Office for Democratic Institutions and Human Rights

NORWAY

INTERNET VOTING PILOT PROJECT
LOCAL GOVERNMENT ELECTIONS
12 SEPTEMBER 2011

OSCE/ODIHR Election Expert Team Report

Warsaw
2 March 2012

TABLE OF CONTENTS

NORWAY
INTERNET VOTING PILOT PROJECT
LOCAL GOVERNMENT ELECTIONS
12 September 2011

OSCE/ODIHR Election Expert Team Report

I. EXECUTIVE SUMMARY

Following an invitation from the Government of Norway to the OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR), the OSCE/ODIHR deployed an Election Expert Team (EET) to follow the preparations and conduct of the internet voting pilot project during the 12 September 2011 local government elections.

The Ministry of Local Government and Regional Development (hereinafter the ministry) initiated an "E-elections 2011" pilot project in August 2008. The ministry's formulated objective was to establish a secure internet voting platform, which would provide improved accessibility for voters. During these elections, internet voting was used as an additional voting channel for voters registered in 10 selected municipalities, whether in country or abroad. It was available during the advance voting period from 10 August to 9 September. A total of 27,557 voters, or 16.4 per cent of eligible internet voters, chose to vote by internet.

The internet voting pilot project was conducted in an open and inclusive manner. Election stakeholders, despite some who questioned the principle of remote internet voting, expressed confidence in the overall administration of the internet voting pilot.

The election act (Representation of the People Act) provides for electoral pilot projects and the internet voting was principally governed by regulations issued by the ministry, which incorporated previous international recommendations on electronic voting. However, many aspects of the internet voting pilot project were not formalized, including the set-up, operation, security, testing and data disposal procedures, as well as defining the grounds for determining invalid electronic votes. The pilot could have benefited from more formalized procedures and a clear time plan from set-up, to operation and counting.

The pilot was implemented under the responsibility of the ministry, which acted impartially and professionally in performing its duties, aiming for high levels of transparency and accountability. Due to unforeseen technical complexities, the ministry experienced delays in the process which affected aspects of operational security and led to errors, but without any reported influence on the integrity of the elections.

The ministry employed high standards in ensuring the security of the internet voting system, including carefully designed hardware and software components and robust encryption schemes to protect the secrecy of the vote. More comprehensive testing, stricter adherence to the segregation of duties, and the provision of comprehensive operational documentation could have further improved security. While good technical efforts were undertaken to prevent the system against denial-of-service attacks, election authorities could have improved collaboration with relevant actors in this regard. The ministry did not educate voters of the potential risks of voting over the internet and how best to protect their computers against malicious software.

To permit verifiability and provide transparency the ministry published the complete internet voting software solution on its website. While this effort at transparency is laudable, the final version of the software was only displayed after election day.

In an effort to permit end-to-end verifiability of elections, internet voters received specially-designed and secret return codes. These allowed voters to check whether their votes were cast as intended. At the same time, the system did not include provisions for voters to verify if their votes were actually counted as cast. Due to the complexity of the design and lack of comprehensive tests of this feature prior to the elections, the authorities experienced some technical problems and minor delays.

The ministry provided substantial technical documentation intended to explain the design of the overall internet voting system. The information geared towards the software implementation, rather than for running the system and did not include step-by-step instructions in terms of set-up, configuration, and operation of the system, which could have been used to easier follow the system's operations. The ministry decided not to formally certify the internet voting system, and undertook no audit to assess if the system functioned as intended, two measures which could have added additional oversight.

The ministry provided full access for observation of all stages of the process. However, the OSCE/ODIHR EET was the only body that conducted consistent, if only partial, observation of the different aspects of internet voting in Norway. It was granted full access to all components and documentation, and was able to follow all related electoral events.

II. INTRODUCTION

On 19 January 2011, the Ministry of Local Government and Regional Development (hereinafter, the ministry) invited the OSCE/ODIHR to follow the pilot project on internet voting during the municipal elections on 12 September 2011. Following an initial assessment visit from 2 to 4 March 2011, the OSCE/ODIHR decided to deploy an Election Expert Team (EET) consisting of one election/legal analyst and two new voting technologies (NVT) analysts.

The OSCE/ODIHR EET followed the use of NVT throughout the process to assess the internet voting pilot practice and provide recommendations for possible improvements. The team conducted a total of six visits during the various stages of internet voting, including the setup and configuration, the start and close of voting, the counting of electronic votes, and data destruction. Its assessment is based on OSCE commitments together with other international standards for democratic elections, as well as with Norwegian legislation.[1]

The OSCE/ODIHR EET wishes to thank the ministry, as well as other national institutions, the pilot municipalities, election authorities, candidates, political parties and civil society organizations for their co-operation during the course of the team's deployment.

[1] OSCE/ODIHR election reports regarding Norway can be found at http://www.osce.org/odihr/elections/norway.

III. BACKGROUND

In 2004, the ministry appointed a working committee from among various stakeholders to assess the possibilities of introducing electronic voting. Two years later, the committee issued a comprehensive report recommending a step-by-step process with the eventual goal of introducing internet voting.[2] Although the initial plan recommended in the report was to gain experience from a gradual approach through the use of electronic voting components in polling stations only, the ministry initiated the "E-elections 2011" pilot project in August 2008. The ministry's stated objective was to "establish a secure internet voting platform for parliamentary, county, and municipal elections, which will provide improved accessibility to voting to all voters" and to use it as an additional voting option in 2011 local government elections.[3]

At the start of the project, the ministry made a call for participation for interested municipalities, with the condition that the application had to be approved by the municipal council. Eleven municipalities were initially selected, based on geographic location and size of the municipality, in order to have a representative and balanced sample.

In May 2010, three MPs submitted a motion to stop the internet voting pilot project, claiming that remote internet voting does not ensure a free and secret vote. The motion was put to vote in the parliament on 19 November 2010 and was endorsed by three political parties. The parliament decided by a majority vote to continue with the pilot project.[4] During this debate, two municipalities cancelled their participation, out of which one was replaced. As such the internet voting pilot was carried out in ten municipalities.[5] In March 2011, the final scope of the project was formally defined with the release of the regulations on internet voting.[6]

IV. OVERVIEW

A. ELECTORAL FRAMEWORK

In contrast to parliamentary elections, in local government elections there is no election commission at the national level to oversee the election process.[7] The elections are organized by county and municipal election commissions. All citizens aged 18 or older can vote on two separate ballots for the county and the municipal councils, depending on which

---

2 See at: http://www.regjeringen.no/upload/kilde/krd/red/2006/0087/ddd/pdfv/298587-evalg_rapport_engelsk201106.pdf.

3 See at: http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Prosjektdirektiv_evalg2011_English.pdf. In addition to internet voting, the project included a few other improvements that were tested. This included an electronic election administration system with an online voter register, standardized format of ballots and standardized scanning equipment for the final counting procedures of paper-based ballots. The OSCE/ODIHR EET, however, did not assess any other process than the internet voting pilot.

4 The decision was taken by 60 votes against 44 votes.

5 Drammen and a district in Oslo canceled their participation. Sandnes replaced Drammen and participated in the pilot together with Bodø, Bremanger, Hammerfest, Mandal, Radøy, Re, Tynset, Vefsn and Ålesund.

6 Ministry of Local Government and Regional Development Regulations No. 355.

7 The authority of the national election commission is limited to appeals for elections at the national level. See 2009 OSCE/ODIHR EAM report, Election Administration chapter, http://www.osce.org/odihr/elections/norway/40529.

municipality they had registered their residence on 30 June. In total, some 3.8 million voters were eligible to vote in the 12 September 2011 local elections. Among them, a total of 167,985 voters were eligible to vote in municipalities that piloted internet voting.

Voters abroad could make use of controlled paper-based voting at diplomatic missions from 1 July to 2 September. In locations with no Norwegian diplomatic missions, postal voting was available. If a voter voted in advance outside of his/her municipality during early voting or by postal vote, he/she received only a unified ballot paper with no possibility to express a preferential choice among listed candidates.[8]

Internet voting was only open during the advance voting period, which ran from 10 August to 9 September. Early voting by paper ballot was also possible in all municipalities during the same period, as well as during the early voting period[9] between 1 July and 9 August. On election day, internet voters were also able to cast their paper ballots at polling stations in their municipalities.

Municipalities sent every voter a polling card by post, informing them where and when to vote. The polling card was not a necessary requirement for voting, however, but its use sped up the process in the polling station. For eligible internet voters, the posted polling card contained return-codes, which enabled each internet voter to verify if their internet vote had been received by the server and stored unchanged in the electronic ballot box.

B. LEGAL FRAMEWORK

The Representation of the People Act (hereinafter, election act),[10] together with regulations relating to parliamentary and local government elections issued by the ministry[11] form the legal framework for local government elections.

While the election act provides for electoral pilot projects[12] the internet voting was principally governed by regulations issued by the ministry,[13] which took into account the Council of Europe's (CoE) recommendations on electronic voting.[14]

Currently, the internet voting regulations lack detailed provisions related to requirements for internet voting and refer instead to the pilot project website, where technical requirements are documented.[15] As a result, many aspects of the internet voting pilot were not formalized, including the set-up, operation, security, testing, and data disposal procedures. In addition, the regulations did not define the concrete grounds for invalidating an electronic vote.

---

8 See the 2009 OSCE/ODIHR EAM report, Early and Advance Voting chapter.

9 In contrast to advance voting, a process of early voting also takes place in which voters have to make special arrangements by notifying municipal authorities.

10 Promulgated in June 2002. Last amended in May 2011 with minor technical amendments.

11 Representation of the People Regulations no. 5, issued on 2 January 2003.

12 Via Article 15.1 of the election act, the King of Norway gives his consent for pilot projects. In practice, however, the King has delegated broad decision making powers to the government.

13 Regulation no. 355, issued on 31 March 2011, as amended on 23 June 2011.

14 Between 2002 and 2004, the Council of Europe developed the only international document on electronic voting. This recommendation Rec(2004)11 includes a set of over 100 legal, technical and organizational recommendations and is available at: https://wcd.coe.int/wcd/ViewDoc.jsp?id=778189.

15 See http://www.evalg.dep.no.

It is recommended that the legal framework is further delineated to include formalized procedures and a time plan for the conduct of internet voting from set-up and operation to counting. Special attention could be given to the experience and best practice gathered in the course of this pilot project.

Any complaints on electoral matters, including internet voting, can be filed with the municipal council, no later than seven days after election day.[16] The council's decision can be appealed to the ministry, which has the final decision, but cannot be brought to the courts.[17] The ministry has the authority to declare a particular election invalid and order a new election in the event that the allocation of council seats could be effected by the appeal.

The Data Protection Inspectorate (DPI), an independent state agency, implements the Personal Data Act (PDA), which regulates the automatic processing of personal data among other things.[18] It gave DPI the authority to stop the operation of data applications, including the internet voting pilot, if personal data is improperly handled.[19]

C. DESIGN

The internet voting pilot was designed to follow the procedure and layout of paper-based voting. In this pilot, a registered voter first opened a webpage,[20] which loaded the required software. The system first authenticated the voter with a username and password, which is also used for identification with other governmental internet applications. When entered correctly, a PIN code was sent to his/her mobile phone, which the voter then entered.[21] Next, the electronic ballots were provided, on which the voter chose one list of candidates. The voter also had the option of casting a blank ballot. In the background and not visible to the voter, the system then encrypted the ballot and signed it with the voter's digital signature.[22] Finally, the voter transmitted the ballot via the server to be stored in the electronic ballot box.

In an effort to provide end-to-end verifiability, the pilot project introduced the use of so-called return codes. Internet voters received specially-designed and secret return codes that allowed voters to verify that his/her cast votes were accurately stored in the electronic ballot box (but not to verify if their votes were counted as cast): when each encrypted ballot was stored, a mathematical function allowed the calculation of these return codes without actually decrypting (opening) the ballot.[23] The codes were then sent by SMS to the voter who could compare them with the unique return codes listed on the voter's polling card. Due to the complexity of the design and lack of comprehensive tests of this feature prior to the elections, the authorities experienced some technical problems and minor delays.

---

16 Article 13-4 of the election act.

17 The 2009 OSCE/ODIHR EAM report and the Venice Commission and OSCE/ODIHR Joint Opinion on the Electoral Legislation of Norway, available at http://www.osce.org/odihr/elections/norway/75054, recommended to include courts in the electoral appeals process.

18 Promulgated in April 2000.

19 The decision of the DPI can be appealed to the independent Privacy Appeals Board.

20 http://www.evalg.stat.no.

21 This is checked by the ID-portal system.

22 As personal ID cards in Norway don't have digital signatures, the voting system assigned one to each voter taking part in the pilot.

23 Return codes were designed as a feature of the El Gamal encryption model, chosen for these elections.

Each voter could re-vote over the internet as often as he/she wanted. Similar to postal voting, the voter's identity was tied to a ballot until the first stage of the counting process, when the encrypted ballot was separated from the ID in the so-called cleansing process. This eliminated multiple ballots from the same voter, ballots from voters who also voted with a paper ballot and ballots from voters not on the voter list. This process also included a check for the validity of a voter's identity. The ballots were then mixed to remove any means of restoring the connection with the voter's identity. Only thereafter were the ballots decrypted using the secret decryption key and tallied.

D. COMPONENTS

The internet voting pilot comprised several main components with a multi-tier design, described in more detail in the project documentation published by the ministry.[24] These components were:

Voting Application: The voting application was a web program that managed all interactions of the internet voting system with the voter. It provided the user (voter) interface, downloaded the java-based secure voting client that encrypted the ballots and provided connection to the Vote Collector Server.

ID-portal: This component authenticated the voters. It is owned and fully operated by the Agency for Public Management and eGovernment (DIFI). Voters needed to sign up to the ID-portal in a one-time registration process.

Vote Collector Server (VCS): This server contained the electronic ballot box located in a data centre in Brønnøysund, which is owned and operated independently by the state agency, Brønnøysund Register Centre (BRC). It reports to the Ministry of Trade and Industry.

Return Code Generator (RCG): This component calculated and transmitted the return codes, via SMS. The RCG is located in a data centre in Tønsberg, which is owned and operated independently by the Directorate for Civil Protection and Emergency Planning (DSB). It reports to the Ministry of Justice and the police.

The ministry servers: This multi-tier component, operated exclusively by the ministry, consisted of cleansing, mixing and counting servers. The cleansing server was responsible for the cleansing process to eliminate multiple ballots from the same voter, ballots from voters that also voted by paper ballot, and ballots from voters not on the voter list. The mixing server mixed the ballots. The counting server decrypted the mixed ballots and tallied the election results.

The ministry configured the VCS and the RCG remotely, using special configuration laptops through a secure connection in a virtual private network (VPN).[25] The ministry servers were initially located at the Crisis Support Unit (CSU) under the Ministry of

[24] See at: http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/technical-documents.html?id=612104.

[25] A VPN is a secure (private) connection between two computers or networks over the public internet.

Justice. This building was heavily damaged during the 22 July bomb attack;[26] hence the servers had to be moved to the less-suitable ministry premises, which were not originally foreseen for hosting servers.

E. PROCUREMENT, MANAGEMENT, AND OVERSIGHT

In March 2009, the ministry initiated a well-documented and transparent procurement process to acquire a complete software solution for internet voting and the online election administration system. The ministry further engaged in a six-month process of competitive dialog with the bidding companies and consortia in order to improve the project specifications. The contract was awarded in December 2009, and the complete tender documentation was made available on the ministry's website.[27]

The ministry had ownership and responsibility for the internet voting system and managed the pilot project. Due to the nature of internet voting, one electoral body charged with co-ordinating it would increase the level of accountability of election administration.

It is recommended that for internet voting, a body with the power to oversee internet voting is formalized. The authorities could determine the distribution of roles and responsibilities between stakeholders involved in internet voting.

The contracted vendor was required to deliver the final software by 1 November 2010. However, the delivery was significantly delayed until 1 July 2011, which considerably decreased the time available to eliminate potential errors. In addition, some changes to the final software were made at a very late stage, including during the voting period. For instance, the final software version used for the vote count was delivered on 10 September, two days before the vote count. The ministry explained to the OSCE/ODIHR EET that the complexity of the internet voting system was underestimated. A number of other technical challenges emerged as a result of the delay and time pressure of the project implementation.

F. INTEGRATION OF INTERNET VOTING WITH PAPER-BASED VOTING

A crucial feature of this internet voting was the ability of voters to override their electronic ballots by casting paper ballots at any time during advance voting, or in polling stations on election day. The system strictly controlled possibilities for double-voting. Ballots cast over the internet before or after paper voting by the same voter were discarded during cleansing, as paper ballots take precedence. The 'one voter, one vote' principle was ensured by counting only the paper ballot or the electronic ballot cast last.

Internet voting was an additional voting channel that voters from the ten selected pilot municipalities were free to use from anywhere, including from outside of Norway. Electronic ballots were instantly available at the start of the advance voting period and voters did not need to go to their embassy or to mail postal votes. In contrast to voters voting outside their municipality or by post, internet voting provided the same ballot paper layout as the paper ballot in polling stations on election day.

---

[26] The attack involved a car bomb explosion in Oslo's government district followed by a shooting rampage at a youth summer camp for members of the Norwegian Labour Party.

[27] See at: http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/technical-documents/specification-tenders-evaluation-and-con.html?id=612121.

V. THE INTERNET VOTING ELECTORAL PROCESS

The internet voting pilot project was conducted in an open and inclusive manner. Election stakeholders, despite some questioning the principle of internet voting, expressed confidence in the overall election administration, including of internet voting.

A. TESTING AND SET-UP OF THE SYSTEM

From October 2010 through May 2011, the participating municipalities conducted a series of pre-pilot internet test elections for youth councils or local referenda, one in each of the ten municipalities piloting internet voting. The main purpose of the internet-based test elections was to see if the system worked as intended. The tests also provided valuable training for the election authorities. New versions of internet voting software were put to use in test elections as features were progressively added.[28] The last version of the software, however, was not completed in time to be tested during any of the trial elections.

It is recommended that election authorities fully test the final version of the internet voting system in test elections before using it in regular, binding elections.

The internet voting system was configured jointly by technicians working at the data centres in BRC and DSB, and by the ministry. During the EET, BRC technicians and those working in the ministry demonstrated a professional level of expertise in properly setting up the system. In DSB, the set-up of the respective servers was conducted by companies that the OSCE/ODIHR EET did not meet.

In both cases, the installation and configuration of the system components were not documented in detail. This would have helped streamline the process and alleviate any complications during the set-up procedures.

The election authorities could consider producing and publishing command level protocols and appropriate instructions for installing and configuring all hardware and software components.

In addition, a detailed operational document could be compiled, comprising all internet voting procedures, to be made publicly available ahead of the election. This could be used as the basis for any audit.

B. PRODUCTION OF POLLING CARDS

The printing process for polling cards containing return codes was created by the printing company and approved by the ministry. However, the printing was not comprehensively tested before the elections, resulting in technical problems that prolonged the process.

The production of polling cards was planned to be completed by the end of July. However, it was discovered on 2 August that three political parties contesting elections had been erroneously excluded from the return code sets. The ministry thus had to recreate and reprint all return codes and polling cards in a contracted period of time. The recreation of

[28] The return codes were introduced in the two test elections: in Radøy in March and Re in April 2011.

return codes in Oslo was also complicated as some essential data for printing was stored in the CSU, which remained inaccessible for several days after the 22 July terrorist attack. The printing of the return codes was completed one day after advance voting had started on 10 August.

The ministry discovered some 30 misprints. Due to a lack of testing of the printing process, voters either did not receive polling cards with the return codes, or voters received two polling cards with different return codes, of which the affected voters were informed. In addition, during the voting period, 74 voters, mainly from one municipality, informed the election authorities that their codes received by SMS did not match those printed on the polling card. The ministry explained to the OSCE/ODIHR EET that they had been able to establish beyond doubt that these errors were a result of the printing process, rather than any electoral manipulation.

In order to enhance the integrity of the overall internet voting process, it is recommended that the printing process of polling cards be further tested and improved, allowing enough time for proper testing.

C. VOTING

Due to problems in the production of return codes, polling started late in two municipalities.[29] Voters could vote 24-hours a day and the ministry periodically published approximate turnout information on its website. The internet voting was conducted in a professional manner without any reported technical problems experienced by the election administration.[30]

The interface for the voter was available in several languages.[31] Voters who were visually impaired were able to use standard accessibility features like Braille or screen readers on their computers. The voting interface was tested for usability and accessibility and appeared informative, intuitive and easy to use to the OSCE/ODIHR EET. The help desk located in Brønnøysund received a total of 641 calls to assist voters with issues they encountered. No formal complaints were received.

A total of 55,785 ballots were deposited in the VCS.[32] Voters still voting at closing received a 'ten minutes' notice at midnight of 9 September to conclude voting, after which the VCS was locked. According to the authorities, voters voted by internet from within Norway and from 35 different countries.[33] A total of 27,557 voters, or 16.4 per cent of the electorate of the ten pilot municipalities chose to vote by internet. However, 72.4 per cent of those voters who chose to vote during the advance voting period voted by internet.

---

29 The problems were solved later the same day, on 10 August. In Sandnes and Ålesund, polling cards were not delivered to some half of the voters before the opening of the polls, as estimated by the ministry, due to delays in printing in combination with the time needed for postal delivery. Some voters received their polling cards two to three days after the opening of the polls.

30 Minor problems included integration issues of Java RTE in Microsoft Internet Explorer 9 (outside of the control of election authorities in Norway) and a few reported cases of long periods of time needed for voters' computers to encrypt and send the electronic ballot.

31 Norwegian Bokmål and Nynorsk, English, Polish, Russian, Serbian/Croatian and Somali.

32 This figure includes ballots for both county and municipal council elections.

33 More precisely, voters' registered mobile phones to receive SMSs with return codes from 35 different countries; some of those voters may have voted from Norway.

D. COUNTING

In order to provide for the secrecy of the ballot decryption key, a so-called 'Electoral Board' was formed for the internet voting pilot, comprising ten representatives of different political parties. On 2 August, each of the ten members publicly received one section of the secret key.

The day after the close of internet voting, operators from the ministry downloaded the encrypted votes from the VCS through secure means of a VPN and started with the vote cleansing, the first step of preparations for the vote counting. During the cleansing, a total of 1,775 electronic ballots were discarded as multiple votes, and 519 ballots were discarded due to voters also voting via paper ballot.

In addition, seven ballots were discarded due to voters not being included in the voter list in the relevant municipality at the time of counting although, according to the ministry, they were on the voter list at the time of voting. The ministry explained that this had occurred in cases where voters had moved to another municipality beforehand and had also voted in the advance voting. Due to the updating of voter lists after 30 June these votes were subsequently deleted. However, as stipulated in the ministry regulations, voter lists should not be updated after the cutoff date in cases where a voter has already cast an advance ballot. This is also the practice with paper ballots.[34]

It is recommended that procedures are developed to ensure that no internet votes cast are invalidated because of late voter register updates.

On election day, the ministry organized a counting meeting during which the Electoral Board reconvened to assemble the decryption key for the first time. On election day, the ballots were decrypted and counted immediately after the close of polls. Once the results were established, the ministry experienced a two-hour delay in publishing and uploading the results onto the online election administration system. This delay was due to an insufficiently tested feature of the program for integrating internet voting results with paper-based voting results. The ministry conducted the vote count professionally and in a well-organized process, experiencing only minor technical difficulties. The ministry provided transparency and all present had a clear view of procedures and handling of the election materials. No complaints were filed related to the vote count and election results.

Due to complexities in the decryption process, the validity of nine votes could not be clearly determined. The ministry established that the invalid ballots were generated either by the voters themselves, by changing the content of the ballot, or through an error in the voting application that added the same candidate or party more than one time in the vote.[35] It is of concern that these invalid ballots were accounted for only after election results were communicated.[36] As there was no close race and the number of votes in question did not

---

34 According to Article 2-8 of the election act, voters should be notified of any changes in the voter lists that affects them. See also Ministry of Local Government and Regional Development Regulations No. 5, 2 January 2003, Articles 1 (f) and 2 (3).

35 The Ministry of Local Government and Regional Development Regulations No. 355 on internet voting does not establish criteria for determining the invalidity of an electronic ballot. Article 10-1(1)f of the election act states that the advance ballot should be invalid if the voter has not cast an approved ballot.

36 The sub-contracting company analyzed this issue and reported to the ministry on 17 October 2011.

have an impact on the ranking of candidates/parties in the results, the ministry stated that the invalidation of these ballots did not influence the election results.

It is recommended to establish clear criteria for determining invalid votes in the electoral framework and that procedures are updated to ensure timely detection thereof.

The ministry contracted a private company to test the accuracy of the counting process with individually designed software. This software employed so-called zero knowledge proofs using the mathematical characteristics of the encryption model to prove that no ballots were added, the encrypted ballots were mixed without alteration, and the ballots were accurately decrypted. However, the remaining formal mathematical proof that the cleansing worked accurately was applied only after results were communicated to the municipalities.

E. DATA DISPOSAL

In order to ensure the secrecy of the votes after elections, the ministry conducted safe deletion of digital files and physical destruction of memory disks used in the production and transfer of sensitive data. Prior to the opening of advance voting, the destruction of the copies of the secret keys stored in the VCS and the RCG took place. The destruction of all copies of the electronic ballot box and all storage media used during the internet voting in the VCS and on ministry computers in Oslo was conducted nine days after the results were determined.

The data destruction process was not formalized in scope and timeframe. Such an approach would further increase the transparency of the process.

The election authorities could describe and formalize the process of data destruction in detail within the regulatory framework.

VI. SECURITY

A. SECURITY AND SECRECY OF THE VOTE

The ministry designed a sophisticated system that involved multiple organizational entities and locations and a novel, specially-designed, advanced cryptographic scheme to protect the secrecy and security of ballots cast in uncontrolled environments. The possibility to re-vote and cancel the vote over internet via paper ballots was one way to limit the possibility of voter coercion or vote buying.[37] Despite the complexity of the system, the strict separation of duties was not always followed, leading to a theoretical possibility that the votes and voter identities could have been copied and later reconstructed.

It is recommended that strict separation of duties is defined and documented at all levels, and included in the electoral regulatory framework.

The management of the secret encryption and decryption keys is an important aspect to the secrecy of the vote. The ministry introduced procedures to control and limit access to these

[37] The coercer could not be certain if the voter's coerced voting over the internet is the last voter's choice unless the coercer engaged in a potentially costly exercise to control the voter's actions for an extended period of time. A similar principle holds for vote buyers.

keys by its technicians, to avoid one person alone having access. However, these procedures were not documented in detail and, in at least one observed case, not followed.

It is recommended that the ministry documents the procedures for the management of secret election keys in detail.

Due to the current design of the encryption model chosen for the internet pilot project, the election decryption key was not independent of other information, but was calculated by using the two secret encryption keys used in the VCS and the RCG. This led to a situation in which the secret decryption key depended on other information stored in more than one physical location, which increased the risk of mismanagement.

It is recommended that the ministry continues to improve the encryption model in order to further tighten the security and secrecy of the vote as well as to reduce complexity in set-up, configuration and testing.

B. SECURITY OF INTERNET COMMUNICATION

During the preparatory phase, the ministry performed an analysis of potential threats.[38] Also, a company was specifically hired to perform different penetration tests and was unable to find vulnerabilities.[39]

The ministry made appropriate efforts to secure the system's components against intrusion. While the internet voting system was designed to treat voters' computers as inherently insecure and possibly infected with malicious software, like an attacker trying to read or change a voters' choice, no systematic effort was made to instruct voters how to protect their computers. The voter received a return code via SMS on his/her mobile phone by the system, which he/she could check against codes provided on their polling card. In case of deviations, they could check if their return codes were correct with the hotline provided by the ministry. However, a malicious agent could potentially be able to read and harvest voters' choices without being detected.

The election authorities could consider informing voters of the potential risks of voting over the internet and how best protect their computers against malicious software.

A serious threat for internet voting is a potential denial-of-service (DoS) attack, in which a malicious agent(s) can overburden the election servers and prevent voters from casting ballots. However, an attacker needs to be extremely resourceful to sustain a DoS attack for a longer period and the month-long advance voting period, in itself, is an effective tool against such a possible attack. The ministry relied on its own resources to prevent any attacks, including the high-level protection built into the VCS and RCG. The ministry did not foresee a need for collaboration with authorities and/or companies specialized in monitoring and securing the Norwegian internet infrastructure.[40] The ministry did not discover any attack attempts during these elections. However, any such attack could put the whole internet voting process at risk and have an impact on public confidence.

---

38 See at: http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/tekniskdok/Security_Objectives_v2.pdf.

39 The company was Combitech AB, from Sweden.

40 One such authority is the crisis emergency response agency NorCERT, which monitors the security of internet connections.

It is recommended that election authorities consider collaboration with relevant agencies actively engaged in providing monitoring and general security of the internet connectivity and, include entities that own and operate major parts of the internet backbone in Norway.

C. SECURITY OF OPERATIONS

All system components at the data centres were mirrored and operated redundantly by using multiple servers so that a failure of a single hardware component would not have negative impact on voters' ability to vote. Also, the election data was replicated in real time to adjacent locations to prevent data loss.

The IT infrastructure was protected by uninterruptible power supply. Batteries and diesel generators in separate rooms at each location ensured protection against power outage, and cooling systems protected against overheating. The data centres were connected to the internet over two separate connections.

The BRC and DSB data centres were not certified according to international information security standards, such as ISO 27,000.[41] However, state-of-the-art operation security mechanisms were applied and security standards were implemented which resulted in significant protection against data loss and unavailability of services.

VII. TRANSPARENCY AND ACCOUNTABILITY

Transparency and accountability of internet voting differs significantly from that of traditional methods of voting, as specific knowledge of ICT and cryptography is required to fully comprehend the system. The public trust in the integrity of elections lies in the ability of any interested individual to ascertain that the system functions as described and in compliance with all regulations and requirements.

The ministry required that the software solution of the winning bid must be made publicly available, thereby significantly increasing the level of transparency of the underlying system. The ministry published the full software solution on its website on 3 June 2011, allowing two months for stakeholders to scrutinize the software before the opening of polls.[42] However, the published software was not the latest version that was actually used and then published on 6 October 2011. The ministry explained to the OSCE/ODIHR EET that time pressure had forced it to prioritize the management of elections over some aspects of transparency.

It is recommended that the election authorities publish the version of the software to be used in internet voting in advance of the opening of the polls.

As required for public projects, the internet voting pilot was evaluated on the project-management level and by a private company with regard to financial expenditures.

---

41 For further information, see: http://www.27000.org.

42 See at: https://source.evalg.stat.no/websvn.

A. CERTIFICATION

The CoE 2004 recommendations on electronic voting state that certification of electronic voting systems should be in place. In addition, the CoE 2011 Guidelines on Certification describe the certification process as a measure ranging from testing and auditing to formal certification in which a certificate is issued.[43] The ministry decided not to formally certify the internet voting system, arguing that it was not needed considering the narrow scope of the pilot project, but that it would be pursued in future applications of the system.

The election authorities could consider delegating formal certification of the internet voting software to an independent competent third party to further increase accountability and transparency.

B. AUDITING

The task of an audit is to assess if the internet voting system functioned as intended, having in mind technical and procedural aspects of the system. The ministry did not foresee a need to include auditing as an obligatory factor in the internet voting regulation and no auditing took place for these elections. The ministry explained to the OSCE/ODIHR EET that it did not want to hire an auditor as part of the project, fearing a conflict of interest. The ministry, however, stated that it was open for any auditing efforts and had anticipated that independent institutions might come forward with requests to audit.

The ministry provided and published substantial technical documentation intended to explain the design of the internet voting system. However, it was mostly geared towards software implementation, rather than for running the system. It did not include step-by-step instructions in terms of set-up, configuration, and operation of the system, which could be used to follow the system's operations more easily.

The election authorities could include provisions in the regulations to explicitly allow for audits to assess if the conduct of the internet voting system functions as intended.

C. OBSERVATION

The ministry provided full access for observation of all stages of the process. However, there was little interest among electoral stakeholders in observing internet voting. This seems partly due to a widely-reported high level of trust in the election authorities to conduct elections securely and accurately. The OSCE/ODIHR EET was the only entity that conducted consistent, if only partial, observation of the different aspects of internet voting in Norway. The EET was granted full access to all components and documentation, and able to follow all related electoral events.

The ministry did not publish a calendar of important events during the preparation and conduct of internet voting. In addition, the internal timetable of key events was developed in detail, but in an *ad hoc* fashion and was frequently adjusted due to delays in the implementation of the system. The ministry informed the OSCE/ODIHR EET about changes in their internal calendar when queried.

---

[43] See Guidelines of the Committee of Ministers of the Council of Europe on Certification of E-voting Systems (2011) at: http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_certification_EN.pdf.

In order to formalize and ensure adherence to events in the conduct of elections, and in order to provide further transparency of internet voting, the election authorities could prepare a detailed election calendar in advance of the election period.

The ministry organized a series of training sessions for representatives of local election authorities, however, no such trainings were provided for electoral contestants.

The election authorities could consider providing trainings to political party representatives and domestic non-partisan observers to familiarize them with the internet voting process and raise awareness for effective election observation.

D. VERIFICATION

The introduction of return codes to allow voters to check whether their votes had been cast as intended was a first step towards full end-to-end verifiability of elections. The particular design of internet voting in Norway allowed for the voter to verify if the vote was cast as intended, but not whether the vote has been counted as cast. The return codes constitute proof of the voter's choice at the time of voting, but they are not a definitive proof, since voters can re-vote over the internet, or cast a paper based ballot.

In addition, the chosen cryptographic model allowed interested individuals to universally verify the correctness of the count using formal mathematical proofs, but the proofs were only completed after communicating results to the municipalities.[44]

It is recommended that the election authorities conduct a full review of the impact of return codes on the security and secrecy of the vote, as well as the timeliness of the universal verification of the count, with the aim to allow for full end-to-end verifiability of elections.

[44] See also chapter on Counting in this report.

ANNEX 1: ELECTION RESULTS

County elections (in the pilot municipalities)

Municipality	Number of eligible voters	Number of e-votes*	Number of cleansed e-votes	Number of valid e-votes **
Bodø	36,635	6,953	258	6,695
Bremanger	2,955	406	30	376
Hammerfest	7,502	1,032	39	993
Mandal	11,764	1,374	56	1,318
Radøy	3,687	742	32	710
Re	6,616	933	36	897
Sandnes	48,689	8,279	344	7,935
Tynset	4,163	790	34	756
Vefsn	10,456	1,268	50	1,218
Ålesund	33,457	5,220	191	5,029
Total	**165,924**	**26,997**	**1,070**	**25,927**

* Before cleansing
**Including blanks

Municipal elections (in the pilot municipalities)

Municipality	Number of eligible voters	Number of e-votes*	Number of cleansed e-votes	Number of valid e-votes **
Bodø	36,635	7,226	269	6,957
Bremanger	2,955	445	38	407
Hammerfest	7,752	1,190	64	1,126
Mandal	11,764	1,523	66	1,457
Radøy	3,687	810	42	768
Re	6,870	1,042	61	981
Sandnes	48,689	8,518	325	8,193
Tynset	4,163	959	56	903
Vefsn	10,456	1,386	58	1,328
Ålesund	34,535	5,679	245	5,434
Total	**167,506**	**28,778**	**1,224**	**27,554**

* Before cleansing

**Including blanks

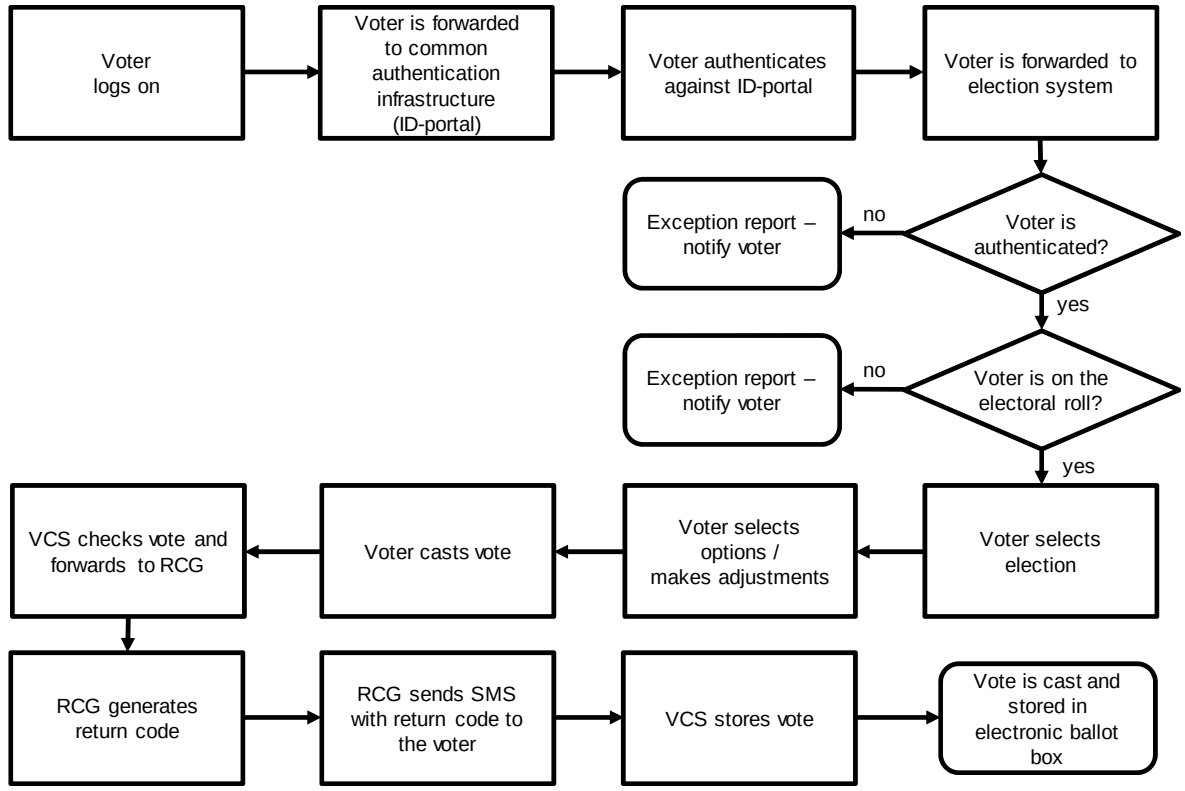
Total cast, cleansed and valid e-votes (county and municipal elections)

Total e-votes cast*	55,775
Total of cleansed votes	2,294
Total valid votes	53,481

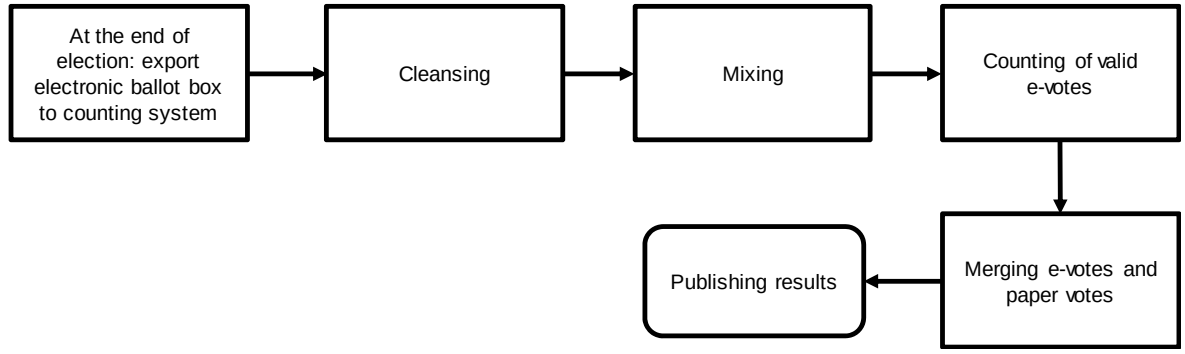
*does not include 9 invalid votes

ANNEX 2: INTERNET VOTING AND COUNTING PROCESSES

Voting Process

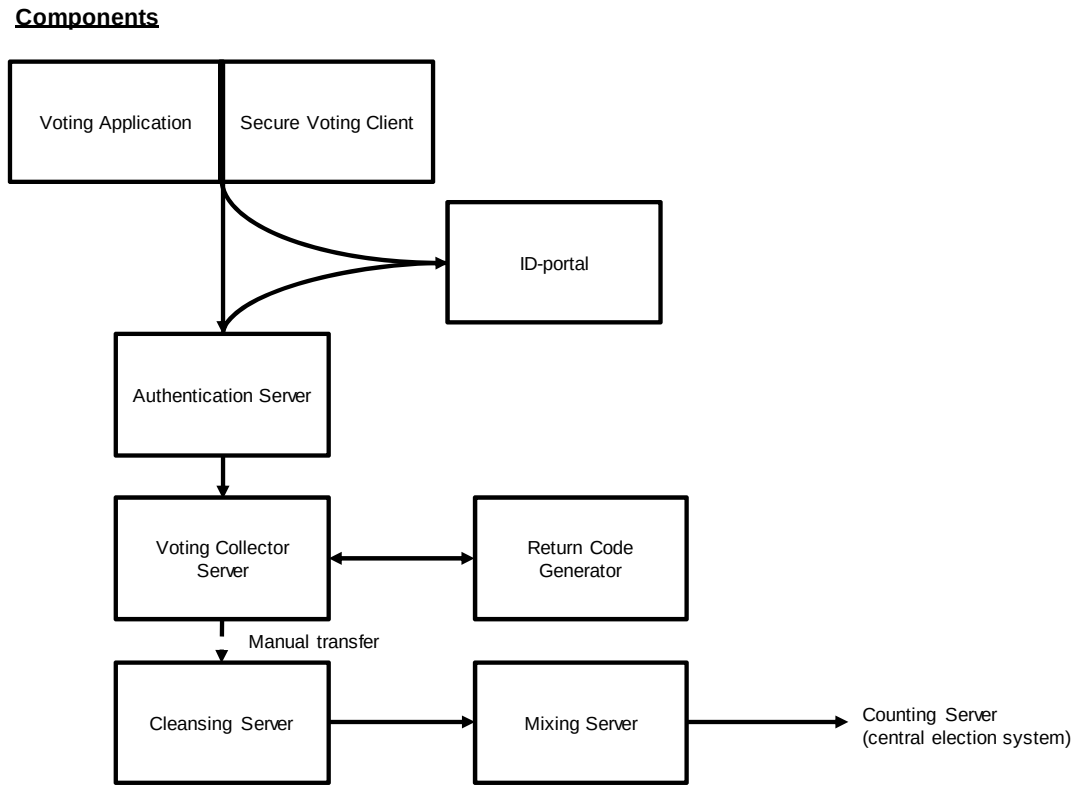


Counting Process



Source: OSCE/ODIHR

ANNEX 3: COMPONENTS



Source: OSCE/ODIHR

ABOUT THE OSCE/ODIHR

The Office for Democratic Institutions and Human Rights (OSCE/ODIHR) is the OSCE's principal institution to assist participating States "to ensure full respect for human rights and fundamental freedoms, to abide by the rule of law, to promote principles of democracy and (…) to build, strengthen and protect democratic institutions, as well as promote tolerance throughout society" (1992 Helsinki Summit Document). This is referred to as the OSCE human dimension.

The OSCE/ODIHR, based in Warsaw (Poland) was created as the Office for Free Elections at the 1990 Paris Summit and started operating in May 1991. One year later, the name of the Office was changed to reflect an expanded mandate to include human rights and democratization. Today it employs over 130 staff.

The OSCE/ODIHR is the lead agency in Europe in the field of **election observation**. Every year, it co-ordinates and organizes the deployment of thousands of observers to assess whether elections in the OSCE region are conducted in line with OSCE Commitments, other international standards for democratic elections and national legislation. Its unique methodology provides an in-depth insight into the electoral process in its entirety. Through assistance projects, the OSCE/ODIHR helps participating States to improve their electoral framework.

The Office's **democratization** activities include: rule of law, legislative support, democratic governance, migration and freedom of movement, and gender equality. The OSCE/ODIHR implements a number of targeted assistance programmes annually, seeking to develop democratic structures.

The OSCE/ODIHR also assists participating States in fulfilling their obligations to promote and protect human rights and fundamental freedoms consistent with OSCE human dimension commitments. This is achieved by working with a variety of partners to foster collaboration, build capacity and provide expertise in thematic areas including human rights in the fight against terrorism, enhancing the human rights protection of trafficked persons, human rights education and training, human rights monitoring and reporting, and women's human rights and security.

Within the field of **tolerance** and **non-discrimination**, the OSCE/ODIHR provides support to the participating States in strengthening their response to hate crimes and incidents of racism, xenophobia, anti-Semitism and other forms of intolerance. The OSCE/ODIHR's activities related to tolerance and non-discrimination are focused on the following areas: legislation; law enforcement training; monitoring, reporting on, and following up on responses to hate-motivated crimes and incidents; as well as educational activities to promote tolerance, respect, and mutual understanding.

The OSCE/ODIHR provides advice to participating States on their policies on **Roma and Sinti**. It promotes capacity-building and networking among Roma and Sinti communities, and encourages the participation of Roma and Sinti representatives in policy-making bodies.

All ODIHR activities are carried out in close co-ordination and co-operation with OSCE participating States, OSCE institutions and field operations, as well as with other international organizations.

More information is available on the ODIHR website (www.osce.org/odihr).