror egentlig jeg har fått en god del svar.

Chapter F

Questions for Riksvalgstyret regarding ballot counting

DET KONGELIGE KOMMUNAL-
OG MODERNISERINGSDEPARTEMENT

Patricia Aas
Langesgate 13
0165 OSLO

Deres ref	Vår ref	Dato
	17/3899-2	5. september 2017

Spørsmål til Riksvalgstyret om opptelling av stemmer ved valget 2017

Vi viser til henvendelse datert 30. august til riksvalgstyret, og henvendelse til riksvalgstyret, Kommunal- og moderniseringsdepartementet og Valgdirektoratet datert 5. august om opptelling av stemmer.

Kommunal- og moderniseringsdepartementet er sekretariat for riksvalgstyret. Siden dette er et praktisk spørsmål har vi avklart med leder av riksvalgstyret at svaret sendes fra oss. Tall i svaret er hentet inn fra kommunene av Valgdirektoratet.

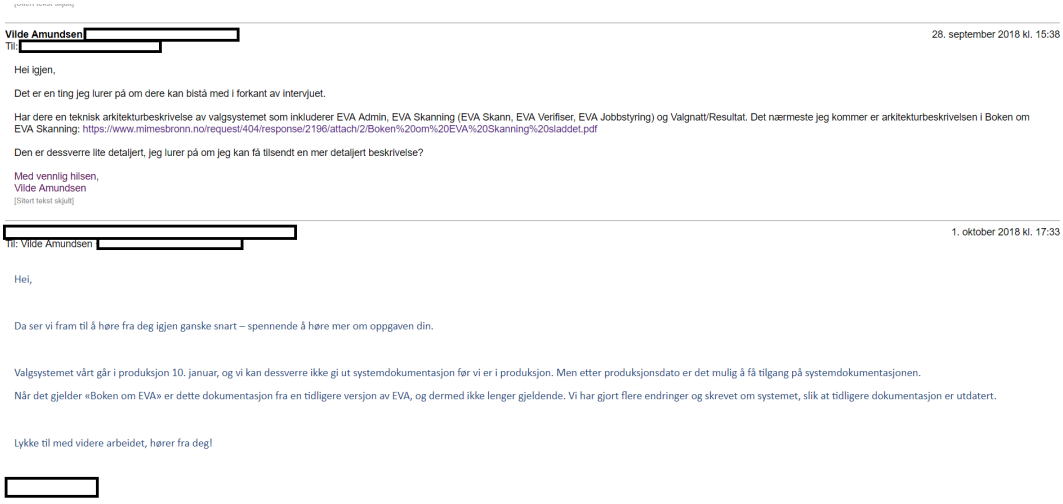
1.Tilsammen hvor mange stemmeberettigede bor i kommuner hvor valgdagsstemmene ikke ville ha blitt manuelt talt?
128 kommune hadde planlagt å skanne både i den foreløpig og den endelig opptellingen. Antall stemmeberettigede i disse 128 kommunene ca. 1 193 000.

2. Av disse, hvor mange bor i kommuner hvor alle maskinelle tellinger skulle foregå i samme lokale?
Det må antas at de kommunene som hadde planlagt maskinell opptelling i både foreløpig og endelig telling ville gjøre det i samme lokale da skannere vanligvis settes opp sentralt i kommunen.

3. Omtrentlig hvor mange forhåndsstemmer skulle bli telt bare maskinelt før fredag?
Forhåndsstemmene telles først opp på valgdagen. Det er ingen opptelling av forhåndsstemmer før mottak av forhåndsstemmer avsluttes 8. september. Det var 175 kommuner som hadde planlagt å telle forhåndsstemmene ved bruk av skanner.

Postadresse	Kontoradresse	Telefon*	Avdeling	Saksbehandler
Postboks 8112 Dep	Akersg. 59	22 24 90 90		Marie Svendsen
0032 Oslo		Org no.		Mjøsund
postmottak@kmd.dep.no	www.kmd.dep.no	972 417 858		22 24 72 69

Chapter G
Mail correspondence with Directorate of Elections



Vilde Amundsen [redacted] 28. september 2018 kl. 15:38
Til: [redacted]

Hei igjen,

Det er en ting jeg lurer på om dere kan bistå med i forkant av intervjuet.

Har dere en teknisk arkitekturbeskrivelse av valgsystemet som inkluderer EVA Admin, EVA Skanning (EVA Skann, EVA Verifiser, EVA Jobbstyring) og Valgnatt/Resultat. Det nærmeste jeg kommer er arkitekturbeskrivelsen i Boken om EVA Skanning: https://www.mimesbronn.no/request/404/response/2196/attach/2/Boken%20om%20EVA%20Skanning%20sladdet.pdf

Den er dessverre lite detaljert, jeg lurer på om jeg kan få tilsendt en mer detaljert beskrivelse?

Med vennlig hilsen,
Vilde Amundsen
[Sitert tekst skjult]

[redacted] 1. oktober 2018 kl. 17:33
Til: Vilde Amundsen [redacted]

Hei,

Da ser vi fram til å høre fra deg igjen ganske snart – spennende å høre mer om oppgaven din.

Valgsystemet vårt går i produksjon 10. januar, og vi kan dessverre ikke gi ut systemdokumentasjon før vi er i produksjon. Men etter produksjonsdato er det mulig å få tilgang på systemdokumentasjonen.

Når det gjelder «Boken om EVA» er dette dokumentasjon fra en tidligere versjon av EVA, og dermed ikke lenger gjeldende. Vi har gjort flere endringer og skrevet om systemet, slik at tidligere dokumentasjon er utdatert.

Lykke til med videre arbeidet, hører fra deg!

[redacted]

Figure G.1: Mail correspondence with the Directorate of Elections regarding *Boken om EVA Skanning*

Vilde Amundsen [redacted] 12. november 2018 kl. 13:43
Til: [redacted]

Hei igjen,

Jeg har akkurat snakket med [redacted] EVRY angående mer detaljert beskrivelse av hvordan tellesystemet settes opp i kommunene. Jeg er interessert i nettverkskonfigurasjon og kommunikasjon mellom de ulike modulene. Jeg så for meg at EVRY som leverandør kanskje kunne bidra med mer informasjon.

[redacted] ønsket ikke å utlevere noe informasjon uten å ha mottatt en skriftlig bekreftelse på deres godkjenning. Jeg forstår at dette kan være vanskelig, men tenkte å høre med dere om det vil la seg gjøre.

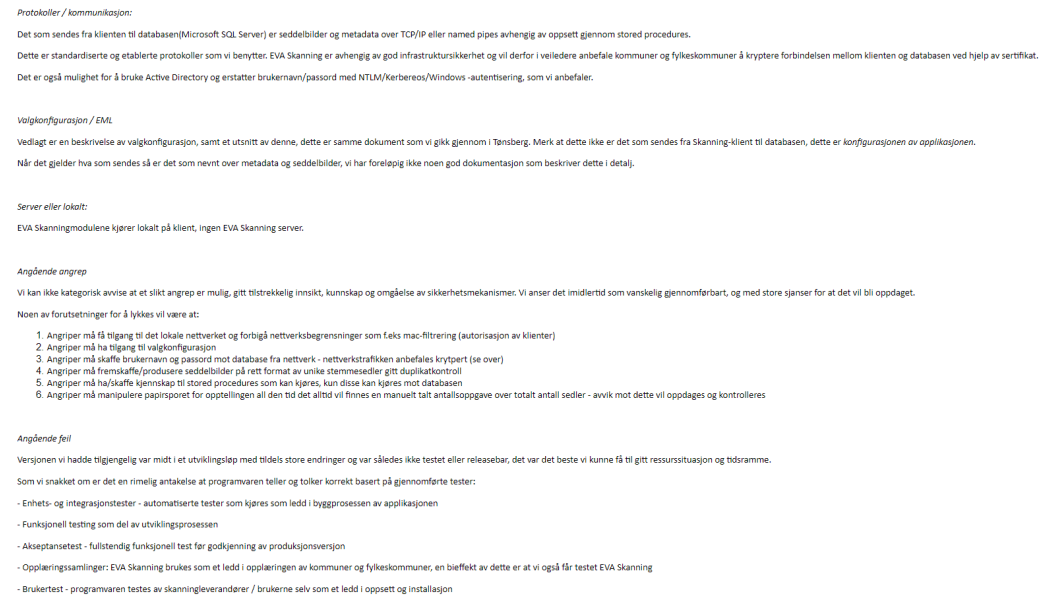
Med vennlig hilsen,
Vilde Amundsen
[Sitert tekst skjult]

[redacted] 14. november 2018 kl. 09:23
Til: Vilde Amundsen [redacted]

Hei
Vi kan ikke gi tilgang på konkrete nettverkskonfigurasjoner, så det går dessverre ikke.
Men vi ser at prinsippene er godt belyst gjennom tilsendt informasjon og gjennomgangen du fikk i Tønsberg.

Lykke til med innspurt av oppgaven.
[redacted]

Figure G.2: Mail correspondence with the Directorate of Elections regarding local area network configurations



Protokoller / kommunikasjon:

Det som sendes fra klienten til databasen(Microsoft SQL Server) er seddelbilder og metadata over TCP/IP eller named pipes avhengig av oppsett gjennom stored procedures.

Dette er standardiserte og etablerte protokoller som vi benytter. EVA Skanning er avhengig av god infrastruktursikkerhet og vil derfor i veiledere anbefale kommuner og fylkeskommuner å kryptere forbindelsen mellom klienten og databasen ved hjelp av sertifikat.

Det er også mulighet for å bruke Active Directory og erstatter brukernavn/passord med NTLM/Kerbereos/Windows -autentisering, som vi anbefaler.

Valgkonfigurasjon / EML

Vedlagt er en beskrivelse av valgkonfigurasjon, samt et utsnitt av denne, dette er samme dokument som vi gikk gjennom i Tønsberg. Merk at dette ikke er det som sendes fra Skanning-klient til databasen, dette er *konfigurasjonen av applikasjonen*.

Når det gjelder hva som sendes så er det som nevnt over metadata og seddelbilder, vi har foreløpig ikke noen god dokumentasjon som beskriver dette i detalj.

Server eller lokalt:

EVA Skanningmodulene kjører lokalt på klient, ingen EVA Skanning server.

Angående angrep

Vi kan ikke kategorisk avvise at et slikt angrep er mulig, gitt tilstrekkelig innsikt, kunnskap og omgåelse av sikkerhetsmekanismer. Vi anser det imidlertid som vanskelig gjennomførbart, og med store sjanser for at det vil bli oppdaget.

Noen av forutsetninger for å lykkes vil være at:

1. Angriper må få tilgang til det lokale nettverket og forbigå nettverksbegrensninger som f.eks mac-filtrering (autorisasjon av klienter)
2. Angriper må ha tilgang til valgkonfigurasjon
3. Angriper må skaffe brukernavn og passord mot database fra nettverk - nettverkstrafikken anbefales krytpert (se over)
4. Angriper må fremskaffe/produsere seddelbilder på rett format av unike stemmesedler gitt duplikatkontroll
5. Angriper må ha/skaffe kjennskap til stored procedures som kan kjøres, kun disse kan kjøres mot databasen
6. Angriper må manipulere papirsporet for opptellingen all den tid det alltid vil finnes en manuelt talt antallsoppgave over totalt antall sedler - avvik mot dette vil oppdages og kontrolleres

Angående feil

Versjonen vi hadde tilgjengelig var midt i et utviklingsløp med tildels store endringer og var således ikke testet eller releasebar, det var det beste vi kunne få til gitt ressurssituasjon og tidsramme.

Som vi snakket om er det en rimelig antakelse at programvaren teller og tolker korrekt basert på gjennomførte tester:

- Enhets- og integrasjonstester - automatiserte tester som kjøres som ledd i byggprosessen av applikasjonen

- Funksjonell testing som del av utviklingsprosessen

- Akseptansetest - fullstendig funksjonell test før godkjenning av produksjonsversjon

- Opplæringssamlinger: EVA Skanning brukes som et ledd i opplæringen av kommuner og fylkeskommuner, en bieffekt av dette er at vi også får testet EVA Skanning

- Brukertest - programvaren testes av skanningleverandører / brukerne selv som et ledd i oppsett og installasjon

Figure G.3: Mail correspondence with the Directorate of Elections regarding possible installation of malicious client on the local area network

Chapter H

Interview guide - Election officials

INTERVJUGUIDE – valgansvarlige

a. Din kommune

2. Navn, nåværende stilling, kommunenavn?
3. Hvor lenge har dere brukt EVA Skanning?
4. Hva er deres tanker om systemet? Fungerer det som det skal? Har dere hatt noen problemer?
5. Hvordan skanner dere? Manuelt og/eller maskinelt?
6. Det har vært litt vanskelig for meg å finne dokumentasjon, siden mye er hemmelig. Hvilke dokumenter beskriver valgprosedyren som skal gjennomføres? Får dere detaljerte instruksjoner? Har dere kjennskap til det boken om EVA skanning?

b. Før valget:

7. Hvem installerer systemet deres? Hvordan foregår installasjonen?
8. Hvilken rolle har skanningsleverandørene i valget? Hvem er de? Kan man velge selv hvilken leverandør man ønsker?
9. Hva avgjør hvilket system dere velger? Hvilken rolle spiller økonomien i valg av tellesystem?
10. Hvordan foregår testing, opplæring og treningen av systemet før valget? Hvem gjennomfører den? Hvem er med? Hvor lang tid brukes det på dette?

c. På valgdagen

11. I følge Boken om EVA Skanning trenger skanneren vedlikehold gjennom valgdagen. Hvordan gjøres dette?
12. Har dere hatt problemer med skanneren ved tidligere valg?
13. Hvem kontakter dere dersom dere har problemer?
14. Det står i Boken om EVA Skanningen at IT kompetanse kan kjøpes fra skanningsleverandørene. Hvilken tilgang har de? Har de tilgang til valgresultatet? Kontaktes de dersom det skjer en feil? Kan de rette feil uten å være til stedet?

d. Etter valget

15. Hvordan håndteres systemet etter valget? Hvem avinstallerer? Hva blir slettet? Hva blir lagret?

e. Sikkerhet og feilhåndtering:

16. Hvilket fokus har dere på sikkerhet? Hvilke tiltak implementerer dere?
17. Hvilke risikoer ser dere for dere at systemet har? Er dette noe dere diskuterer før valget?
18. Hvordan oppdages feil dersom begge tellingene skjer maskinelt?
19. Hva skjer dersom det oppdages en feil?

20. Hvordan er kommunikasjonen med KMD, valgdirektoratet og andre kommuner dersom det skjer en feil?
21. Finnes det dokumenter som forklarer hva som skal gjøres dersom dere oppdager en feil?

Chapter I

Written answers from the Directorate of Elections

Svar til masterstudent Vilde Amundsen 20. desember 2018.

1. Er trafikken i det lokale nettverket på tellesentralen kryptert? I så fall, hvordan?

EVA Skanning er avhengig av god infrastruktursikkerhet og vi anbefaler i veiledere at kommunene og fylkeskommunene krypterer forbindelsen mellom klienten og databasen ved hjelp av sertifikat. Vi anbefaler også å bruke Active Directory og erstatte brukernavn/passord med NTLM/Kerbereos/Windows -autentisering.

2. Hvor og hvordan lagres brukernavnet og passordet til databasen?

Brukernavn og passord finnes i EVA Skanning konfigurasjonsfiler. Oppsett av EVA Skanning blir gjort av kommuner og fylkeskommuner med eller uten bistand fra ekstern leverandør. Valgdirektoratet har inngått en rammeavtale for teknisk bistand på vegne av landets kommuner og fylkeskommuner.

Til valget i 2019 vil brukernavn og passord være kryptert i standardoppsett ved hjelp av Data protection API (innebygget i Windows).

3. Er databasen konfigurert til å lytte etter eksterne eller interne kall? Er dette forskjellig på liten og stor installasjon?

Ved liten installasjon er databasen ikke tilgjengelig for andre enn skanningoperatøren. Det benyttes LocalDB, som bare tillater én bruker å se databasen.
Ved stor installasjon er det avhengig av hvordan brannmuren er satt opp. Men med mindre administrator har åpnet for eksterne tilkoplinger til databasen, er ikke databasen synlig for noen utenfor det lokale nettverket.

4. I en liten installasjon, er klienten (koblet til skanneren) koblet til Internett?

I og med at liten installasjon innebærer èn PC og èn skanner må klienten minimum være tilkoblet internett ved overføring av opptelling fra EVA Skanning (jobbstyring) til EVA Admin. Klienten trenger ikke være tilkoblet internett under skanning og verifiseringsprosessen.

5. Hvordan tolkes partiet på stemmesedlene? Er det ved nummeret nederst til venstre, eller teksten øverst? Hvordan tolkes stempelet? Sjekker programvaren om det er noe der? Eller ser den etter et spesifikt mønster?

Partiet leses ut i fra seddelnummeret nederst på stemmeseddelen. Fra og med 2019-valget leses partinavnet også fra teksten øverst på seddelen, for å kontrollere for eventuelle rettinger utført av velgeren. Stempel tolkes ut i fra fyllingsgrad i stempelfeltet på stemmeseddelen.

6. Har skanningsleverandørene tilgang til å yte fjernsupport? Ifølge dette dokumentet [1] har de det.

[1] - https://www.mimesbronn.no/nn/request/405/response/2439/attach/3/Signert%20kontrakt%20Evry%20Sladdet.pdf

Det er kommuner og fylkeskommuner som er ansvarlige for den praktiske valggjennomføringen, herunder installasjon og oppsett av skanningløsning, samt gjennomføring av maskinell telling av stemmesedler. Valgdirektoratet tilbyr programvare og veiledning rundt bruken av programvaren. I veilederen for 2017 beskrives rutiner og praksis som forhindrer uautorisert eller unødvendig bruk fjernaksess.

Veileder for 2017 valget sier følgende:

"Påse at klientene kun når skanning databasen, EVA Admin-miljøet for EVA Skanning og ID-porten. Det kan være hensiktsmessig med tilgang til valgmedarbeiderportalen og eventuelt lovdata, men dette er strengt tatt ikke nødvendig. Databaseserveren trenger ikke internettilgang."

"Etablere rutiner som sikrer at uvedkommende ikke har tilgang til systemer og stemmesedler"

"Sikre at utstyret blir oppbevart sikker når det ikke er i bruk, og etablere rutiner for låsing og utlogging fra systemet ved fravær fra arbeidsplassen"

"Etablere rutiner som sikrer at alle benytter personlige kontoer ved pålogging"

"Etablere rutiner som sikrer at sertifikater og konto/passord ikke gjøres tilgjengelig for andre. Etablere rutiner som sikrer at alle benytter personlige kontoer ved pålogging"

7. Hvis det er kommunens ansvar å sikre de lokale nettverkene, hvordan kontrollerer dere at dette er gjort sikkert? Hva definerer dere som et sikkert lokalt nettverk?

Vi jobber kontinuerlig med å bedre sikkerhet, både i systemene våre og i andre deler av valggjennomføringen.
Den totale sikkerheten er en kombinasjon av blant annet:
- tekniske løsninger
- tiltak basert på intern/ekstern testing og revisjon
- veiledning og opplæring av valgmedarbeidere, leverandører m.m.
- rutiner og prosesser i opptelling og håndtering av stemmesedler

I tillegg har alle kommuner har et valgstyre som gjennomgår alle avvik og må godkjenne valgoppgjøret. Deretter skal fylkesvalgstyret gjøre det samme. Ved stortingsvalg er det til slutt riksvalgstyret som fordeler utjevningsmandater, og stortinget godkjenning valget. Behandling og godkjenning i flere instanser før endelig resultat fastsettes er en viktig del av valgordningen.

Et sikkert lokalt nettverk har følgende karakteristika:

- Er beskyttet med brannmur mot omverden som kun tillater absolutt nødvendig trafikk ut og inn
- Har mac filtrering for å holde kontroll på tilkoblede klienter
- Trafikk mellom klienter er kryptert
- Er fysisk sikret med kontroll på antall aksesspunkter og aksesspunktenens plassering (kablet nettverk)

8. Hvordan kan offentligheten stole på at EVA Skanning er sikker, hvis det ikke er mulig for offentligheten å kontrollere det?

Vi ønsker å bidra til størst mulig åpenhet om valg og valggjennomføring i Norge, og jobber målrettet med dette. Vi praktiseres åpenhet så langt det lar seg gjøre samtidig som vi må ivareta sikkerheten i valggjennomføringen. Valggjennomføringen er en kombinasjon av manuelle og maskinelle prosesser med kontroll på mange nivåer, og rutiner og prosesser er tilgjengelig på våre portaler valg.no og valgmedarbeiderportalen.no.
Vi jobber kontinuerlig med å sikre at alle som jobber med valg i Norge får god opplæring i prosedyrer og lovverket, blant annet gjennom opplæringssamlinger, webinar og e-læring.
Vi har tett dialog med andre myndigheter og fagmiljøer innen sikkerhet. I tillegg har et eksternt selskap utført revisjon av kildekoden.
Vi har hatt flere penetrasjonstester av både installert system og koderevisjoner av kildekodene. Rapportene fra disse gjennomgangene er for tiden gradert informasjon, men vi vil avgradere store deler av disse når tiltak er iverksatt. Hvilken type testing som da er foretatt vil bli åpent tilgjengelig. Vi har også planlagt flere tester før valget i 2019.
Vi vil publisere systemdokumentasjon og kildekode for valgsystemene i 2019 når systemene går i produksjon (januar, april og juni).

9. Hvorfor har ikke kildekoden for EVA Skanning 2017 blitt publisert? Hvorfor var det ikke mulig å teste denne når jeg var i Tønsberg?

Vi har ikke mottatt innsynskrav til kildekoden fra 2017. Det er stilt spørsmål til når denne tilgjengeliggjøres i henvendelser til oss og i sosiale medier. Vi har prioritert arbeidet med å klargjøre kildekoden for valget i 2019 for publisering på en måte gjør at den kan forstås mht. struktur og sammenheng. Vi jobber med å få systemene våre klare til valg 2019. Det er under en måned til produksjonssetting av de første applikasjonene. Vi jobber med å tilrettelegg for en god og sikker valggjennomføring i 2019, og dette er hovedfokus for oss.
Dette ble også omtalt da du var på besøk hos oss i Tønsberg.

10. Dersom Boken om EVA Skanning er utdatert, og ikke lenger gyldig, er det mulig å få en ikke-sensurert versjon?

Som vi snakket om da du var i Oslo så ble Boken om Eva Skanning benyttet som et internt arbeidsdokument som ikke var tilrettelagt for publisering.
Det er ikke et representativt for systemet slik det er i dag, og vi publiserer ikke utdatert dokumentasjon.

Chapter J

Official reply to consultation memorandum from the Norwegian University of Science and Technology

Bakgrunn
Dette høringssvaret har sitt utgangspunkt i et masteroppgavearbeid av Vilde Amundsen under utførelse dette høstsemesteret ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU, i samarbeid med ekstern veileder M.Sc. Patricia Aas, og intern veileder og faglig ansvarlig professor Stig F. Mjølsnes.

Mastergradsarbeidet har som oppgave å beskrive og undersøke informasjonssikkerheten i EVA Skanning-systemet, og analysere de mekanismer og prosedyrer for å oppdage feil som benyttes i manuell og maskinell telling. Innsamlingen og bearbeiding av informasjon om disse problemstillingene har kandidaten gjort ved å intervjue representanter fra Kommunal- og moderniseringsdepartementet, i Valgdirektoratet og valgansvarlige i 18 kommuner. Videre har Valgdirektoratet gjort en demonstrasjon for studenten av det nye EVA Skanning systemet under utvikling for valget i 2019. Master-rapporten blir ferdigstilt januar 2019, en foreløpig oversikt er gjengitt her til slutt.

Kommentarer til forskriftsendringsforslaget
Departementet foreslår en endret valgforskrift der den foreløpige opptellingen av både forhåndsstemmer og valgtingsstemmer skal foregå for hånd. I tillegg
foreslår departementet at forskriften skal beskrive en rutine (ikke ennå formulert)
ved avvik mellom foreløpig opptelling og endelig opptelling, dersom endelig opptelling er foretatt maskinelt ved skanning.

- Forslaget er: § 37a Foreløpig opptelling av stemmesedler (1) Den foreløpige opptellingen av stemmesedler etter valgloven § 10-4 femte ledd og § 10-5 skal skje ved manuell telling.

1. Tellenøyaktighet og metode
Det er svært interessant å observere den markerte uenighet som uttrykkes når det gjelder spørsmålet om manuell eller maskinell telling er mest nøyaktig og pålitelig. Mens praktikere hevder at maskinell telling reduserer risikoen for feil (se for eksempel andre høringssvar), vil derimot teoretiske artikler av akademikere fremholder manuell telling som gullstandarden. Det kan tenkes at en norsk kilde for slike telleavvik kan hentes fra opptellings-protokoller i kommunene?
Schneier [1] nevner en empirisk undersøkelse gjort ved Rice University publisert i 2012 som estimerer feilraten i to manuelle tellingsmetoder til mellom 1% og 2% [2]. En (lovfestet) feilrate for telling i amerikanske valg på 1 feil per 10 millioner skannede stemmeseddel-linjer er nevnt på websiden votersunite.org. Samme sted er det listet skannerutstyr brukt i valgsammenheng med typisk feilrate på 1 feil per 1000 linjer og mer [3].

2. Feiltyper
Det er metodisk viktig å skille mellom minst tre typer feil, kategorisert etter årsak. Det er tilfeldige feil (f.eks. mekanisk årsak), systematiske feil (f.eks. programvarefeil), og intensjonelle feil/angrep (f.eks. uautorisert database-endring) , som hver krever sin egen analysemetodikk. Uenigheten beskrevet i kommentar 1 kan ha sin forklaring i en sammenblanding av analysemodellene for disse.

3. Manuell foreløpig opptelling
Uautorisert manipulasjon av tellemaskiner kan i prinsippet gjøres skjult og i forkant, dette er vel dokumentert i mange internasjonalt publiserte papers over det siste tiåret. Følgende må det etableres kontrollmekanismer for å oppdage slike angrep. En manuell foreløpig opptelling vil kunne hjelpe til med å detektere manipulerte tellemaskiner i endelig opptelling ved at avvik blir synlig, der telleprosessene er uavhengige. På den andre siden: ``hensikten med den foreløpige opptellingen er å komme frem til et raskt foreløpig resultat som kan presenteres for publikum'' (sitat fra Den norske valgordningen i hovedtrekk, kap.6). En manuell foreløpig telling vil selvsagt ta mer tid enn en maskintelling. Departementet begrunner valget av at den foreløpige opptellingen skal gjøres manuelt, og ikke den endelige, at den foreløpige opptellingen av valgtingstemmer kan foregå på stemmestedene.

- Forslag til ny § 37a (2) er: Ved avvik mellom en foreløpig og en endelig opptelling som er foretatt maskinelt, skal opptelling foretas på nytt. Ny maskinell opptelling kan ikke foretas av de samme personer som foretok endelig opptelling første gang.

4. Uavhengige telleprosesser

Uavhengige funksjonelle prosesser er et sentralt konsept i design av pålitelige systemer. En ny maskinell opptelling kan gjøres mest mulig *uavhengig* av forrige maskintelling ved å benytte uavhengig installerte skannere, andre datamaskiner og programvare, separat datakommunikasjon, og skifte operatører for å unngå gjentak av samme mulige systematiske og/eller intensjonelle feil.

5. Noe om statistisk sampling for verifisering av valgresultat

Stikkprøvekontroll av for eksempel 1% av stemmesedlene er en enkel form for etterprøving med (forfeilet) hensikt å styrke et valg er gjennomført med korrekt utfall. Prof. Stark ved U.C. Berkeley har nylig foreslått en mer effektiv metode basert på statistisk hypotese-testing som han kaller "risk-limiting audit" [4]. Masteroppgaven vil undersøke om slike metoder passer i norsk valgorganisering.

Om informasjonssikkerheten i valgteknisk system EVA

Masterkandidatens foreløpige resultater viser at det er lite offentlig informasjon tilgjengelig om EVA Skanning. Valgdirektoratet ønsker heller ikke å spesifisere hvordan det lokale nettverket i kommunene settes opp. Kandidaten oppfatter det derfor slik at informasjonssikkerhet ikke er prioritert. Hoved-mekanismen for feildeteksjon som benyttes er avhengig av en sammenligning av resultatet fra den foreløpige og den endelige tellingen. Dersom begge tellingene gjøres maskinelt finnes det ikke et pålitelig sammenlignbart resultat (under antakelsen om at manuell telling gir korrekt resultat). Dersom foreløpig telling gjøres manuelt, vil det i de fleste kommuner være den endelige maskin-opptellingen som blir registrert, der også eventuell omtellingen som oftest gjøres maskinelt. Dette nedvurderer verdien av den manuelle tellingen.

Referanser

[1] https://www.schneier.com/blog/archives/2012/02/error_rates_of.html

[2] GOGGIN, Stephen N.; BYRNE, Michael D.; GILBERT, Juan E. Post-election auditing: effects of procedure and ballot type on manual counting accuracy, efficiency, and auditor satisfaction and confidence. *Election Law Journal: Rules, Politics, and Policy*, 2012, 11.1: 36-51.

[3] http://www.votersunite.org/info/AccuracyIgnored.asp

[4] LINDEMAN, Mark; STARK, Philip B. A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, 2012, 10.5: 42-49.

Chapter K

NSA Report on Russia Spearphishing

[redacted] DIRNSA

National Security Agency

Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, [redacted] Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any foreign government outside of the original recipients.

SUMMARY (U)

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [redacted] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance [redacted]

Declassify On: 20420505

and beacon out to malicious infrastructure. In October 2016, the actors also created a new email address that was potentially used to offer election-related products and services, presumably to U.S.-based targets. Lastly, the actors sent test emails to two non-existent accounts ostensibly associated with absentee balloting, presumably with the purpose of creating those accounts to mimic legitimate services.

Campaign Against U.S. Company 1 and Voter Registration-Themed Phishing of U.S. Local Government Officials (S//SI//REL TO USA, FVEY/FISA)

Russian Cyber Threat Actors Target U.S. Company 1 (S//REL TO USA, FVEY/FISA)

(TS//SI//OC/REL TO USA, FVEY/FISA) Cyber threat actors [redacted] executed a spear-phishing campaign from the email address noreplyautomaticservice@gmail.com on 24 August 2016 targeting victims that included employees of U.S. Company 1, according to information that became available in April 2017.[1] This campaign appeared to be designed to obtain the end users' email credentials by enticing the victims to click on an embedded link within a spoofed Google Alert email, which would redirect the user to the malicious domain [redacted].[2] The following potential victims were identified:

- U.S. email address 1 associated with U.S. Company 1,
- U.S. email address 2 associated with U.S. Company 1,
- U.S. email address 3 associated with U.S. Company 1,
- U.S. email address 4 associated with U.S. Company 1,
- U.S. email address 5 associated with U.S. Company 1,
- U.S. email address 6 associated with U.S. Company 1, and
- U.S. email address 7 associated with U.S. Company 1.

(TS//SI//OC/REL TO USA, FVEY/FISA) Three of the malicious emails were rejected by the email server with the response message that the victim addresses did not exist. The three rejected email addresses were U.S. email address 1 to 3 associated with U.S. Company 1.

1. (TS//SI//OC/REL TO USA, FVEY/FISA) *The GRU* [redacted] *is also rendered as military unit* [redacted]
2. (TS//SI//OC/REL TO USA, FVEY/FISA) *For additional information on* [redacted] *and its cyber espionage mandate, specifically directed at U.S. and foreign elections, see* [redacted]

[redacted] DIRNSA

(TS//SI//OC/REL TO USA, FVEY) COMMENT: The [redacted] actors were probably trying to obtain information associated with election-related hardware and software applications. It is unknown whether the aforementioned spear-phishing deployment successfully compromised all the intended victims, and what potential data from the victim could have been exfiltrated. However, based upon subsequent targeting, it was likely that at least one account was compromised.

Cyber Threat Actors Create Spoofed Account and Voter Registration-Themed Targeting of Local Government Officials (TS//SI//OC/REL TO USA, FVEY/FISA)

(TS//SI//OC/REL TO USA, FVEY/FISA) The [redacted] cyber threat actors created a new operational email account vr.elections@gmail.com with the username "U.S. Company 1" on 27 October 2016. (COMMENT: It is likely that the cyber threat actors created this email address to appear as if they were an employee of U.S. Company 1.) The cyber threat actors had in the email account two trojanized Microsoft Word documents with the titles "New_EViD_User_Guides.docm" and "NEW_Staging_Checklist_AIO_Style_EViD.docm". Both of these documents had identical content and hash values, and contained the same malicious Visual Basic script. The body of the trojanized documents contained detailed instructions on how to configure EViD software on Microsoft Windows machines. According to EViD's FAQ website (UNCLASSIFIED), EViD software allows poll workers to quickly check a voter's registration status, name and address. (END OF COLLATERAL)

(TS//SI//OC/REL TO USA, FVEY/FISA) Subsequently, the cyber threat actors used the vr.elections@gmail.com account to contact U.S. email addresses 1 to 122 associated with named local government organizations. (COMMENT: It possible that the targeted email addresses were obtained from the previously compromised account(s) of U.S. Company 1.) The "NEW_Staging_Checklist_AIO_Style_EViD" document was last modified on 31 October 2016 and the "New_EViD_User_Guides" document was last modified on 1 November 2016. (COMMENT: This likely indicates that the spear-phishing campaign occurred either on 31 October or 1 November , although th e exact date of the spear-phishing campaign was not confirmed.)

(TS//SI//REL TO USA, FVEY) COMMENT: Given the content of the malicious email it was likely that the threat actor was targeting officials involved in the management of voter registration systems. It is unknown whether the aforementioned spear-phishing deployment successfully compromised the intended victims, and what potential data could have been accessed by the cyber actor.

Technical Analysis of the Trojanized Documents (U//FOUO)

(TS//SI//OC/REL TO USA, FVEY/FISA) Both trojanized Microsoft Word documents contained a malicious Visual Basic script that spawns PowerShell and uses it to execute a series of commands to retrieve and then

run an unknown payload from malicious infrastructure located at a U.S. IP address on port 8080, probably running Microsoft-IIS/7.5 Server. (COMMENT: The unknown payload very likely installs a second payload which can then be used to establish persistent access or survey the victim for items of interest to the threat actors.) The request used a user-agent string of "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko". Lastly, the malicious Microsoft Word documents hashed to the following values:

- MD5 Hash:5617e7ffa923de3a3dc9822c3b01a1fd,
- SHA-1 Hash:602aa899a6fadeb6f461112f3c51439a36ccba40, and
- SHA-256 Hash:f48c9929f2de895425bdae2d5b232a726d66b9b2827d1a9ffc75d1ea37a7cf6c.

Operational Accounts Spoofing Legitimate Elections-Related Services (S//REL TO USA, FVEY)

Spoofing Email Address Associated With U.S. Company 2 (U//FOUO)

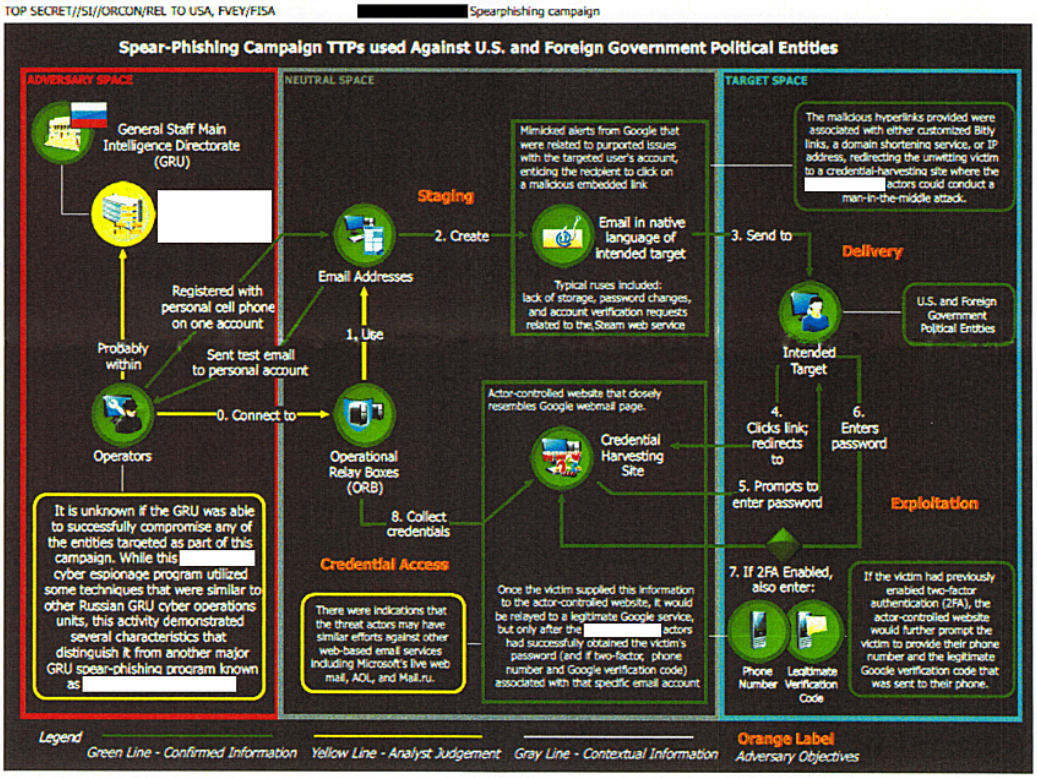
(TS//SI//OC/REL TO USA, FVEY/FISA) In parallel to the aforementioned campaign, the [redacted] cyber threat actors created another new operational email account elevationsystem@outlook.com on 19 October 2016. They then used this email address to send a test message to another known [redacted] operational email account. In that test email, which was written in English, the threat actors spoofed U.S. Company 2, and offered election-related products and services. All emails associated with this account were later deleted, and it was unknown if there was any targeting using this email account. (COMMENT: G iven that the email body was written in English and prepared less than 1 month before the 2016 U.S. Presidential election, it was likely intended for U.S.-based targets.)

Spoofing Absentee Ballot Email Addresses (U//FOUO)

(TS//SI//OC/REL TO USA, FVEY/FISA) Additionally, the [redacted] cyber threat actors sent what appeared to be a test email to two other accounts, requestabsentee@americansamoaelectionoffice.org and r-questabsentee@americansamoaelectionoffice.org. In both cases the actors received a response from the mail server on 18 October stating that the message failed to send, indicating that the two accounts did not exist.

> (TS//SI//REL TO USA, FVEY) COMMENT: Given that the test email did not contain any malicious links or attachments, it appeared the threat actors' intent was to create the email accounts rather than compromise them, presumably with the purpose of mimicking a legitimate absentee ballot-related service provider.

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA [redacted] Spearphishing campaign



TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA