Compliance with International Standards

Norwegian E-Vote Project

Jordi Barrat i Esteve and Ben Goldsmith

June 2012

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
25 YEARS

Global Expertise. Local Solutions.
Sustainable Democracy.

Compliance with International Standards

International Foundation for Electoral Systems
1850 K Street, NW, Fifth Floor
Washington, DC 20006
Email: editor@ifes.org
Fax: 202.350.6701

Compliance with International Standards

Norwegian E-vote Project

INTERNATIONAL FOUNDATION FOR ELECTORAL SYSTEMS
IFES
25 YEARS

Global Expertise. Local Solutions.
Sustainable Democracy.

Compliance with International Standards

Norwegian E-vote Project

Jordi Barrat i Esteve and Ben Goldsmith

June 2012

Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the International Foundation for Electoral Systems.

About IFES

The International Foundation for Electoral Systems (IFES) supports citizens' right to participate in free and fair elections. Our independent expertise strengthens electoral systems and builds local capacity to deliver sustainable solutions.

As the global leader in democracy promotion, we advance good governance and democratic rights by:

- Providing technical assistance to election officials
- Empowering the under-represented to participate in the political process
- Applying field-based research to improve the electoral cycle

Since 1987, IFES has worked in over 135 countries – from developing democracies, to mature democracies.

For more information, visit www.IFES.org.

Table of Contents

1. Executive Summary

This assessment report on *Compliance with International Standards* has been conducted as part of a larger assessment of the Norway E-Vote Project, a pilot of Internet voting during the September 2011 local government elections. This report represents one of seven assessment topics conducted on behalf of the Ministry for Local Government and Rural Development (hereafter "the Ministry") in order to analyze the recent pilot, and determine whether a broader adoption of Internet voting would be suitable for future Norwegian elections.

The compliance of the Norwegian Internet voting system with international electoral standards is especially relevant as some of these standards have been directly adopted into the Norwegian electoral legal framework for the 2011 Internet voting pilots. The Ministry's Regulations Relating to Trial Electronic Voting[1] states, in Section 3, that the Council of Europe's Legal, Technical and Operational Standards for E-Voting[2] (hereafter referred to as 'the Council of Europe Recommendations' or 'the recommendations') forms the basis of these trials, unless otherwise specified.

The Ministry, therefore, requested that an assessment be conducted to evaluate the compliance of the Norwegian Internet voting system with the Council of Europe's Recommendations, as well as other international electoral standards relating to electronic voting. In doing this assessment, each recommendation was categorized as whether the Norwegian Internet voting system complied with it or not.

Assessment by Category of Compliance

Of the 112 Council of Europe Recommendations, the Norwegian Internet voting system was found to be fully compliant with 85 of them. For 10 recommendations, the system was found to be partially compliant and for three recommendations it was determined that the system was non-compliant. For the remaining 14 recommendations, 10 were found to be not applicable for the Norwegian Internet voting system and for a further four it was not possible to determine compliance.

The reasons why the Norwegian Internet voting system was found to be non-compliant with three recommendations related to the fact that it was possible for invalid ballots to be accepted by the system and for ballots to be submitted after the end of the 30 minute voting session limit. In both cases the voter received no indication that an invalid vote had been cast, which would not be included in the count, and invalid ballots were not recorded as invalid on the system but discovered in a post-election audit.

The Norwegian Internet voting system was found to be partially compliant for 10 recommendations due to a number of factors. Amongst these partially compliant assessments, access to information was a

[1] See www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/E-valgsforskriften_endelig_versj_230611_engelsk.pdf, [last accessed May 10, 2012].

[2] Council of Europe (2004) Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and Explanatory Memorandum, at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Key_Documents/Rec percent282004 percent2911_Eng_Evoting_and_Expl_Memo_en.pdf [last accessed November 3, 2011].

recurring theme. This includes issues such as:; the late availability of the final version of the source code, the unavailability of the authentication portal components for review by the Ministry, the need for a simplified system of documentation, observer access to system interventions, public procedures for checking the status of software, and open access to audit logs.

Control procedures were another theme amongst these cases of partial compliance. Key issues were: the need for coherent and comprehensive procedures for the management of the Internet voting system being required, and to better include the municipal and county electoral committees (as the bodies legally responsible for the local elections) in the management of the Internet voting system.

Additionally, the failure to initially include the Internet votes in one county's election results, the failure to provide special measures for elderly voters to try out the Internet voting system before the election and the requirement for an external check/certification of the new Internet voting system also led to findings of partial compliance.

For three of the four recommendations for which it was not possible to determine if the Norwegian Internet voting system was compliant, the inability to determine compliance was due to the possibility for the system to generate and accept invalid ballots. Additionally, one recommendation relates to the conclusions and consequences of the audit process. As this is still ongoing, it is not possible to determine compliance with the recommendation.

Of the 10 recommendations which are found to be not applicable, seven of them are specifically excluded from the Norwegian electoral legal framework by the Regulations Relating to Trial Electronic Voting. The remaining three recommendations relate to online candidate nomination and voter registration, neither of which is part of the Norwegian Internet voting system being trialled.

Thematic Assessment

The thematic assessment section of the report covers a number of issues that were seen as important in the assessment of the Norwegian Internet voting system's compliance with the Council of Europe Recommendations. While some of these key issues arise out of areas in which the Norwegian Internet voting system was found to be non-compliant or partially compliant with the recommendations, this is not always the case.

Secrecy and Freedom of the Vote – the need for a secret ballot, and for the voter to freely express their opinion when voting, are fundamental electoral principles. As a consequence, these principles play a prominent role in the Council of Europe Recommendations and other sources of international electoral standards. Internet voting in general, and specific aspects of the Norwegian Internet voting system, presents a number of challenges to the realization of these principles. Secrecy at the point of voting, the link between the voter identity and the vote value in the system, and the use of return codes, are key issues in this regard.

In the opinion of this assessment that these issues are addressed in a way that successfully reduces the risks associated with remote Internet voting to acceptable levels and the Norwegian Internet voting system is in compliance with secrecy and freedom of the vote aspects of the Council of Europe

Recommendations. This finding is based on the opportunities that Internet voters have for repeat voting, either through additional Internet votes or by casting a paper ballot, and the primacy attached to the paper ballot. This means that even if an Internet voting act is observed or subject to coercion, a subsequent vote can still be cast and that any paper ballot cast from a supervised environment will supersede an Internet ballot.

Invalid Ballots – in principle, invalid Internet votes should not exist as voting software should be designed so that making invalid ballot choices is not possible. However, nine invalid ballots and one out-of-time ballot were recorded during the 2011 local government elections. That the invalid and out-of-time ballots did not produce an error message to the voter and in fact resulted in return codes being sent, led to all three findings of non-compliance with the recommendations in this assessment. The fact that the cause of these invalid ballots could not be determined and that the different possible causes would lead to different assessments of compliance, led to three findings that it was not possible to determine compliance with the Council of Europe Recommendations.

While the issue of invalid Internet ballots was the largest cause of non-compliance in the assessment, the issue needs to be put into perspective. There were only 10 invalid votes, split across a number of elections. The impact was negligible, and did not affect the results in any way. It is also worth noting comparisons with paper voting, remote and in person, which do permit the submission of invalid ballots and do not inform the voter that this is the case upon submission. Furthermore, the Internet voting solution supplier is now aware of the issue and a modification to the system has been identified which will deal with this issue in the future.

Audit - the need to be able to audit the functioning of an electronic voting system is also very prominent in the Council of Europe Recommendations. The need for transparency and the possibility to audit the correct functioning of the system have been central to the design of the Norwegian Internet voting system. The system is also designed to allow E2E verification.

Despite the audit requirements included in the Council of Europe Recommendations being extensive and detailed in nature, the Norwegian Internet voting system has managed to implement mechanisms that, in the opinion of the IFES team, manage to fully comply with these audit requirements. Not only was this audit of the process possible, but it was conducted by an organisation that was, in principle, independent.

Compliance With Other Emerging Electronic Voting Standards – other emerging standards relating to electronic voting largely deal with issues also covered by the Council of Europe Recommendations, but sometimes identify a requirement that is slightly different to the recommendations, or add to the requirements of the recommendations. Of the 15 additional emerging standards identified, the Norwegian Internet voting system was found to be in compliance with 11, with two being assessed as partially compliant and two as non-compliant.

The non-compliant standards related to the need for independent certification of electronic voting systems. The Council of Europe Recommendations also contains provisions relating to certification procedures, but these recommendations were excluded by the Ministry in the Regulations Relating to

Trial Internet Voting. The intention is that the Norwegian Internet voting system would only be certified if it is to be used more widely in the future. The two emerging standards with which the Norwegian Internet voting system is seen to be partially compliant relate to transparency and access to information.

Conclusion

As a package, the Council of Europe Recommendations represents a very comprehensive and detailed set of standards for the conduct of electronic voting. For the Norwegian Internet voting system to fully comply with 85 of the 102 relevant recommendations and only be non-compliant with three recommendations, is a significant achievement given the exacting nature of the Council of Europe Recommendations. Even the three non-compliant recommendations and the 10 partially compliant recommendations should be carefully considered within the relevant context.

This was a pilot of a new Internet voting system in Norway. The nature of a pilot is that it is used as a learning exercise. In this context, findings of non-compliance need not be seen as a failure of the Internet voting system. In fact, many of the issues identified in this assessment would be relatively easy to remedy in any future implementation of Internet voting in Norway. The one technical issue identified, invalid ballots, already has a solution identified, which the Ministry has tested and believes will resolve the problem in the future.

The use of remote Internet voting from uncontrolled environments will always present challenges when it comes to issues such as secrecy and freedom of the vote. Voting from uncontrolled environments, including postal voting, can never provide the same protection for these principles as paper voting from controlled environments. However, it must be recognised that the use of Internet voting, and other forms of electronic voting, can help elections better achieve other basic international electoral standards, such as providing better access to voters in general and especially voters with disabilities (who may actually be able to vote unassisted, and secretly, with electronic voting).

It is important to note, in this regard, that every election system represents a country-specific attempt to balance the range of different electoral standards. It is sometimes the case that the better achievement of one standard can only be achieved at the expense of others, secrecy and transparency being a good example. Each country and election administration body will need to find the most appropriate balance of these standards given the country’s electoral, political, social and legal environment.

Oppsummering av rapport 7

Denne rapporten omhandler et av syv temaer som er vurdert på oppdrag av Kommunal - ogRegionaldepartementet i forbindelse med forsøk med elektronisk stemmegivning. Hensikten er blant annet å vurdere om innføring av internettstemmegivning vil være egnet for framtidige norske valg. Denne rapporten ser på hvorvidt den norske e-valgsløsningen er i tråd med internasjonale valgstandarder for elektronisk stemmegivning. Europarådets juridiske, tekniske og operasjonelle standarder for elektronisk stemmegivning står sentralt i denne gjennomgangen. Disse har blitt innlemmet i norsk valgregelverk gjennom forskriften for forsøk med elektronisk stemmegivning.

Den norske e-valgsløsningen var i tråd med 85 av Europarådets 112 anbefalinger. E-valgsløsningen var delvis i samsvar med 10 av anbefalingene, og oppfylte ikke tre av anbefalingene. Av de resterende 14 anbefalingene var det 10 som ikke var aktuelle for den norske e-valgsløsningen, og for ytterligere fire var det ikke mulig å vurdere hvorvidt disse var i samsvar med løsningen.

Det at det fantes ugyldige internettstemmer, samt måten disse ble håndtert på av systemet, var årsaken til at e-valgsløsningen ikke var i samsvar med tre av anbefalingene. Der systemet kun delvis var i samsvar med anbefalingene skyldes dette flere forhold, deriblant tilgang til nøkkelinformasjon om e-valgsløsningen, formaliserte kontrollrutiner for systemtilgang og problemer med å inkludere internettstemmer i det endelige resultatet.

I den tematiske gjennomgangen i rapporten omhandles flere temaer som ansees å ha betydning i vurderingen om det norske forsøket er i overensstemmelse med Europarådets anbefalinger. Hemmelige og frie valg er et viktig prinsipp i Europarådets anbefalinger, men e-valgsløsningen anses for å være i tråd med dette kravet på grunn av muligheten til å stemme elektronisk flere ganger, og fordi en papirstemme alltid overstyrer en elektronisk stemme. Forekomsten av ugyldige stemmer var en viktig årsak til at e-valgsløsningen ikke er i tråd med flere av anbefalingene, men bør settes i en sammenheng. Det var kun 10 ugyldige og for sent innkomne internettstemmer fordelt på flere valgdistrikter, og disse påvirket heller ikke valgresultatet. En løsning er nå implementert for at denne typen ugyldige stemmesedler ikke skal kunne oppstå i fremtiden. Mekanismene for ende-til-ende-verifisering i e-valgløsningen gjorde at systemet oppfylte samtlige av anbefalingene knyttet til kontroll av systemet.

Det norske e-valgsystemet ble også vurdert mot andre nye standarder på e-valgsområdet. Stort sett ble systemet funnet å være i samsvar med disse standardene. Forholdene som førte tilmanglende overholdelse var stort sett de samme som førte til manglende samsvar med Europarådets anbefalinger.

Europarådets anbefalinger utgjør et meget omfattende og detaljert sett av standarder for gjennomføring av elektronisk stemmegivning. At det norske e-valgsystemet overholder 85 av 102 relevante anbefalinger, og at det bare er tre av anbefalingene som ikke overholdes, er en betydelig prestasjon sett i lys av hvor krevende Europarådets anbefalinger er. Mange av problemene som er identifisert i denne rapporten vil det være relativt enkelt å rette på ved eventuelle fremtidige internettvalg i Norge, og man får håpe at det man det man har lært gjennom dette forsøket blir tatt med videre hvis det blir fremtidig bruk av internettstemmegivning i Norge.

2. Introduction

In 2008, the Norwegian Government took a decision, discussed and approved by the Storting (the Norwegian Parliament), to trial the use of Internet voting for Norwegian elections. It was decided that this trial would take place during the local government elections held on September 11-12, 2011. Ten of Norway's 429 municipalities were selected by the Ministry of Local Government and Regional Development (hereafter, "the Ministry") to pilot the use of Internet voting during these elections. Internet voting was available in these municipalities during the advance voting period, from August 10 – September 9.

The primary objectives behind the Internet voting project were to provide better accessibility to voters, to ensure rapid implementation of elections and the efficient use of resources in municipalities, as well as facilitating direct democracy. The Internet voting solution, provided by ErgoGroup and Scytl, was used in pre-trials for youth council elections and local referenda in all of the pilot municipalities from autumn 2010 through spring 2011.

The Ministry, which has responsibility for the oversight of elections throughout Norway, decided to conduct an independent assessment of the Internet voting pilot, and issued a request for proposals for a "Research and Evaluation of the E-vote 2011-Project" covering seven areas of assessment. One of the assessment areas related to compliance with international standards:

> *"The customer would like to receive an analysis of the extent to which the e-voting trials is in compliance with international standards, hereby the Council of Europe Recommendation on legal, operational and technical standards for e-voting, the United Nations International Covenant on Civil and Political Rights and the European Convention of Human Rights (ECHR)."*

The International Foundation for Electoral Systems (IFES) was selected to provide the Ministry with this aspect of research and evaluation of the Norwegian e-voting project. In order to conduct research and evaluation into this topic of assessment, IFES put together a team of experts with considerable experience in electronic and Internet voting:

- **Jordi Barrat I Esteve** is a constitutional law professor in Catalonia and has been involved in a wide range of electronic voting research projects covering many countries using electronic voting technologies, including Internet voting. He has been directly involved in analyzing both Spanish experiences (e.g., Madrid Participa, EU Constitution Referendum, CETIB) and other international examples of electronic voting (e.g., Venezuela, Mexico, Belgium and France).
- **Ben Goldsmith** has been involved in managing international elections and providing advice to election management bodies for nearly 15 years, including supporting the implementation of a number of election technology projects. He helped the Election Commission of Pakistan to conduct a preliminary feasibility study about the use of electronic voting machines, has written a book on conducting electronic voting and counting feasibility studies, and presented to conferences on emerging standards for electronic voting.

During the research process the team has been supported by Michel Chevallier, Electronic Voting Expert, Andrea Mandt, a Norwegian Research Assistant, and IFES' Applied Research Centre (ARC): ARC Director Rakesh Sharma, Project Manager; Hani Zainulbhai, Research Coordinator; and David Jandura, Research Coordinator.

This report represents the results of IFES' evaluation on this assessment topic. The report is divided into four main sections:

- **Assessment Methodology** – this section provides an overview of the ways in which the IFES collected data for the assessment of the Norwegian Internet voting system's compliance with international electoral standards. The framework of standards that is used for this assessment will also be discussed. The Council of Europe's recommendations on e-voting are at the core of the framework of standards, due to this being the focus requested by the Ministry and incorporated into the Norwegian legal framework for the Internet voting pilots. But they are also the most comprehensive set of standards specifically related to electronic voting. Other sources of electronic voting standards will also be introduced. In order to provide analysis of the entire set of Council of Europe recommendations, a classification system is developed so that each recommendation can be categorized as compliant, non-compliant or otherwise.
- **Assessment By Category of Compliance** – this part of the assessment will provide a quantitative assessment of compliance. The categorization system outlined in the assessment methodology section will be applied to determine how many of the 112 Council of Europe Recommendations the Norwegian Internet voting system complies with. The recommendations with which the system is found to be non-compliant will be listed. The reasons for any non-compliance will also be discussed.
- **Thematic Assessment** – the thematic assessment section covers the themes emerging from the analysis of the Norwegian Internet voting system. These include the secrecy and freedom of the vote, invalid ballots, audit mechanisms and compliance with other non-Council of Europe electronic voting standards.
- **Summary of Key Findings** – the key findings from the assessment of the Norwegian Internet voting system's compliance with international standards will be presented.

The main body of the report will present the summarized findings of the assessment into the Norwegian Internet voting system's compliance with international electoral standards. The main body of the report is based on a recommendation-by-recommendation assessment of the system's compliance with the Council of Europe recommendations, as well as other relevant emerging electronic voting standards. This detailed assessment of compliance with each of the Council of Europe Recommendations is included in the annex of this report.

Before progressing into the assessment of the performance of the Norwegian Internet voting system against the framework of international standards, it is worth making a few points about the Council of Europe Recommendations.

Reading the Council of Europe's Recommendations in 2012, eight years after it was approved by the Committee of Ministers of the Council of Europe and having in mind the compliance of an Internet voting system with its 112 standards, one is first struck by this recommendation's attempt to translate literally into the IT world the requirements of paper-based voting. It is also evident that the recommendations were written for two different kinds of electronic voting, polling station electronic voting and remote electronic voting, while also covering e-registration and the electronic registration of candidates.

The recommendations do not build on existing public international law, such as the European Convention on Human Rights and its protocols or the Venice Commission decisions, but try to cover anew the whole electoral field as if the use of IT tools would render all previous legislation obsolete.

Internet voting was in its infancy when the Council of Europe Recommendations were written. We know now that e-enabled elections are far more complex than previously thought, not only technically, but also legally and from the procedural point of view. Yet, the recommendations say little on the legal basis, trying, on the contrary, to cover every possible situation in a technically neutral way. The consequence is a sometimes vague wording that makes the enforcement of the recommendation more difficult than it should be.

Putting together different voting channels and different stages of the electoral process, because they all rely on IT for their implementation, also appears to be problematic from a legal point of view. The eclectic approach of the Council of Europe Recommendations, covering these different voting channels and stages of the electoral process, might lead to an approach of handpicking some of the recommendations to comply with. However, this would be contrary to the spirit of the recommendations, as it would for any piece of legislation. In principle is it is not appropriate to pick and choose the recommendations that are to be complied with, ignoring others. Yet the need to comply with the recommendations as a package and the varying nature and applicability of recommendations that relate to a specific technology solution pose a problem for countries attempting to implement the Council of Europe Recommendations.

Although Norway made the recommendations part of its legal framework for the municipal and county elections of September 2011 in the 10 Internet voting pilot municipalities, it decided that recommendations 25, 40, 41, 49, 52, 111 and 112[3] would not apply.

Once one begins assessing the compliance of the Norwegian Internet voting system with the remaining 104 applicable standards, it is clear that this assessment is very complex. A number of standards may appear to be overlapping or redundant. This is, for instance, the case with recommendations 32 and 33 (access to the electronic voting system); 6 and 44 (prevention of casting more than one vote); 12 and 48 (manipulative influences exercised over the voter), and standards 16 to 19 (secrecy of the vote). In this regard, the explanatory memorandum that accompanies the recommendations is vital, not only in better understanding each individual recommendation but also the subtle differences between

[3] These standards relate to certification procedures (25, 111 and 112), online voter registration (40 and 41), information about voting options (49) and voting from supervised environments (52).

recommendations. This explanatory memorandum is attached to the Council of Europe Recommendations, and is referred to extensively in this report.

In some cases, the wording of the recommendations appears too detailed. An example is recommendation 32, stating that "Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments (…)." Would it not have been simpler to write "only authorised persons shall have access…." adding that "there must be clear authorisations procedures"? This same standard goes on: "Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried outside election periods." There are obviously a lot of aspects to this single recommendation and it may be difficult to categorise it as some aspects might be compliant and others non-compliant. Another example of this can be seen in recommendation 28, mixing very different issues of reliability and security in one recommendation.

As a result, there were times when it was difficult to determine with any degree of certainty whether the Norwegian Internet voting system was in compliance with a specific recommendation or not. There were instances where this compliance was subject to interpretation of some aspects of the recommendations or the compliance of the system. Where different interpretations of a recommendation would lead to different findings in terms of compliance, the assessment erred on the side of compliance as long as the interpretation leading to a finding of compliance was as likely to be correct as the interpretation leading to a finding of non compliance.

When the details of the Norwegian Internet voting system are analysed, the difficulty in drafting general rules applicable across a wide range of electoral and technological scenarios becomes abundantly clear. Because the elections considered in this analysis are local and because Norway has a decentralised model for election administration, local electoral authorities are in charge of administering elections. For organisational reasons, however, the Norwegian Internet voting system was centrally managed. This also contributed to certain discrepancies between the principles of the recommendations and the practice of implementing the Norwegian system.

Related to this difficulty in designing standards applicable to all circumstances, recommendation 5, banning the casting of more than one vote, is a good example of how a rule too rigidly formulated can prevent compliance with the letter of the rule, while compliance is achieved with its spirit. The casting of repeat votes is the Internet voting solution chosen by Estonia and Norway to mitigate concerns about voter coercion and vote buying with remote voting. Prohibiting the casting of more than one "valid" vote (thus adding the word "valid" to the standard) would have been enough to make Norway and Estonia fully compliant without any need for more complex teleological interpretation of the recommendation. A similar situation occurs with recommendation 6, requiring that voters be prevented from casting a vote by more than one voting channel.

The recommendations are technically neutral in their wording, but not in their consequences when attempting to comply. Furthermore, the recommendations ignore the fact that sometimes it is not possible, in fact maybe it is never possible, to achieve full compliance with every standard as a package. Trade-offs between standards are sometimes necessary in electronic voting. Good examples of standards that will entail opposing, possibly contradictory, approaches to the conduct of elections include the need for secret voting vis-a-vis the need for transparency, and the need to be able to audit the function of the voting system. Likewise, stressing the accessibility of voting mechanisms may run contrary to ensuring the integrity of the process if voter registration and voter authentication are so easy that fraud will be easy to commit. The benchmark that is applied in this assessment for determining if such trade-offs fail to meet international standards will not be a perfect electoral process, for paper-based elections do not meet this standard of perfection either. Rather, the benchmark used in this assessment is paper voting in polling stations but also remotely with postal voting.

Finally, while polling station electronic voting is IT-based, but keeps some elements of the real world, remote electronic voting is fully inscribed into the cyber world. The contours and shape of this world are slowly appearing to us, the more so with each passing year. As a result, we know more about this environment today than we did back in 2004, and the nature of this environment along with the way that we interact with it has changed significantly. One example is people's willingness to reveal more of themselves in the cyber world - notably on so-called "social media" - than in the real world. Another is the expression in the cyber world of opinions that would probably not be stated in face-to-face encounters.

In this respect, assessing the compliance of an Internet voting system with the Council of Europe's recommendations raises the question that lawyers working on Internet-related issues have already raised, but have failed to answer univocally: does the cyber world require laws of its own, do we have to rewrite the existing laws to adapt them to new situations that have no equivalent in the real world, or are current laws sufficient to cover the cyber world too?

The Council of Europe Recommendations answer this in their own way. Their very existence assumes the need for a new set of standards, not so much for the cyber world as for the IT systems dealing with realisation of political rights. The truth may lie halfway between both positions, and in some ways this can be seen in the recommendation: the technical standards, recommendations 61 to 112, are more pertinent than the legal and operational ones, indicating that some issue do not change when the medium used to vote does. That IT systems used in the context of political rights need a stronger regulation and oversight than common IT systems is clear – the stakes are much higher with voting.

3. Assessment Methodology

The principle aim of this assessment is to determine the compliance of the Norwegian Internet voting system with the Council of Europe Recommendations, which Norway has adopted into its electoral legal framework through the Regulations Relating to Trial Electronic Voting issued by the Ministry. While these recommendations have done much to establish standards in the field of electronic voting, they need to be put into the context of more general international electoral standards to obtain a proper understanding of the Council of Europe Recommendations. The recommendations also make it clear that they are not intended to replace the existing framework of electoral standards but that all of the existing standards continue to apply. The first part of this section will introduce the general framework of international electoral standards that continue to apply, and can be seen as the foundation on which the recommendations are established.

Next, the section will look at what can be seen as a group of emerging standards with respect to electronic voting, and therefore relevant to Internet voting. The Council of Europe Recommendations are only one of the sources that define this group of emerging standards. It is, however, a critically important one not just because Norway has chosen to adopt it into its electoral legal framework for the Internet voting trial. Having outlined the standards that will be used in the assessment, the system of categorizing compliance with these standards will be outlined. Finally, the way in which compliance was researched and determined with the standards will be explained.

General International Electoral Standards

There are different approaches that can be taken in defining the content of international electoral standards, but in recent years opinion appears to have coalesced around the concept of international electoral standards as defined by public international law.[4]

Public international law based electoral standards are well elaborated in documents issued by the United Nations,[5] the European Commission,[6] the Organization for Security and Cooperation in Europe (OSCE)[7] and the Venice Commission.[8] The ways in which these electoral standards are categorized by the different institutions are not exactly the same but, despite this, they do illustrate a common understanding of the content of international electoral standards. Drawing directly from the wording of Article 25 of the International Covenant on Civil and Political Rights (ICCPR), the core of these international electoral standards can be defined as the following:

[4] See for example the Inter-Parliamentary Union's publication in 1994 - Goodwin-Gill, G. (1994) Free and Fair Elections: International Law and Practice, Inter-Parliamentary Union: Geneva and the updated version - Goodwin-Gill, G. (2006) Free and Fair Elections: New Expanded Edition, Inter-Parliamentary Union: Geneva.

[5] Centre for Human Rights (1994) Professional Training Series No.2: Human Rights and Elections – A Handbook on the Legal Technical and Human Rights Aspects of Elections, United Nations: New York and Geneva.

[6] European Commission (2007) Compendium of International Electoral Standards: Second Edition, European Commission: Brussels.

[7] OSCE (2007) Election Observation Handbook: Fifth Edition, OSCE Office for Democratic Institutions and Human Rights: Warsaw.

[8] European Commission for Democracy Through Law (Venice Commission) (2002) Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report, Adopted by the Venice Commission at its 52nd session (Venice, 18-19 October 2002), CDL-AD(2002) 23 rev.

- **Fair Elections (without any distinctions)** – Elections should be conducted so as to ensure equal conditions for participation in the electoral process for all eligible candidates and voters, irrespective of gender, religion, ethnicity, political affiliation, language, literacy or disability.
- **Genuine Elections** – Elections must be held for institutions that have authority, must be conducted in a credible manner, must present voters with real choices between candidates for election, with the results of elections representing the will of the people.
- **Periodic Elections** – Elections must be held frequently enough to ensure that governmental authority continues to reflect the will of the people and that there is regular opportunity for the voters to change government.
- **Universal Suffrage** – Legal and operational limitations on access to candidacy or the right to vote must be minimized and must not be discriminatory in nature, except where such limitations are reasonable or necessary.9
- **Equal Suffrage** – Voters should each be provided the same number of votes in each election being conducted and electoral districts should be reasonably equal in size so that each vote cast has a similar weight.
- **Secret Ballot** – In order that voters are able to freely express their electoral preferences in the absence of intimidation, the ballot should be completed in private and it must not be possible to link a voter to a voting preference.
- **Free Elections** – The electoral environment must be such that information on electoral contestants can be made available to voters, informed discussion about electoral options can take place, and voters are able to make electoral choices without intimidation.

These political/electoral rights and standards do not operate in a vacuum. In fact, political rights work in parallel with other human rights and a healthy electoral environment relies on the realization of these broader human rights. Human rights relevant to the conduct of elections include the rights to freedom of expression,[10] freedom of information,[11] freedom of assembly,[12] freedom of association,[13] freedom of movement,[14] to non-discrimination,[15] and to self-determination.[16] Transparency is also an essential component for a credible electoral process. The requirement for transparency is derived in part from some of the human and political rights standards outlined above.[17] It is also based on other international standards, such as anti-corruption standards, which require public affairs to be conducted in a transparent manner.[18]

[9] For example, on the basis of age, nationality, residence, mental incapacity or criminal conviction.
[10] Article 19 of the ICCPR.
[11] Article 19 of the ICCPR.
[12] Article 21 of the ICCPR.
[13] Article 22 of the ICCPR.
[14] Article 12 of the ICCPR.
[15] Article 2 of the ICCPR.
[16] Article 1 of the ICCPR.
[17] For example, the right to information, that elections are credible (genuine) and that elections are conducted in a fair manner.
[18] See the United Nations Convention Against Corruption, especially articles 5, 7, 9, 10 and 13.

Electronic Voting Standards

The international electoral standards outlined above are equally relevant for the use of technologies to assist the processes of voting and counting, as clearly stated in the Council of Europe's 2004 Recommendation on Legal, Operational and Technical Standards for E-voting:

> "e-voting shall respect all the principles of democratic elections and referendums."[19]

Increasingly so, the use of new technologies for voting and counting are fundamentally changing the way the components of the electoral process are conducted. As a result, the use of technologies for voting and counting is also challenging this body of international electoral standards.

Some of these standards are no longer adequate to deal with electronic voting and counting technologies. Other technology-related operations are not covered at all by the existing set of standards. For example, it is clear that the use of electronic voting and counting technologies will have little or no impact on the right to freedom of movement or freedom of association. However, other standards such as the secrecy of the vote or the fairness of the electoral process may be significantly impacted by the use of such technologies.

As a result, there have been initiatives in recent years to evolve these international electoral standards in order to cope with the challenges of using voting and counting technologies.[20] The Council of Europe Recommendations did much to set the agenda for this adaption of existing standards for electronic voting and counting technologies. However, the limitations of the recommendations must also be recognized. The Council of Europe Recommendations are just that, only recommendations and as such are not binding on Council of Europe member states. Furthermore, in principle they are only applicable to member states of the Council of Europe, as this is the organization that adopted them. In reality, their authority is much wider than this implies, but they do not enjoy as much global authority as similar recommendations from a United Nations body might.

The Council of Europe has followed up this recommendation with the publication of an E-voting Handbook[21] presenting guidelines for implementing e-enabled elections and guidelines on certification and transparency for e-enabled elections[22]. In 2006, the European Commission also published a report titled *Methodological Guide to Electoral Assistance,* which covers support for the introduction of

[19] Council of Europe (2004), p. 7.

[20] It is worth noting that a number of national standards have also been developed to guide the use of electronic voting and counting technologies, such as the U.S. Election Assistance Commission's (2005) Voluntary Voting System Guidelines (http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx [last accessed May 9, 2012]. However, these standards are only national standards and do not entail international obligations on other states. The sources referenced in the discussion on emerging standards all relate to international organization's commitments or guidance to their members states, or international NGOs which are influential in the area of establishing electoral standards.

[21] Caarls, S. (2010) E-voting Handbook: Key steps in the implementation of e-enabled elections, Council of Europe Publishing: Strasbourg.

[22] Council of Europe (2011a) Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribed requirements and standards and Council of Europe (2011b) Guidelines transparency of e-enabled elections both drafted by the Council of Europe's Directorate of Democratic Institutions, "Good Governance in the Information Society" Project.

election technologies, including electronic voting and counting technologies and the standards that might be applicable in their use.[23]

The OSCE's Office for Democratic Institutions and Human Rights,[24] the Organization of American States,[25] the Carter Center[26] and the National Democratic Institute for International Affairs (NDI)[27] have also approached the issue of standards for electronic voting and counting technologies from the perspective of observing elections in which these technologies are used. Elections using electronic voting and counting technologies are inherently less transparent than paper based elections, as electronic events take place, which are not possible to observe with the naked eye.[28] This makes it more difficult to determine the credibility of the electoral process and whether any fraud or mistakes have taken place in their conduct. In fact, leading experts in the field of e-voting argue that the lack of transparency with electronic voting and counting systems is the greatest challenge facing the implementation of such technologies.[29]

As a result, the use of electronic voting and counting technologies has presented particular problems for organizations attempting to observe and evaluate the conduct of elections. Publications by these leading election observation organizations are consequently highly relevant to the debate on emerging standards for the use of electronic voting and counting technologies.

In analyzing these important publications, it is clear that some trends are emerging in the recommendations being made by all of these organizations about the conduct of elections using electronic voting and counting technologies. Common themes can be seen in the following areas:

- **Transparency** – Transparency is related to many of the more specific emerging standards below, but is important enough to merit discussion separately. Transparency is a general electoral standard, but one which is particularly challenged by the use of electronic voting and counting technologies. Special focus needs to be placed on the realization of transparency while using these technologies. This means that as much of the operation of the process using electronic voting and counting technologies is transparent or observable (Council of Europe 2004: recommendations 23 and 56) and the election management body is required to take active

[23] European Commission (2006) Methodological Guide to Electoral Assistance, see http://ec.europa.eu/europeaid/multimedia/publications/documents/thematic/ec_methodological_guide_on_electoral_assistance_en.pdf [last accessed May 9, 2012].

[24] OSCE (2005) Challenges of Election Technologies and Procedures: Final Report, Supplementary Human Dimension Meeting, PC.SHDM.GAL/5/05; OSCE (2008) OSCE/ODIHR Discussion Paper in Preparation of Guidelines for the Observation of Electronic Elections, ODIHR.GAL/73/08.

[25] OAS (2010) Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions, General Secretariat of the Organization of American States (GS/OAS), see www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf [last accessed May 9, 2012].

[26] Carter Center (2007) Developing a Methodology for Observing Electronic Voting, see http://www.cartercenter.org/documents/elec_voting_oct11_07.pdf [last accessed May 9, 2012].

[27] Pran, V. and Merloe, P. (2007) Monitoring Electronic Technologies in Electoral Processes: An NDI Guide for Political Parties and Civic Organizations, National Democratic Institute for International Affairs, see http://www.ndi.org/files/2267_elections_manuals_monitoringtech-preface_0.pdf [last accessed May 9, 2012].

[28] OSCE (2008), p. 2.

[29] Krimmer, R. (Ed.) (2006) Electronic Voting 2006: Overview of Proceedings of 2nd International Workshop, co-organised by the Council of Europe, ESF-TED, IFIP WG8.6 and E-Voting.CC.

steps to promote this transparency (Carter Center 2007: 6). Political actors must have access to the electronic voting process, and manuals or guidelines should exist for the implementation of the technology (OAS 2010: 28), as well as documents related to certification, testing and security (OSCE 2008: 17). However, access should be provided for observers in a manner that does not obstruct the electoral process (Pran and Merloe 2007: 62; OSCE 2008: 17).

- **Public Confidence** – Closely related to, and relying heavily upon, transparency is the requirement that voters understand and have confidence in the electronic voting or counting technology being used (Council of Europe 2004: recommendation 20). Public confidence requires that stakeholders are involved in the introduction of electronic voting and counting technologies (The Carter Center 2007: 8), are provided information so they understand the technologies being used (Council of Europe 2004: recommendation 21; OAS 2010: 20), simulations of the systems take place (Pran and Merloe 2007: 59) and voters are informed well in advance about the introduction and what is required to participate (Council of Europe 2004: recommendation 38; OSCE 2008: 14).
- **Usability** – Electronic voting and counting technologies must be easy to understand and use for as many voters as possible (Council of Europe 2004: recommendation 1; OSCE 2008: 13; OAS 2010: 20). Users (voters) should be involved in the design of electronic voting and counting technologies (Council of Europe 2004: recommendation 62) and in public testing (OSCE 2008: 14). Furthermore, these electronic voting and counting technologies must try to maximize the accessibility of the voting system for persons with disabilities (Council of Europe 2004: recommendation 3; OSCE 2008: 13; OAS 2010: 20; Pran and Merloe 2007: 76) and afford voters the possibility to stop and cancel their vote before confirmation of their choice (Council of Europe 2004: recommendation 14; OSCE 2008: 13-14).
- **System Certification** – Electronic voting and counting technologies must be certified by an independent body before use and periodically thereafter. This ensures the system continues to meet the requirements of the electoral jurisdiction as well as the technical specifications for the system. Furthermore, the certification process should be conducted in a transparent manner providing electoral stakeholders access to information on the process (Council of Europe 2004: recommendations 24-5; OSCE 2008: 22; Pran and Merloe 2007: 65-5 and 72; The Carter Center 2007: 7).
- **System Testing** – Any electronic voting or counting system should be subjected to a comprehensive range of testing30 before it is approved for use by an EMB (Council of Europe 2004: recommendation 73; OSCE 2008: 22; OAS 2010: 20; Carter Center 2007: 7). This testing should take place transparently and with access for political actors (OAS 2010: 28; Pran and Merloe 2007: 67).
- **System Security** – The opportunities for systematic manipulation of the results mean that system security needs to be taken extremely seriously. Security measures need to be taken to ensure that data cannot be lost in the event of breakdown; only authorized voters can use an electronic voting or counting system; system configuration and results generated can be authenticated; and only authorized persons are allowed to access electronic voting, counting

[30] A full range of tests are described later in this guide.

and results management functionality (Council of Europe 2004: recommendations 32-2 and 77-99; Carter Center 2007: 7-8; OAS 2010: 19-20). Attempts to hack into electronic voting and counting machines or the election management system into which results are received, need to be detected, reported and protected against (OSCE 2008: 12).

- **Audit and Recount** – Electronic voting and counting technologies must be auditable (Council of Europe 2004: recommendation 59; OSCE 2008: 7; OAS 2010: 20) so it is possible to determine whether they operated correctly. It must be possible to use an electronic voting or counting system to conduct a recount (Council of Europe 2004: recommendation 26; OSCE 2008: 7). Such recounts must involve meaningful manual recounts of ballots cast electronically (OSCE 2008: 19) and not merely a repetition of the electronic result already provided (Pran and Merloe 2007: 78).
- **Voter Verified Audit Trail** – In addition to the above requirements for auditability in any electronic voting or counting system, it must also be possible to assure voters that their votes are being counted as cast (Carter Center 2007: 7) while also ensuring that the secrecy of the vote is not compromised (OSCE 2008: 18). This requires that electronic voting systems create an audit trail which is verifiable. 31 It should provide the voter with a token/code with which to perform the verification externally and not show the way in which the vote was cast. The most common solution to this for in-person electronic voting machines is through the production of a VVPAT, and this solution is emerging as a standard in this regard (OSCE 2008: 8 and 23; Pran and Merloe 2007: 72 and 75).32 It should be noted that this VVPAT solution is not appropriate for remote electronic voting, which uses electronic voting machines (e.g. Internet voting, text message voting etc.) as there would be nothing to stop a voter from removing the paper record of the vote, making vote buying and voter coercion possible.33
- **Mandatory Audit of Results** – The existence of an audit trail for electronic voting and counting systems achieve little if it is not used to verify that the electronic results and the audit trail deliver the same result. Doing so also serves to build public confidence in the operation of the electronic voting or counting technologies. A mandatory audit of the results generated by electronic voting or counting technologies should be required by law and take place for a statistically significant random sample of ballots (Council of Europe 2010: 12; OSCE 2008: 18; Pran and Merloe 2007: 64 and 79).
- **Secrecy of the Ballot** – The secrecy requirement is not a new standard but it is one that is made more difficult by electronic voting and counting technologies. This is especially the case for remote electronic voting systems where voters have to first identify themselves and vote

[31] Electronic counting machines have a natural voter verified audit trail in the paper ballot which was completed by the voter.

[32] Although it must be said that a voter verified paper audit trail is not the only way in which this can be achieved. In Belgium for example, the vote is stored on a magnetic card which can be verified on other voting machines before being placed in the ballot box. This Belgian system is creates a voter verifiable audit trail without the use of paper. This is not to say that the Belgian system is better or worse than the VVPAT solution, merely to indicate that there may be other non-paper methods of achieving the standard.

[33] In fact, one of the greatest challenges facing remote e-voting remains the establishment of a vote verification mechanism for remote voters in an easily understandable way, which does not also provide a way to violate the secrecy of the vote. There are some solutions, which provide codes to voters that can be checked to see that the vote is included in the count, but nothing that can prove the value of the verified vote without relying on complicated mathematical proofs, which the average voter would have to trust just as much as the operation of an electronic voting machine.

electronically using the same interface. The use of electronic voting and counting technologies must comply with the need for secrecy of the ballot (Council of Europe 2004: recommendations 16-19; OSCE 2008: 11-12; Carter Center 2007: 9; OAS 2010: 19).

- **Incremental Implementation** – Whenever electronic voting and counting technologies are introduced they should be done so in an incremental manner and should start with less important elections. This will allow public understanding and trust to develop in the new system, and provide time to deal with problems and resistance (OSCE 2008: 23; Carter Center 2007: 2).

These standards are still in their nascent stages. It is quite possible that their content may change as they continue their evolution and emerge as internationally recognized standards. However, at this point in time they represent the closest that we have to an international consensus on standards for electronic voting.

The Norwegian Internet voting system will also be assessed against these emerging standards to see if it complies with them. It should be noted that some of the standards identified above are part of the Council of Europe Recommendations and therefore compliance with these aspects of the standards is dealt with when the recommendations are assessed. It is also worth noting that while it would be preferable if the Norwegian Internet voting is in compliance with non-Council of Europe emerging electronic voting standards, there is not the same legal obligation for the system to do so. These other emerging standards have not been incorporated into the legal electoral framework in the same way that the majority of the Council of Europe Recommendations have through the Regulations Relating to Trial Electronic Voting.

Additionally, it is worth recognizing that that there are other groups of standards that are relevant to the implementation of electronic voting projects. Some countries have developed national standards for the implementation of electronic voting. The U.S. is one such example, with their *Voluntary Voting System Guidelines* (VVSG) developed by the Election Assistance Committee.[34] While Norway has not developed such national standards for electronic voting, there are other international standards relevant for electronic voting but not directed at electronic voting. These include various ISO standards and Common Criteria standards.

This assessment will not attempt to assess the compliance of these more technical and non-election related standards, but will focus on the Council of Europe Recommendations primarily and also assess the compliance with other emerging electronic voting standards.

Categorization System

In assessing whether the Norwegian Internet voting system is in compliance with the Council of Europe Recommendations, it was necessary to develop a system of categorization so that the overall compliance could be assessed quantitatively. The development of this system of categorization for

[34] See http://www.eac.gov/vvsg/ [last accessed April 30, 2012].

compliance was necessary for obtaining a quick overview of the compliance of the Norwegian Internet voting system without reading the assessment of each of the 112 recommendations.

Compliance with the recommendations was categorized in the following way:

- **Fully Compliant** – the Norwegian Internet voting system was assessed to meet all the requirements of the recommendation as far as could be determined with the information obtained.
- **Partially Compliant** – the Norwegian Internet voting system was found to meet some of the requirements of the recommendation but also failed to meet some important aspects of the recommendation.
- **Non-compliant** – the Norwegian Internet voting system was found to not meet aspects of the recommendation, which were seen as fundamental to the purpose of the recommendation.
- **Not Possible to Determine** – there was either insufficient information to determine whether the Norwegian Internet voting system was in compliance with the recommendation or the facts could not conclusively prove whether compliance was achieved or not.
- **Not Applicable** – the recommendation was not applicable to the Norwegian Internet voting system. This was because the specific recommendation was excluded from being applicable by the Regulations Related to Trial Electronic Voting or the recommendation was related to aspects of electronically enabled elections, which were not part of the Norwegian Internet voting system.

It is important to note the disadvantages of categorizing each recommendation. It would be easy to only consider the categorizations and not the reasoning behind the assessment of each recommendation – which is included in Annex 1 of this report. The discussion of the compliance of each recommendation often reveals important nuances and principles which are obscured by the simple, yet still useful, categorization of the recommendation's compliance.

For example, some recommendations are categorized as compliant but only because it is possible to reasonably interpret the requirement of the recommendation in a number of ways and some of these interpretations would lead to a finding of compliance (while other interpretations would not). In such cases we have erred on the side of compliance. In other cases the finding of compliance has been based on stated assumptions, which may not be accurate. Even when the Norwegian Internet voting system is categorized as being compliant with such recommendations, this obscures the potential for non-compliance with other interpretations of the recommendation or if the assumptions are incorrect. Likewise, in some cases the Norwegian Internet voting system was found to be non-compliant with a recommendation due to a problem in the system (for example the submission of invalid ballots), but a solution has subsequently been found that should ensure that this does not happen in the future.

Therefore, while the categorization system is important for obtaining a rough overview of the compliance of the Norwegian Internet voting system, a full understanding of IFES' assessment of the system's compliance can only be obtained by a full reading of the assessment.

It is also important to note that the categorization system will only be applied to the Council of Europe Recommendations. These recommendations are clearly articulated in the 112 recommendations, as well as being supplemented by the explanatory memorandum, so that a clear understanding of the recommendations is normally easy to determine. The other emerging standards for electronic voting that were identified previously are much less clearly defined and elaborated. Therefore, the Norwegian Internet voting system's compliance with these emerging standards will be dealt with in the qualitative assessment section of this report.

Data Collection

In order to conduct this assessment the IFES team spent a long time reviewing the documents made available by the Ministry about the Norwegian Internet voting system. Many of these documents were publicly available on the Ministry's website[35], but the Ministry also made many other internal documents available to IFES for the purpose of this assessment.

In addition, the IFES team attended a number of events that helped to increase their knowledge of the Norwegian Internet voting system. On September 11, 2011, the Ministry held the Norwegian E-Vote 2011 Conference. The Ministry invited both Norwegian and international speakers to give presentations at the conference. The audience included among others electoral observers, representatives from electoral authorities in other countries and researchers in the field of electronic voting. The IFES team also attended the Decryption and Counting Ceremony for Internet votes on September 12, 2011. Both events proved invaluable in obtaining a better understanding of the Norwegian Internet voting system.

As the IFES team began to use this information to start assessing the compliance of the Norwegian Internet voting system with the Council of Europe Recommendations, it became clear that in many cases additional information was required. This was largely due to the fact that many of the Council of Europe Recommendations are very specific or very technical in nature, and required much more detailed information to assess them. As a result, IFES submitted a series of questions to the Ministry to obtain more detailed and technical information about the system and the management of the system, as well as the Ministry's opinions in some cases as to whether and how they had complied with specific recommendations.

The Ministry was forthcoming with prompt and detailed responses to these questions, and this information proved vital in conducting this assessment. The Ministry also took the opportunity to provide extensive comments to early drafts of this report and the other assessment reports produced by IFES. The discussion ensuing from these comments was also invaluable in obtaining a clearer understanding of some of the more technical aspects of the Norwegian Internet voting system and in exchanging opinions relevant to the compliance of the system with the Council of Europe Recommendations.

On the basis of this information gathering and the categorisation system developed, the IFES team started to assess the compliance of the Norwegian Internet voting system with each of the

[35] See http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658 [last accessed May 1, 2012].

recommendations. The recommendations were divided up between the team members for the drafting of the initial analysis of the compliance of the system with each recommendation. These initial assessments were reviewed by at least one other team member, and the extensive comments that this process resulted in were then discussed within the team again in order to clarify and finalise the assessment of each recommendation.

Once all of the individual assessments were conducted, the team attempted to take a holistic view of the themes that emerged from the analysis. This holistic assessment also ensured that a consistent approach was taken to the same issue when dealt with by multiple recommendations and reviewed again all of the recommendations where the Norwegian Internet voting system was found to be non-compliant. Only when this process was conducted were the thematic sections of the report written.

4. Assessment by Category of Compliance

As outlined in the sections above, there are five categories used in determining whether the Norwegian Internet voting system is compliant or not with the Council of Europe Recommendations. The categories allocated in this assessment to the 112 Council of Europe Recommendations are summarised in Figure 1 below:

Figure 1 – Overall Compliance of the Norwegian Internet Voting System

Assessment Finding	Number of Recommendations
Fully Compliant	85
Partially Compliant	10
Non-Compliant	3
Not Possible to Determine	4
Not Applicable	10
Total	**112**

The Norwegian Internet voting system was found to be compliant with the vast majority of the Council of Europe Recommendations, 85 out of 112. A further 14 were either not applicable or were not possible to determine, meaning that for only 13 of the recommendations was the Norwegian Internet voting system determined as not being compliant in some way.

Non-Compliance

The three recommendations, which the Norwegian Internet voting system was found to be non-compliant with are listed in Figure 2.

Figure 2 – Recommendations for which the Norwegian Internet Voting System was Found to be Non-compliant

No.	Recommendation	Assessment
14	The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.	Non-Compliant
58	In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.	Non-Compliant
91	The fact that a vote has been cast within the prescribed time limits shall be ascertainable.	Non-Compliant

The reasons why the Norwegian Internet voting system was found to be non-compliant in these cases related to the fact that it was possible for invalid ballots to be accepted by the system and for ballots to be submitted after the end of the 30 minute voting session limit. In both cases, the voter received no indication that an invalid vote had been cast, which would not be included in the count, and invalid ballots were not recorded as invalid on the system but discovered in a post-election audit.

These issues are of significant importance to the integrity of the Norwegian Internet voting system, but will be discussed in greater detail in the Thematic Assessment section below.

Partial Compliance

The 10 recommendations which the Norwegian Internet voting system was found to be partially compliant with are listed in Figure 3.

Figure 3 – Recommendations for which the Norwegian Internet Voting System was Found to be Partially Compliant

No.	Recommendation	Assessment
8	Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.	Partially Compliant
21	Information on the functioning of an e-voting system shall be made publicly available.	Partially Compliant
22	Voters shall be provided with an opportunity to practice any new method of e-voting before, and separately from, the moment of casting an electronic vote.	Partially Compliant
24	The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.	Partially Compliant
32	Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.	Partially Compliant
33	While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and any election observers.	Partially Compliant
69	The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.	Partially Compliant
73	Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with technical specifications. The findings shall be submitted to the competent electoral authorities.	Partially Compliant
74	All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be notified.	Partially Compliant
108	The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.	Partially Compliant

The reasons why the Norwegian Internet voting system was found to be partially compliant in these cases were due to a number of factors. Amongst these partially compliant assessments, access to information was a recurring theme, issues including; the late availability of the final version of the source code; the unavailability of the authentication portal components for review by the Ministry; the need for a simplified system of documentation; observer access to system interventions; public procedures for checking the status of software; and open access to audit logs.

The Ministry actually made significant efforts to provide access to information about the Norwegian Internet voting system. However, the need for transparency in order to generate trust and confidence in the system is considerably greater with Internet voting. These partially compliant recommendations certainly identify areas in which the ministry should attempt to improve transparency mechanisms and access to information in the future, but the efforts it has made in this regard should not go unrecognised.

Control procedures were another theme amongst these cases of partial compliance. Key issues were: the need for coherent and comprehensive procedures for the management of the Internet voting system being required; and to better include the municipal and county electoral committees (as the bodies legally responsible for the local elections) in the management of the Internet voting system.

The Ministry insists that it did use system management and access procedures (such as system access by teams of two people) which complied with the Council of Europe Recommendations. However, the fact that these system management procedures were split across many different documents makes it difficult to check that coherent and comprehensive procedures were in place for access to the various components of the Internet voting system. This partial compliance should be an easy issue to resolve for future use of the Norwegian Internet voting system.

Additionally, the failure to initially include the Internet votes in one county’s election results, the failure to provide special measures for elderly voters to try out the Internet voting system before the election and the requirement for an external check/certification of the new Internet voting system also led to findings of partial compliance.

Difficulties in including the Internet votes cast in one pilot municipality in the county election results was largely a result of problems in the interface between the new election management system that was being trialled in the Internet voting pilot municipalities and the existing election management system in use at the county level. While it represents a partial non-compliance with recommendation 8, it is not expected to be an issue in any future elections. The ministry has indicated that in future elections, most municipalities and counties will be using the new election management system thereby addressing this problem.

The failure to subject the Norwegian Internet voting system to an external check/verification, which led to a finding of partial compliance with recommendation 73, is interesting because of the general approach taken towards the issue of certification of the system. As this was a pilot for the use of Internet voting in Norway, and perhaps in recognition that independent certification of electronic voting systems can take time and be costly, the Ministry excluded a number of other recommendations related to certification from the Regulations Relating to Trial Electronic Voting.[36] However, if Internet voting were to be implemented nationally, the Ministry indicated that an independent certification process would be conducted.

Furthermore, the text of recommendation 73 only mentions the need to check and approve the equipment, with reports submitted to the election management body. There is no indication in the text itself that this recommendation requires an external certification process. As such, the Ministry may not have seen this as a recommendation that needed to be excluded, as other recommendations relating to certification were from the Regulations Relating to Trial Electronic Voting, because of its approach to certification in the pilot process.

However, the explanatory memorandum to this recommendation states that: “A clear distinction should be made between checking done on a regular basis after each election or referendum, and the checking done whenever the system is modified in any respect. In the first case, employees of the entity running the election or referendum system might do the checking. However in the second case an external body should do the checking, as the check is closer to being a certification procedure.”

The second kind of checking referenced above is most appropriate in the Norwegian case as the Internet voting system had never been used before in a binding political election. However, this external check, similar to a certification process, was not conducted and as a result the Norwegian Internet voting system was found to be in partial compliance with this recommendation – having met other aspects of the recommendation.

It is assumed that the inclusion of this recommendation in the Regulations Relating to Trial Electronic Voting, or the components related to the need to certification-like procedures, was an oversight by the Ministry, given its general approach to certification of the system in the pilot process.

[36] See recommendations 25 and 111, which were excluded.

Not Possible To Determine

Figure 4 lists the four recommendations for which it was not possible to determine if the Norwegian Internet voting system was in compliance.

Figure 4 – Recommendations for which it was not Possible to Determine if the Norwegian Internet Voting System was in Compliance

No.	Recommendation	Assessment
34	The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.[37]	Not Possible to Determine
60	The conclusions drawn from the audit process shall be applied in future elections and referendums.	Not Possible to Determine
92	Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.	Not Possible to Determine
95	The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.	Not Possible to Determine

For three of the four recommendations falling into this category, the inability to determine compliance was due to the possibility for the system to generate and accept invalid ballots. This issue is dealt with in detail in the thematic section of the report. Additionally, one recommendation relates to the conclusions and consequences of the audit process. As this is still ongoing it is not possible to determine compliance with the recommendation, but it is to be hoped that findings and recommendations from the audit process will be applied to any future use of the Norwegian Internet voting system.

[37] This is an example of a multifaceted recommendation and it is only the initial component of this recommendation that was not possible to determine. The Norwegian Internet voting system was found to be compliant with the other components of this recommendation.

Not Applicable

Figure 5 lists the 10 recommendations which are not applicable to the Norwegian Internet voting system.

Figure 5 – Recommendations which are Not Applicable to the Norwegian Internet Voting System

No.	Recommendation	Assessment
25	Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.	Not Applicable
40	The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.	Not Applicable
41	In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.	Not Applicable
42	The possibility of introducing online candidate nomination may be considered.	Not Applicable
49	If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.	Not Applicable
52	In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.	Not Applicable
87	The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.	Not Applicable
88	The fact that voter registration has happened within the prescribed time limits shall be ascertainable.	Not Applicable
111	Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation.	Not Applicable
112	In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Co-operation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.	Not Applicable

Of the 10 recommendations which are found to be not applicable, seven of them are specifically excluded from the Norwegian electoral legal framework by the Regulations Relating to Trial Electronic Voting (recommendations 25, 40, 41, 49, 52, 111 and 112). The remaining three relate to online candidate nomination and voter registration, neither of which is part of the Norwegian Internet voting system being trialled.

5. Thematic Assessment

The thematic assessment section of the report covers a number of issues that were seen as important in the assessment of the Norwegian Internet voting system's compliance with the Council of Europe Recommendations. While some of these key issues arise out of areas in which the Norwegian Internet voting system was found to be non-compliant or partially compliant with the recommendations, this is not always the case.

Four issues are covered: the secrecy and freedom of the vote, invalid ballots, audit and compliance with emerging electronic voting standards.

Secrecy and Freedom of the Vote

As discussed earlier, the secrecy of the vote is one of the fundamental principles with which elections are expected to comply. The source of this standard can be traced back to the 1966 International Covenant on Civil and Political Rights (ICCPR), which states that elections, "shall be held by secret ballot, guaranteeing the free expression of the will of the electors" [art. 25 (b)]. This principle has been repeated in many subsequent international treaties, for example the First Protocol of the European Convention on Human Rights foresees, "free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature."[38]

As evident in these treaties, the principle of the secret vote is closely linked to the need to guarantee the free expression of the will of the voter. In fact the secret ballot, sometimes called the Australian Ballot due to its origin, was introduced in order to end the coercion that voters were being subjected to during public voting procedures. It also ensures that those wishing to buy the votes of electors would never know for sure whether the voter had voted as they may have been paid to vote.

In fact, the secrecy of the vote requires two components. Firstly, it requires that voters are able to cast their votes in private, unobserved by anyone, ensuring that only the voter will know how they have cast their ballots. Secondly, secrecy requires that electoral procedures are such that the ballot and personal identification data about the voter cannot be later reconstructed to break the anonymity of the vote.

As shall be discussed in this section, both aspects of secrecy – privacy and anonymity - are challenged by the use of Internet voting. Nevertheless, it is the opinion of this assessment that the Norwegian Internet voting system has found ways of addressing these concerns in ways which meet the Council of Europe Recommendations.

Legal Framework Related to Secrecy and Freedom of the Vote

Given the importance of the principle of secrecy to the conduct of elections it is not surprising to find that this principle is reflected in the Council of Europe Recommendations in a number of places. The fourth section (recommendations 16-19) of the first chapter of the Council of Europe's Recommendations is entirely devoted to the principle of secrecy. The four recommendations in this

[38] Article 3 of the First Protocol to the European Convention on Human Rights.

section address the following issues: 16 (nothing endangers the secrecy of the vote), 17 (anonymity of the votes cast), 18 (secrecy when a small number of ballots are cast) and 19 (secrecy during the electronic processing of the ballots).

The third section of the first chapter (recommendations 9-15) concern free suffrage, and as such some of these recommendations are relevant to the discussion of secrecy. Recommendations in this section cover the following topics: 9 (free expression of voter opinion), 10 (prevention of voting precipitately), 11 (alteration of votes before casting and not recorded), 12 (no manipulative influences), 13 (blank votes), 14 (inform voter when vote has been successfully cast), and 15 (no changes once the ballot is cast). Recommendations 9, 11 and 12 are clearly related to the secrecy of the vote.

Finally, within the technical and operational standards: recommendations number 34 and 35 require the confidentiality of the votes and separation of voter identification data; recommendation 51 prohibits voting receipts with remote voting systems; and recommendation 93 with residual information, which could be used to determine the value of the vote cast.

It is clear from the many places in which secrecy is included in the Council of Europe Recommendations that the freedom and secrecy of the vote are seen as vitally important principles in the use of electronic voting.

Apart from the obligations assumed by Norway by its adoption of the Council of Europe Recommendations, the Norwegian electoral legal framework includes other guarantees related to the secrecy of the vote. The Representation of the People Act (2002) (hereafter referred to as the Election Law) includes clear provisions related to secrecy when it states that, “it is not permitted for unauthorised persons to keep check of who comes to vote or to undertake investigations of voters or any similar questioning of the voters.”[39] It also expects that, “the elector shall in a secluded room and unobserved fold the ballot paper together in such manner that it is not possible to see for which electoral list the elector is voting.”[40]

Key Issues with Secrecy and Internet Voting

The principles of secrecy and freedom of the vote are challenged in many different ways by the use of Internet voting systems. The Norwegian Internet voting system raises the following concerns related to the secrecy and freedom of the vote.[41]

- **Secrecy at the point of voting** – Norwegian Internet voting takes place in uncontrolled environments and therefore there is no supervision by electoral authorities of that environment. While the polling committee can ensure that voters are alone when they mark their ballot in the polling station, there is no such guarantee for Internet voters. Voters may not be alone when casting an Internet ballot, and those present may coerce the voter to cast the ballot in a manner which does not express the will of the voter.

[39] Section 9-4 (1).

[40] Section 9-5 (3).

[41] Many of these concerns are also relevant for other Internet voting solutions, although some are specific to the Norwegian Internet voting system.

- **Record of the voting session on the remote device** – computers used for Internet voting keep records of the activities conducted on the computer in many different ways. This makes it possible that data recorded on the computer can be used to determine how a voter has voted, violating the secrecy of the vote.
- **Generation of return codes for polling cards** – each voter receives a polling card with codes for all of the party lists on the ballot. The Ministry was responsible for generating the polling cards for the Internet voting municipalities. The process of printing these polling cards requires that information on each voter, and the return codes allocated to each party for that voter, are known. If this link is known to the Ministry for the printing of the polling cards, then this connection might be used later to determine how voters had voted when they receive their return code.
- **Creation of the return code** – once a voter casts a ballot the Internet voting system generates the relevant return code to the voting choice made by the voter, and sends the return code to the voter's mobile phone. This would seem to require the existence of a link between the voter identity and the return codes (and therefore the value of the vote) during the voting process, and that those with access to the system could use this link to violate the secrecy of the vote.
- **Return code as a voting receipt** – the return code is used to prove to the voter that the Internet voting system has received the vote as it was cast by the voter. As such the return codes can be seen as proofs of how voters cast their ballots, and such proofs are prohibited as they facilitate voter coercion and vote buying.
- **Link between voter ID and vote value** – the Norwegian Internet voting system requires that stored vote data remain linked to the identity of the voter so that repeat votes can be properly dealt with, and only one vote be counted per voter. If the stored vote data includes both the value of the vote (which is needed to count the vote) and the identity of the voter then it may be possible to use these two pieces of data to breach the secrecy of the vote.
- **Secrecy during the counting process** – the secrecy of Internet votes could be violated in a couple of ways during the counting process. If a small number of Internet votes were cast then the publication of results for the Internet component of the result could breach the secrecy of these votes. Additionally, the votes are recorded on the Internet voting system as they are received, and with a time stamp. The timestamp data and the order of recorded Internet votes might be used to violate the secrecy of individual votes.

We will look at each of these issues and discuss the mechanisms that are in place in the Norwegian Internet voting system to address these concerns.

Compliance and the Norwegian Approach

Secrecy at the Point of Voting

This issue is of fundamental importance for the conduct of Internet voting, and is possibly the greatest challenge facing Internet voting. A starting point for considering this issue might be the fact that paper balloting is not always conducted in controlled environments. Postal voting is a voting procedure which is used in many countries for voters who cannot attend the polling station on Election Day. All of the secrecy and freedom of the vote concerns which can be raised about Internet voting can also be raised about postal voting. Postal voting is used in Norway for voters who are abroad. The argument could easily be made that if postal voting is allowed, as it is in many countries, then there is no reason to exclude Internet voting, which carries the same risks in this regard.

This position is supported by the report of the Venice Commission on the compatibility of remote voting and electronic voting (Venice Commission 2004). Finding mixed practices in the 30 countries surveyed for the report, the Venice Commission determines that postal voting is not incompatible with Protocol 1 of the European Convention on Human Rights. The Venice commission states, however, that minimum standards must be maintained for protecting the secrecy of the ballot and that postal voting should only be allowed if it is safe and reliable.[42]

The Venice Commission goes on to say that its analysis of non-supervised postal voting can be applied to the issue of electronic voting:

> *"Consequently, electronic voting is neither generally permitted by human rights nor ruled out a priori. Instead, its acceptability depends on the legal, operational and technical standards implemented in the procedure. In order to establish specific standards, it will be necessary to compare the precautionary measures for e-enabled voting with those for postal voting. Insofar as a potential recommendation set out security measures comparable with those for postal voting, e-enabled voting could be compatible with the European standards in this area and with Article 3 of Protocol 1.6 In this context, it is necessary to ensure that the confidentiality of electronic voting is guaranteed by measures comparable with those applicable to postal voting, especially by preventing data manipulation, protecting anonymity to prevent possible disclosure of the elector's wishes, and by maintaining the authenticity and integrity of the votes cast."*[43]

The Venice Commission concluded that:

> *" . . . remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either non-supervised postal voting or electronic voting."*[44]

However, the Norwegian history of postal voting provides some context for this argument. As recalled by Eivind Smith, a Professor of Public Law at the University of Oslo, Norway has a "long tradition of postal voting. However, older systems of postal voting have been restricted or abolished for fear of different kinds of abuse" (Smith 2011: 9).[45] Right now postal voting is only available for expatriates as the last option to enfranchise voters who otherwise have no way of participating. According to Professor Smith, the introduction of Internet voting would break the trend to limit the use of remote voting from

[42] Paragraphs 62, 63 and 65.

[43] Paragraph 66.

[44] Paragraph 69.

[45] This is taken from an unofficial translation of a paper, "Secret Electronic Elections?", provided to the Ministry as a legal opinion on the Internet voting project. The paper was further developed and published in the law review Lov og Rett, Vol 49(6), page 307-323.

uncontrolled environments only when, “one is unable to attend the poll itself, on polling day to be precise” (Smith 2011: 6).

Although Smith correctly depicts the situation in Norway, postal voting is a legitimate means of casting a ballot and therefore Internet voting does not increase the risks already accepted. The decision to limit or extend remote channels and the goals they are pursuing may be the subject of continuous political evaluation, but it cannot ignore the fact that postal voting is currently in use in Norway. While there may be grounds to limit the use of such remote voting mechanisms, the desire to enfranchise voters who cannot attend supervised voting arrangements could never justify using a voting system that failed to meet basic electoral standards.

Moreover, Internet voting can be seen as a remote voting mechanism that includes additional features representing a significant improvement over current postal voting mechanisms. Repeat voting and the primacy of the paper ballot are features of the Norwegian Internet voting system which can be seen as addressing many of the secrecy and freedom concerns related to remote voting mechanisms.

Repeat voting, first used in the Estonian Internet voting system, allows Internet voters to cast as many Internet ballots as they wish to. The system is designed so that only the last Internet vote is counted. This means that a voter could be observed, or even coerced, while casting an Internet ballot, but they would then be free to cast another Internet ballot when not being observed or coerced. Anyone present when a voter cast an Internet vote would not know if the vote that they observed was the last one cast by the voter, and therefore not know for sure how the voter had voted.

It could be argued that coercers and vote buyers could overcome this feature by ensuring that they observe voters in the final hours or minutes of the Internet voting period, denying the voter the opportunity to cast a subsequent Internet ballot. However, the possibility for Internet voters to cast a paper ballot and the primacy of any paper ballot also serve to mitigate this concern. There is an extended period of early and advance paper voting from locations throughout Norway in the two months before the election. In this period, any voter can take the opportunity to cast a paper ballot in a controlled environment where the secrecy of the ballot is assured. Likewise, Internet voters can cast a paper ballot on Election Day by attending any polling station within the municipality. While it might be possible for vote coercers to monitor Internet voters attending polling stations on Election Day, it would be impractical to monitor all of the locations at which votes could be cast during the early and advance voting periods for the entirety of these periods.

The combination of repeat voting and the primacy of the paper ballot, for which secrecy can be ensured, can be understood to deal effectively with the challenges of ensuring the secrecy and freedom of the vote for Internet voting at the point of voting.

Record of the Voting Session on the Personal Computer

Recommendation 93 requires that residual information be destroyed after the voter has cast a remote electronic vote. Clearly if this was not the case then the secrecy of the vote could be violated by analysis of the residual information. The explanatory memorandum recognises the difficulty in this, saying “technically there may be limited means to ensure this in a remote voting environment. Nevertheless, every measure possible shall be taken to delete such residual information when the vote has been cast." Both the recommendation and the explanatory memorandum seem to assume that, in the case of remote e-voting, it will be extremely difficult or even impossible to completely ensure the destruction of residual information.

Despite the difficulties in ensuring that this information is removed, the security requirements for the Norwegian Internet voting system make it clear that this is a requirement of the system. The general security requirements of the system state that:

> *"Residual information holding the e-voter's decision or the display of the e-voter's choice shall be destroyed after the vote has been cast. When voting in an uncontrolled environment, the e-voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote (e.g. cookies)."*[46]

The supplier of the Internet voting system, Ergo Group, confirmed in its tender documents that this requirement was met by the system.

In addition to this, the system provides the possibility for repeat voting and casting a paper ballot making any residual information which may remain worthless. Even if the residual information is used to reconstruct the value of a vote and the voter identification details associated with the vote, there is no way of knowing if this data relates to a ballot that will be counted for the voter.

Return Codes

The use of return codes represents a significant advance in the Norwegian Internet voting system when it comes to the verifiability of the Internet voting system and the mechanisms for generating voter trust in the accurate functioning of the voting system. However, they also present a number of challenges when it comes to the secrecy and freedom of the vote.

Firstly, the printing of the return codes on the polling card requires that a set of return codes for each voter be calculated and used to print the polling cards. This link could be used by people other than the voter with the return code to determine how an individual voter had cast their ballot. However, the Ministry assured the assessment team that all files used to produce the return code on the polling cards were destroyed once the printing had taken place, meaning that without the voter's polling card (which was sent only to the voter) the return code would be meaningless.

However, the system must be able to produce the appropriate return code when a voter submits an Internet vote. Therefore it may seem obvious that the Internet voting system has to maintain a link between voter identity and the return code, and therefore those with access to the system could use this link to violate the secrecy of the vote.

The Norwegian Internet voting system uses a complex system of separated server functions, encryptions and hash functions to ensure that it is capable of producing the appropriate return code for the voter

[46] This can be found at '7 Security Requirements: OS 4.4" in the document, 'SSA_u_Appendix2B_Requirements_Table' which lists system requirements.

when a vote is received. It does this in a way that makes it impossible to link the voter identity and the value of the vote. The Vote Collection Server (VCS) and the Return Code Generator (RCG) are separate, secure servers, located several hundred miles apart and managed by different Ministries.

The VCS receives the vote, which has been encrypted by the voting applet, and re-encrypts this vote before passing it to the RCG through a secure Virtual Private Network connection. The RCG applies its secret key to the re-encrypted vote, thus deriving what is known as "the long return code." This is a new partial re-encryption of the vote. A hash function of the long return code is created, and based on this hash there is a lookup in the database for the correct "short return code" to be sent to the voter.

As a hash function is a one way function, the generation of the hash cannot be reversed in order to calculate the value of the re-encrypted vote (even if this re-encrypted vote could then be decrypted). This means that only the RCG has the information required to connect the identity of the voter to a hash function of a re-encrypted vote, and that there is no way that the actual content of the vote could be calculated from this information.

This complicated procedure ensures that prior to the counting process, during which the votes are decrypted by the keyholders, it is not possible to determine the way in which voters have voted through the data stored on the system.

A further complication arises with return codes when it comes to the secrecy of the vote; the return code can be considered a vote receipt and a way that voters could prove to third parties how they have voted. This is clearly prohibited by recommendation 51, which says that, "A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast."

At first glance, it seems clear that the provision of the return code does violate this recommendation, as it provides the voter with "a proof of the content of the vote cast." This is the very purpose of the return code, so that voters can be certain that the Internet voting system has received their votes as they were cast, and is a critical mechanism in enabling trust in the system.

However, it would be wrong to conclude consideration of the issue at this point. In fact, a proper assessment is much more nuanced and a full examination requires an understanding of why this recommendation is included. The purpose of ensuring that voters are not in possession of a proof of how they voted is to eliminate the possibility for voters to sell their votes to political parties/candidates or to facilitate the coercion of voters. Ensuring the secrecy of the vote, with no proof of how a vote is cast, makes the conduct of such practices unfeasible as the vote coercer or vote buyer will never know how the voter has actually voted.

In this context, it is important to note that while the return code does prove how the voter has voted, it does not prove the value of the vote that will be counted for that voter. Voters are able to vote as many times as they want using the Internet voting system, with only the last Internet vote being counted. Therefore, a return code could be superseded by a subsequent return code, and a vote-buyer or coercer will have no guarantee that the return code that they are shown represents the vote that will be counted for the voter. Internet voters can also vote using paper ballots on Election Day or in the advance voting period, and any paper ballot will be counted instead of an Internet ballot. Such uncertainty will remove the incentive to engage in practices such as vote-buying and voter coercion.

A literal interpretation of recommendation 51's wording would necessarily lead to a conclusion that the Norwegian Internet voting system does not comply, because the voter is left with a receipt about the way in which they have voted. However, if the recommendation is interpreted in the context of measures to ensure that voter coercion and vote buying do not take place, then the Norwegian Internet voting system meets this standard as any receipt provided/recorded need not represent the vote which is actually counted.

It is this second, more contextual, interpretation of the recommendation which is used in this assessment. The use of return codes, despite being a voting receipt, is not seen as a violation of the secrecy of the vote as it does not prove to third parties the content of the vote which will be counted for the voter.

Secrecy During the Count of Internet Votes

Due to the possibility for repeat voting with the Norwegian Internet voting system and the need to cleanse repeat votes, the stored vote data must include the identity of the voter along with the content of the vote. This creates the possibility for violating the secrecy of the vote when the vote is decrypted.

The encrypted ballots stored on the VCS use a double envelope approach similar to that used for paper postal votes. The outer envelope is removed during the initial stage of the counting process during the cleansing process when repeat votes are filtered so that only one vote is counted for each voter and paper ballots supersede any Internet ballots. The outer envelope contains the voter identity credentials. This means that the votes that pass to the mixing phase of the counting process, and which are still encrypted, have no data which can link the value of the vote to the identity of the voter.

The mixing phase of the counting process is also designed to address concerns about the secrecy of stored votes. Stored votes are logged on the system with a time stamp. Therefore, if the order in which voters have submitted votes to the Internet voting system is known, then once the votes are decrypted the order in which the decrypted votes are recorded can be used to determine how individual voters voted. The mixing phase addresses this issue by taking groups of encrypted votes, re-encrypting them and re-ordering them. The resulting mixed votes have different values, as they have been re-encrypted, and are in a different order, making it impossible to link them back to the vote data on the VCS – which has the vote identification details in the outer envelope of the stored vote.

Only once this re-encryption and mixing process has been conducted are the votes decrypted, ensuring that the decrypted votes are made totally anonymous.

A final issue exists with respect to the secrecy of Internet votes during the counting process; it concerns situations where there are small numbers of Internet votes submitted. When a small number of Internet votes are received, counted and reported this may breach the secrecy of the vote for these Internet voters.

According to the explanations provided by the Ministry, “if there were less than 20 e-votes in an electoral area, then these e-votes are added to the second smallest electoral area, and then the third smallest electoral area, until you’d reach at least 20 votes. These e-votes would then be marked as belonging to 'Area 0000', to avoid that one of these small electoral areas will be registered with more e-votes than it actually had.”

This solution does not completely solve the problem. For example, if dealing with municipal elections, merging electoral areas would only be feasible within the same municipality and it is possible to imagine a small municipality with only one electoral area and a small number of voters. However, Internet voting does not seem to increase the problems that already exist in this regard with traditional paper-based voting.

Conclusion

The secrecy and freedom of the vote are key electoral principles and ones which are seen as very important for the implementation of electronic voting. Internet voting in general, and the Norwegian Internet voting system in particular, present significant challenges in maintaining the secrecy and freedom of the vote.

It is clear that remote voting from uncontrolled environments does not, and maybe cannot, provide the same level of guarantees for the secrecy and freedom of the vote as is provided by paper balloting in a polling station environment. However, the secrecy and freedom of the vote are only two of the principles that elections are required to comply with. In reality, designing an electoral system requires a balancing of principles, some of which work in opposing directions.

The need to enfranchise voters who cannot attend the opportunities to vote in controlled environments during the early and advance voting periods or on Election Day, has led Norway to permit the use of postal voting for overseas voters. Therefore, a relaxation of the principle of secrecy and freedom of the vote has been accepted in Norway for voters using postal voting to participate. If postal voting is seen in Norway as a voting mechanism which meets basic electoral principles, then there seems little reason to reject Internet voting.

In fact, the way in which Norway has implemented its Internet voting system can be seen as a significant improvement over postal voting in the way that the secrecy and freedom of the vote are protected. The Norwegian solution to Internet voting may in fact become a benchmark for future Internet voting systems in the way that it deals with this complex and difficult issue for remote voting.

The decision on whether the secrecy risks related to using Internet voting are acceptable, especially if Internet voting is widely used, will ultimately be a political one. This assessment’s finding is that that the way Internet voting has been implemented in Norway does not violate the principles of the secret ballot and the free expression of the will of the voter, as elaborated in the Council of Europe Recommendations. This finding is largely due to the possibility for repeat voting and the primacy of the paper ballot, although the comparison with the use of postal voting in Norway is also relevant.

Invalid Ballots

Invalid ballots are ballots which do not comply with the electoral rules in some respect or on which the intention of the voter cannot be determined. Under the Norwegian electoral system, ballot paper approval is detailed in section 10-3 of the Election Law:

> *(1) A ballot paper shall be approved if:*
>
> *a) it bears a public stamp when it has been cast on election day,*[47]
>
> *b) it is clear to which election the ballot paper applies,*
>
> *c) it is clear for which party or group the elector has voted, and*
>
> *d) the party or group has put up a list in the constituency. A ballot paper intended for another constituency may be approved only if it applies to a registered political party.*

Ballot papers are invalid if they do not comply with these requirements. Invalid ballots are normally seen as a failure in the system due to mistakes in the administration of elections or in the way in which voters have interacted with the system in recording their votes. It should be the intention of election administrators to minimize the incidence of invalid ballots by implementing voting systems in which the involuntary invalidation of ballots is less likely to occur.

The paper balloting system that Norway uses leads to lower levels of invalid ballots than seen in many other countries. Norway has a separate paper ballot for each party list running for election. Voters choose the ballot for their party of choice in the polling booth. They can then cross off candidates on the party list to give personal votes to those candidates, and give personal votes to candidates from other lists by writing the names of such candidates on the ballot. A significant cause of invalid ballots in other countries occurs when the intention of the voter cannot be determined because more than one party/candidate has been selected on the ballot. The selection of a ballot by the voter to insert into the ballot box makes it clear which party list they support even if the intention of the voter is unclear with respect to personal votes on ballot. Nevertheless, invalid ballots still exist in Norway, with a nationwide rate of 0.13 percent invalid ballots in the 2011 municipal elections and 0.10 percent in the 2011 county elections.

In principle, invalid Internet votes should not exist as the voting software should be designed to prevent invalid ballot choices being made. In fact, eliminating the possibility of invalid ballots (but not blank ballots, which are a legitimate expression of voters' choices) is seen as one of the big advantages of electronic voting. However, as will be explained in detail below, nine invalid Internet votes and one rejected Internet vote were recorded in the Norwegian Internet voting pilot.

[47] Section 10-3(1a) of the Election Law is not applicable for the approval of Internet votes, as these votes cannot be cast on election day – see section 21(4) of the Regulations Relating to Trial Electronic Voting.

Cases of Invalid Ballots

After the completion of the cleansing, mixing and decryption processes for Internet votes on the evening of the elections, the decrypted votes were counted for their relevant elections. Subsequently the Ministry reviewed the logs from this process and discovered that of the 53,916 votes which passed through these stages to be counted, nine votes could not be interpreted after decryption. In fact, these Internet votes had more ballot selections than permitted under the election rules, and were therefore not included in the count of Internet votes.

The votes were distributed amongst the various local government elections in the following manner:

Figure 6 – Distribution of Invalid Internet Votes[48]

Election	Number of Invalid Votes
Rogaland County	1
Sogn og Fjordane County	1
Møre og Romsdal County	2
Nordland County	1
Sandnes Municipality	1
Bodø	2
Hammerfest	1
Total	**9**

The Ministry confirmed that the invalid votes could not have impacted the results of their respective elections as the margin between the last candidate elected and the first candidate not elected is larger than the number of invalid votes in every election affected. However, the generation of invalid Internet votes should not be possible and is indicative of some flaw in the Internet voting process.

Scytl, the supplier of the core Internet voting system, was asked to investigate how these invalid votes could have been generated. The Scytl report[49] considered several possible sources for the generation of invalid Internet votes, including:

- A configuration error when specifying or assigning the voting areas to the voters
- An attack by the same voter that cast the vote by forging a vote containing more than one selection for the same candidate or party
- An error in the applet that included the same party or candidate twice in the encrypted vote50

After exhaustive analysis the possibility of a configuration error was discarded by Scytl, "[t]herefore, the final conclusion is that the votes were generated by including more than one selection for the same candidate due to an attack or an applet error when casting the vote."[51] When considering these two possibilities Scytl concluded that:

[48] Data provided by the Ministry in email of October 21, 2011.

[49] Ergo Group/Scytl (2011) "Audit Report of the 2011 Municipal and County Council Election Results", version 0.1, October 17, 2011, provided by the Ministry in an email dated October 24, 2011.

[50] *Ibid*, p.5.

[51] *Ibid*, p.5.

> *Unfortunately, both cases generate the same type of invalid vote and it is not possible to distinguish which one has generated it. Furthermore, both cases occur in the voting side and therefore, are impossible to detect*.[52]

It was noted that these invalid votes had been detected during the counting process and therefore not included in the count. However, the voter would have believed that a valid vote had been submitted at the time of voting, as these invalid votes were accepted by the RCG and would have led to a return code being sent to the voter (although the return code would have indicated that one more personal vote was recorded than was cast).

Furthermore, Scytl identified a number of improvements that would solve this problem in the future and to report it to the voter when they submit the vote.[53]

In addition to these nine invalid votes, one late vote was found. During the cleansing process, one vote was cleansed, and not included in the count, because it was submitted after the expiry of the online voting session by the voter. When voters log on they are given 30 minutes to complete their voting transaction and if they exceed this time they are automatically logged out. The submission of a vote after the 30 minute period also should not have been possible.

In this case it seems that although the voter completed the voting transaction before the end of the 30 minute window, it was so close to the end of the 30 minutes that when the system began to process the vote while it was within the 30 minute window. However, the completion of the vote transaction on the server occurred after the 30 minutes, if only by a matter of milliseconds. The rules for the cleansing process are strictly applied and the vote was rejected for being submitted after the 30 minutes. The voter would have received a return code, however, and will have had no reason to believe that the vote was not going to be included in the count.[54]

While this situation was statistically highly unlikely to happen, it does demonstrate a (minor) flaw in the Internet voting system.

Norway is not the only Internet voting country which has experienced the anomaly of having invalid Internet votes. In 2011, Estonia held parliamentary elections and its final results included a null vote. According to the OSCE/ODIHR report, “during the counting, one vote was determined invalid by the vote counting application, since it was cast for a candidate who was not on the list in the corresponding constituency. The project manager could not explain how this occurred.”[55]

A similar incident took place in New South Wales, during the 2011 local elections. It was observed that an output file of the votes did not appear to agree with the number of votes actually printed. The official explanation is that the java script allowed the introduction of non-numeric characters to be entered as

[52] *Ibid*, p.10.

[53] *Ibid*, p.5.

[54] For the explanation provided during the decryption ceremony and subsequent questions see the record of the ceremony at http://media01.smartcom.no/Microsite/dss_01.aspx?eventid=6316, at 53 minutes to 1 hour and 1 minute.

[55] See the Report of the *Office for Democratic Institutions and Human Rights*, which is available on-line: http://www.osce.org/odihr/77557 [last accessed May 4, 2012].

ballot preferences. This failure affected 43 ballots whose validity had to be assessed by electoral authority, “resulting in one of the four affected Legislative Assembly ballot papers and eight of the affected Legislative Council ballot papers being treated as informal [invalid].”[56]

Despite occurrences of invalid ballots in other Internet elections, and the small numbers of ballots affected in Norway, the fact that such invalid ballots are possible does have implications for compliance of the Norwegian Internet voting system with the Council of Europe Recommendations.

Relevance for Compliance with Council of Europe Recommendations

None of the Council of Europe Recommendations specifically address the issue of invalid ballots, but the existence of invalid (including out of time) ballots, and the way in which they occurred, has implications for the assessment of several of the recommendations. Invalid ballots were an issue when assessing the following recommendations:

- 14. The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed. (Non Compliant)
- 34. The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted. (Not Possible To Determine)
- 58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such. (Non-compliant)
- 91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable. (Non-compliant)
- 92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote. (Not Possible To Determine)
- 95. The e-voting system shall ensure that the voter’s choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box. (Not Possible To Determine)

In fact, invalid ballots were responsible for all three findings of non compliance made in this assessment as well as three cases out of four where it was not possible to determine compliance with the recommendations.

In the cases where the Norwegian Internet voting system was found to be non-compliant with the Council of Europe Recommendations (recommendations 14, 58 and 91), the reason for the non-compliance was not necessarily the existence of the invalid ballots, but the way in which they were dealt with by the system. The voters who submitted invalid ballots were sent return codes for the submitted

[56] See the New South Wales Election Commission Annual Report (p. 28), at http://www.parliament.nsw.gov.au/prod/la/latabdoc.nsf/0/3abef1db9c32a557ca25793b0022aaf3/$FILE/NSWEC_Annual_Report_2010-2011.pdf and the report of the audit conducted by PWC (pp. 5 and 13), at http://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/93481/iVote_Audit_report_PIR_Final.pdf [last accessed May 11, 2012].

votes and not given any indication by the voting applet that an invalid vote had been submitted.[57] In doing so they indicated that a vote had been submitted successfully when this was not the case, in violation of recommendation 14. The Internet voting system also failed to properly record and report that invalid votes had been submitted. The nine invalid votes were only discovered by a post-election audit by Scytl. This may have been because the occurrence of invalid votes in the system had been considered to be impossible, but this failure represented a failure to comply with recommendation 58.

Similarly, the one ballot which was cast outside of the 30 minute voting session period is problematic as the voter who cast this ballot will have received no indication that the vote would be rejected, and again received a return code. Therefore, in this very specific instance of a ballot being submitted in the very last milliseconds of the voting session time limit, the fact that the vote has not been cast in the prescribed time limit is not ascertainable. While this is a statistically unlikely scenario, it represents a problem in principle as it is possible to cast a vote which is outside of the permissible time period but which does not lead to the voter being informed that the vote has been cast unsuccessfully.

For the three recommendations where it was not possible to determine compliance, the issue in question focuses on the causes of the invalid ballots. Recommendation 34 requires that the system maintain the integrity of the votes, 92 that the system protects against the modification of the votes, and 95 that the voter’s choice be accurately represented in the stored vote. The Scytl report on the invalid ballots ruled out a system configuration error as the cause of the invalid ballots, but could not determine whether a voting applet error was the cause of the invalid ballots, or whether it was due to an attempt by the voter to hack the vote being submitted.

If invalid ballots are a result of a deliberate attempt by the actual voters to try and manipulate the voting system, then the system would be in compliance with these three recommendations: the integrity of the vote cast would have been maintained (recommendation 34); the system would have recorded the vote as it was cast and not allowed it to be subsequently modified (recommendation 92); and, the (invalid) voters’ choice would have been accurately represented in the stored vote (recommendation 95). Alternatively, if the invalid ballots were the result of a voting applet error, then the integrity of the vote would not have been maintained, the vote would have been modified after casting, and the voter’s choice would not have been accurately represented.

As Scytl could not determine the actual cause of the invalid ballots, it was not possible to determine if the Norwegian Internet voting system was in compliance with these recommendations.

Conclusions

While the issue of invalid Internet ballots was the largest cause of non compliance in the assessment, as well as being the cause of several recommendations for which an assessment concerning compliance was not possible, the issue needs to be put into perspective. Invalid ballots only affected 10 votes, and were split across a number of elections. The impact was negligible and did not affect the results in any way. It is also worth noting comparisons with paper voting, remote and in person, which do permit the submission of invalid ballots and do not inform the voter that this is the case upon submission.

[57] Although the return code will have indicated that one more personal vote was recorded than actually cast.

Nevertheless, the existence of these invalid ballots and the way that the Norwegian Internet voting system dealt with them is of concern and clearly impacts the system's compliance with the Council of Europe Recommendations, and therefore with the system's legality under the Norwegian electoral legal framework. However, this was a pilot of the Internet voting system, and such pilots are conducted precisely to try and identify these sorts of issues.

The Ministry and Scytl are now aware of the issue and have identified a modification to the system, which will address this issue in the future. It is hoped that this modification will implement some form of coherence check, as the Geneva Internet voting system does, against every vote that is received in order to verify that the ballot meets the validity rules. Where this is not the case, the voter should be informed of the failure to cast a valid ballot so that another attempt can be made to vote.

Audit

When compared to paper-based voting from controlled environments, electronic voting and especially remote Internet voting suffer from a lack of transparency that is difficult to compensate for. Paper-based voting in controlled environments allows for a level of observation of the process that enables observers to effectively verify the correct functioning of the voting and counting processes. Electronic voting systems need to provide other mechanisms to ensure that the results produced are accurate and generate stakeholder trust in the process.

Audit mechanisms play a significant role in this assurance process, both internally within the election management body but also with voters, political parties, candidates, media, and observers. The ability to audit the functioning of an electronic voting system is also very prominent in the Council of Europe Recommendations.

Audit and the Council of Europe Recommendations

When discussing recommendation 100, the Explanatory Memorandum defines the auditing of the election process as, "the means by which, in particular, the processes used to collect and count the vote can be examined, in order to confirm the authenticity of the result." The main recommendations which deal with the issue of audit are as follows:

- 26. There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable. (Fully Compliant)
- 59. The e-voting system shall be auditable. (Fully Compliant)
- 100. The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application. (Fully Compliant)
- 102. The audit system shall be open and comprehensive, and actively report on potential issues and threats. (Fully Complaint)
- 103. The audit system shall record times, events and actions, including:
    - all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.:

  - any attacks on the operation of the e-voting system and its communications infrastructure;
  - system failures, malfunctions and other threats to the system. (Fully Compliant)
- 104. The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions. (Fully Compliant)
- 105. Disclosure of the audit information to unauthorized persons shall be prevented. (Fully Compliant)
- 106. The audit system shall maintain voter anonymity at all times. (Fully Compliant)
- 107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted. (Fully Compliant)
- 108. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes. (Partially Compliant)
- 109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system. (Fully Compliant)
- 110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed. (Fully Compliant)

Audit Mechanisms

The Norwegian Internet voting project was designed to be implemented in a transparent manner, and a number of different audit mechanisms were included. On a project level, the Ministry contracted Veritas to conduct on-going quality assurance assessments to the Steering Committee. These assessments focused on the procurement and project management aspects of the pilots.

In terms of the functioning of the system itself, the delivery of return codes to each voter on the completion of their Internet vote can be seen as the first stage in the audit process, with voters empowered to check that the system had received a vote of the same value that they had cast. This does not ensure, however, that the system records the votes as it has received, that it does not modify the votes in some way, and that votes received by voters (and only these votes) are correctly included in the results.

The Norwegian Internet voting system was designed so that all of these checks could be made, but recognising the importance of an independent audit of the system, the Ministry did not wish to conduct these checks itself. When no independent organisation indicated an intention to conduct this audit the Ministry decided to contract an outside organisation to do so. Promis AS was awarded a contract by the Ministry to conduct verification functions for the Internet voting system, including the verification/audit of the processing of ballots received on the VCS through the counting and results process.

The audits that Promis AS performed included the following:

- **Verification of the certificate from the ID portal** – the independent auditor conducted a physical inspection of ID portal certificates obtained through the Ministry and through a second channel independent of the Ministry.

  Both certificates were found to be identical, demonstrating that the ID portal certificate matched the certificate used in the cleansing process to verify that all ballots had a valid authentication token from the ID portal and were legitimate votes.

- **Comparison of hashes between the VCS and the RCG** - independent software was developed to verify that the hashes of the encrypted votes stored on the VCS were the same as the hashes of the encrypted votes stored on the RCG, and that no additional votes were stored on either server. This proves that votes of the same value are stored on each server.

  In fact the comparison of the votes stored on the VCS and RCG found that there were 53 votes stored on the RCG, which were not present on the VCS. The Ministry had in fact indicated to Computas AS that between 54 and 57 votes would be found on the RCG with no corresponding encrypted vote on VCS. The Ministry indicated that these entries on the RCG were not problematic as they represented cases where an encrypted vote was not stored on the VCS due to some technical problem. The voters casting these ballots were informed on-screen that the vote had not been cast and a receipt was never sent out to the voter.

  All of the other votes stored on the VCS and RCG were identical.

- **Verification of the integrity of the ballot box after data transferred from the VCS to the Ministry's premises** – independent software was developed to check that every ballot stored on the VCS was present and identical in the copy of the ballot box used for the counting process.

  This independent software showed that the contents of the VCS were identical to the contents of the ballot box used for the counting process.

- **Verification that the cleansing process has not injected new votes to the ballot box** – independent software was developed to check that the result of the cleansing process did not contain any votes that were not registered on the VCS.

  All of the votes which were passed from the cleansing process for counting were represented in the ballot box from the VCS.

- **Verification of zero-knowledge proofs regarding the correct mixing and re-encryption of the encrypted votes** – the mixing process stage of the counting process creates a zero-knowledge proof to demonstrate that each mix-node has decrypted and encrypted groups of votes it has received as input correctly. Independent software was developed to check these zero-knowledge proofs, and in doing this check, verify that the mixing process output votes as the same value as were input into the process.

All of the zero-knowledge proofs were found to be correct, demonstrating that the mixing process produced a randomized, but accurate, copy of the ballots, which entered into the mixing process.

- **Verification of the zero-knowledge proofs regarding the correct decryption of the encrypted votes** – the decryption process for the votes, which are to be counted, produces a zero-knowledge proof for each vote which is decrypted. Independent software was developed to check the zero-knowledge proof for each decrypted vote.

  All of the zero-knowledge proofs were found to be correct, demonstrating that the correct private key was used to decrypt the votes passed from the mixing process and therefore that the decrypted vote values accurately reflect the encrypted vote values.

In addition, every event on infrastructure components and transactions on the various servers used by the Internet voting system (such as the VCS, RCG, cleansing server, mixing server and tabulation server) was logged using immutable logs. These logs were monitored by the Ministry using a professional log monitoring system as the project unfolded, and were also reviewed through a comprehensive post-election audit. Ongoing monitoring of the functioning of the infrastructure also took place, with alerts sent to key staff when issues of concern arose.

Relevance for Compliance with Council of Europe Recommendations

Despite the extensive and detailed nature of the audit requirements included in the Council of Europe Recommendations, the Norwegian Internet voting system has managed to implement mechanisms which in the opinion of the assessment team manage to comply with these audit requirements.

The combination of verification mechanisms means that the system is end-to-end (E2E) verifiable, with every stage of the processing of Internet votes being subjected to the possibility of audit and verification. The E2E verifiability is achieved using different mechanisms than many other E2E solutions (which provide the voter with a token to prove that their vote has been included unaltered in the final count) but these mechanisms still achieve the same goal of E2E verifiability.

Not only was this audit of the process possible, but it was conducted by an organisation which was, in principle, independent. While the organisation that conducted the audit was contracted to do so by the Ministry, it was only because no other organisation indicated that it would conduct the audit (which had been the expectation of the Ministry). Faced with the prospect of either having to do the 'independent' audit themselves or having no entity do the audit, the Ministry chose to contract Promis AS for the task.

One area of slight concern that could be addressed by the Ministry for future elections is related to the openness of the audit process. Recommendation 102 requires that the audit system be open. The Ministry indicated that the transaction logging process was open to observer groups if they had wished to view it as the Internet voting period progressed. While the willingness to provide access to the audit logs was positive, it is not clear how this possibility was communicated to observers. The comment is somewhat complicated by the fact that no domestic observers registered for the 2011 municipal and county elections. IFES was registered as an international observer and did not receive any information about the possibility to monitor the audit (although it was also not present in Norway during the

Internet voting period). It is to be hoped that observers would be informed of the possibility for the observation of the audit logs during any future use of Internet voting in Norway.

Nevertheless, this relatively minor issue does not detract from the overall compliance of the Norwegian Internet voting system with the audit requirements contained in the Council of Europe Recommendations. Even the one partial exception to this compliance (recommendation 108) seems to require an exceptional level of access to the audit system, a level of open access that many, if not all, other Internet voting systems would likely fail to achieve.

Conclusion

The Norwegian Internet voting system has made significant efforts to provide a system which is auditable and audited, and that provides mechanisms for stakeholders to independently check the correct functioning of the system. As such, the Norwegian Internet voting system may function as a role model in audit standards for Internet voting systems in the future.

Compliance with Other Emerging Electronic Voting Standards

A discussed earlier, the Council of Europe recommendations play a central role in the body of emerging standards relating to electronic voting. The Norwegian Internet voting system's compliance with the Council of Europe Recommendations has already been assessed and discussed above. This section of the report will therefore only address compliance with emerging standards not covered by the Council of Europe Recommendations. The Norwegian Internet voting system is not under the same legal obligation to comply with these emerging standards as it is for the Council of Europe Recommendations. Nevertheless, these additional emerging standards represent an important benchmark against which the Norwegian Internet voting system can be assessed.

Transparency

Election management bodies need to take active steps to promote the transparency of electronic voting[58]
As discussed in the assessment of the Council of Europe recommendations related to transparency (for example, recommendations 20-23) significant steps were taken by the Ministry to make the Norwegian Internet voting system transparent and understandable. The Ministry's website included many pages of information about the Internet voting system, including source code, system documents and presentations on the system. The Ministry also provided special events for observers related to observation of the Internet voting process, with a conference on e-voting the day before the election and a counting and decryption ceremony on the evening of the election.

While the assessment of the Council of Europe Recommendations identified areas in which additional transparency measures were needed, this should not detract from the significant efforts (active steps) that the Ministry made to provide transparency in the Internet voting process.

This requirement has been partially met by the Norwegian Internet voting system.

[58] (Carter Center 2007:6).

Political actors must have access to manuals or guidelines for the implementation of the technology[59]
The creation of a manual is a product that is more normally developed for supervised voting channels. For example, when electronic voting machines are used in polling stations, a manual can help polling staff to set up the voting machines and to answer any questions about or problems with the machine during polling.The development of such manuals is not as necessary for uncontrolled voting environments. It is not practical to provide each voter with a manual and there are not staff supervising the conduct of Internet voting who could have the manual and be trained in its contents. However, the Ministry's website did have instructions for using the Internet voting systems and Frequently Asked Questions available to voters. They also sent Internet voting instructions to each voter in the pilot municipalities.

This requirement has been met by the Norwegian Internet voting system.

Political actors must have access to documents related to certification, testing and security[60]
As the Norwegian Internet voting system did not go through a certification process, there are no documents related to certification. Some security related documents were made available by the Ministry on its website, but no testing documents were made available.

This requirement is only partially met by the Norwegian Internet voting system.

Access should be provided for observers in a manner that does not obstruct the electoral process[61]
The different kinds of access that were provided to observers at the different stages of the Internet voting process do not seem to have obstructed the conduct of Internet voting in any way.

This requirement is met by the Norwegian Internet voting system.

Public Confidence

Stakeholders are involved in the introduction of electronic voting and counting technologies[62]
Stakeholders have a role in the debate about whether to use electronic voting technologies, and their opinions have to be taken into consideration when a decision is made about the use of the technology. There was a very open debate in Norway about the use of the Internet voting system, and in 2010 the Storting engaged in a very comprehensive debate on whether the Internet voting trial should proceed. The Storting agreed to proceed with the Internet voting pilot, although many were skeptical about it.

Additionally, voter groups were also involved in trialing the system before it was used in the pilots. The Ministry provided a number of opportunities for voters to test the Internet voting system before they used it in the local government elections. The Internet voting system was used in trial ballots in each of the pilot municipalities in the 12 months preceding the local government elections. These ballots were for youth councils and for local consultations, and the lessons from these trials were used to further develop the system used in the pilots.

[59] (OAS 2010:28).
[60] (OSCE 2008:17).
[61] (Pran and Merloe 2007: 62; OSCE 2008: 17).
[62] (Carter Center 2007: 8).

This requirement is met by the Norwegian Internet voting system.

Simulations of the electronic voting system should take place[63]
As discussed above, the Ministry conducted trial ballots for voters in each of the pilot municipalities. Voters in the pilot municipalities were also provided the opportunity to experiment with the Internet voting platform through a test Internet voting website established by the Ministry. This website was an authentic copy of the actual Internet voting website, including the use of third party authentication mechanisms (such as the MinID portal) and return codes, and was available from July 20 to August 1.

This requirement is met by the Norwegian Internet voting system.

Usability

Users (voters) should be involved in the public testing of the electronic voting system[64]
The trials discussed above which were held in each pilot municipality in the 12 months prior to the pilot can be considered as public testing of the electronic voting system.

This requirement is met by the Norwegian Internet voting system.

System Certification

Electronic voting and counting technologies must be certified by an independent body before use and periodically thereafter[65]
While this emerging standard is covered by the Council of Europe Recommendations, as well as a number of other sources for emerging standards, the certification of the Norwegian Internet voting system was specifically excluded from the Regulation Related to Trial Electronic Voting, which incorporated the recommendations into the electoral legal framework.

As the Ministry decided not to utilize a certification process for the Internet voting pilots, this requirement is not met by the Norwegian Internet voting system.

The certification process should be conducted in a transparent manner providing electoral stakeholders access to information on the process
While this emerging standard is covered by the Council of Europe Recommendations, as well as a number of other sources for emerging standards, the certification of the Norwegian Internet voting system was specifically excluded from the Regulation Related to Trial Electronic Voting, which incorporated the recommendations into the electoral legal framework.

As the Ministry decided not to utilize a certification process for the Internet voting pilots, this requirement is not met by the Norwegian Internet voting system.

[63] (Pran and Merloe 2007: 59).
[64] (OSCE 2008: 14).
[65] (OSCE 2008: 22; Pran and Merloe 2007: 65-5 and 72; Carter Center 2007: 7).

System Testing

System testing should take place transparently, with access for political actors[66]
Stakeholders should not only have access to the testing process itself, but also to the results of the testing and the test reports.

Stakeholders in Norway were not invited to observe the testing of the Internet voting system and were not provided access to documents relating to the testing of the system.

This requirement is not met by the Norwegian Internet voting system.

System Security

Attempts to hack into electronic voting and counting machines or the election management system into which results are received, need to be detected, reported and protected against[67]
The Norwegian Internet voting system implemented mechanisms to protect against unauthorized intrusions into the system. It also implemented monitoring mechanisms so that any anomaly was detected, reported and an appropriate warning sent to Ministry staff. While attempts to hack into the system were detected, none were successful.

This requirement is met by the Norwegian Internet voting system.

Audit and Recount

Recounts must involve meaningful manual recounts of ballots cast electronically and not merely a repetition of the electronic result already provided[68]
It is debatable whether there was a recount of the Internet votes in the Internet voting pilots for the 2011 municipal and county elections. The Election Law requires that ballots be counted in two rounds, with a provisional and a final count. This process was conducted for the Internet ballots, but it was not a recount of the same ballots and was therefore not comparable.

The preliminary results for the Internet ballots cast during the pilots did not include information about all of the paper ballots cast, as some paper ballots were still being processed at the time that the data on paper votes was obtained by the Ministry for the preliminary count of Internet ballots. The subsequent processing of paper ballots may have led to additional Internet votes being cleansed and not included in the final count of Internet votes.

The second count of Internet ballots would, therefore, not be expected to produce the same results and accordingly does not meet the purpose of a recount – to check that the first count was correct.

An audit process was conducted, and this checked that all Internet ballots, which were received were processed unaltered through the count, and that only those ballots were included in the results (with the exception of cleansed ballots). While this represented a check on the integrity of the processing of

[66] (OAS 2010: 28; Pran and Merloe 2007: 67).
[67] (OSCE 2008: 12).
[68] (OSCE 2008: 19; Pran and Merloe 2007: 78)

Internet ballots, including the counting process, this audit did not perform a recount of the votes which were included in the final results.

This requirement is not met by the Norwegian Internet voting system.

Voter Verified Audit Trail

It must also be possible to assure voters that their votes are being counted as cast while also ensuring that the secrecy of the vote is not compromised[69]

This emerging standard is generally applicable to electronic voting machines operated in controlled environments, and a voter verified paper audit trail is not seen as appropriate for remote voting as it allows the voter to prove to others how they have voted. Despite this, the Norwegian Internet voting system appears to meet this requirement.

The return code provided to the voter does not assure the voter that their vote has been counted as cast, but it does prove that their vote has been received as cast – which is the first stage of verifying the integrity of the vote throughout the process. The other stages of vote integrity are proven by the independent audit of the Internet voting system conducted by Promis AS (and discussed in more detail in the thematic section on audit). The combination of the return code and the independent audit proves to the voter, if they trust the independent auditor, that their vote has been counted as cast.

This has to be done in a manner that does not violate the secrecy of the vote. The return code could be seen as a receipt that proves how the vote was cast. However, as discussed in the thematic section on secrecy and freedom of the vote, although return code is a receipt of the vote, because of the possibility for repeat voting and the primacy of the paper ballot, it can never be proven to anyone other than the voter that a return code represents a ballot that is included in the count.

This requirement is met by the Norwegian Internet voting system.

Mandatory Audit of Results

A mandatory audit of the results generated by electronic voting or counting technologies should be required by law and take place for a statistically significant random sample of ballots[70]

This emerging standard is targeted at the use of electronic voting or counting machines in controlled environments. It is not applicable to remote voting from uncontrolled environments, for which previous requirements for audit adequately cover the requirements.

[69] (Carter Center 2007: 7; OSCE 2008: 18).

[70] (OSCE 2008: 18; Pran and Merloe 2007: 64 and 79).

Incremental Implementation

Whenever electronic voting and counting technologies are introduced they should be done so in an incremental manner and should start with less important elections[71]

It is not possible to say that the Norwegian Internet voting system has been implemented in an incremental manner as an assessment of this statement would only be possible over a series of elections. However, incremental implementation must be seen as, by starting on a small scale in the beginning and in only piloting the Internet voting system initially in 10 municipalities, the Ministry has at least started on a small scale to begin with.

While not wanting to detract from the significance of municipal and county elections, such elections are generally considered as being less important than national elections. Therefore, the Norwegian Internet voting system has also met this aspect of the emerging standard.

This requirement is met by the Norwegian Internet voting system.

Conclusions

Two issues emerge from this assessment of the compliance of the Norwegian Internet voting system with other emerging electronic voting standards – transparency and access to information, and certification.

As the assessment of the Council of Europe Recommendations found, there are a number of areas in which the transparency of the process could be improved and additional access to information provided. This should not detract from the considerable efforts that the Ministry has made to try and make the Internet voting system transparent. However, there are areas where this transparency could be improved further and this has a negative impact on the compliance of the system with some of these emerging standards.

Clearly the Norwegian Internet voting system does not comply with the emerging standards on the need for, and process of, certification of the system as a decision was taken not to conduct certification of the system for the pilots.

[71] (OSCE 2008: 23; Carter Center 2007: 2).

6. Summary of Key Findings

The Norwegian Internet voting system was assessed against the Council of Europe Recommendations and against a body of other emerging electronic voting standards, as defined in documents from the Council of Europe, OSCE, OAS, Carter Center and NDI. While the majority of the Council of Europe Recommendations have been adopted into the legal electoral framework for Norwegian elections through the Ministry's Regulations Related to Trial Electronic Voting, the other emerging standards have not been 'adopted' in the same way for Norway. Nevertheless, it is interesting to see how the Norwegian Internet voting system complies with these other emerging standards even if findings of non-compliance do not have the same legal implications as non-compliance with the Council of Europe Recommendations.

Of the 112 Council of Europe Recommendations, 10 were found to be not applicable to the Norwegian Internet voting system. This was either because they were excluded from being applicable by the Regulations Related to Trial Electronic Voting (seven recommendations) or they related to aspects of electronic voting which were not implemented in the Norwegian Internet voting system (three recommendations) – such as candidate nomination and voter registration. Of the remaining 102 recommendations, the Norwegian Internet voting system was found to be fully compliant with 85 recommendations, partially compliant with 10 recommendations, non-compliant with three recommendations, and for four recommendations it was not possible to determine if the system was in compliance.

The three cases of non-compliance were all related to the submission of invalid and out-of-time ballots on the Internet voting system, and specifically the way in which the system dealt with these ballots. The 10 cases of partial compliance were due to additional measures that the Ministry could have taken to provide information to stakeholders about the Internet voting system, control procedures for the management of the system, mechanisms to ensure that Internet votes were included in the final results, the failure to provide special measures for elderly voters to try out Internet voting, and the requirement for an external check/certification of the system.

The four cases in which it was not possible to determine whether the system was in compliance with the Council of Europe Recommendations were largely a result of uncertainty about the causes of the nine invalid ballots received by the Internet voting system, but also due to the fact that it is still not known whether the findings of the audit process will be applied in future elections using Internet voting.

The other emerging standards relating to electronic voting largely deal with issues also covered by the Council of Europe Recommendations, but sometimes identify a requirement that is slightly different to the recommendations, or add to the requirements of the recommendations. In total, 15 emerging standards were identified which can be seen as additional to the Council of Europe Recommendations (many of the standards identified by the institutions listed above serve to re-enforce and repeat the standards that the Council of Europe has identified in its recommendations).

Of the 15 additional emerging standards identified, the Norwegian Internet voting system was found to be in compliance with 11, with two being assessed as partially compliant and two as non-compliant.

The non-compliant standards related to the need for independent certification of electronic voting systems. The Council of Europe Recommendations also contains provisions relating to certification procedures, but these recommendations were excluded by the Ministry in the Regulations Relating to Trial Internet Voting. The intention is that the Norwegian Internet voting system would only be certified if it is to be used more widely in the future.

The two emerging standards with which the Norwegian Internet voting system is seen to be partially compliant relate to transparency and access to information. As indicated in the assessment of Council of Europe Recommendations, much has been done by the Ministry to create a transparent Internet voting process but there remain additional measures that could be taken to enhance transparency and provide access to key documents about the system.

In conducting the assessment of the Norwegian Internet voting system's compliance with the Council of Europe Recommendations a number of key themes were identified and discussed in greater detail. These were the secrecy and freedom of the vote, invalid ballots, and audit.

Secrecy and Freedom of the Vote

The secrecy and freedom of the vote are fundamental to the conduct of elections which meet international standards. The secrecy of the vote requires that voters are able to cast their votes in private, unobserved by anyone, ensuring that only voters themselves will know how they have cast their ballots. It also requires that electoral procedures make it impossible to link a ballot and a voter's personal identification data in order to avoid breaking the anonymity of the vote. Without the secrecy and anonymity of the ballot, the freedom of the voters to express their true ballot preferences may be compromised.

The importance of this standard is reflected in the Council of Europe Recommendations, with 11 recommendations identified which re-enforce the need for this secrecy and freedom. The prominence of this standard throughout the recommendations is a reflection of the challenges that electronic voting, and especially Internet voting, presents to the realization of these standards. At the core of this challenge is the fact that uncontrolled voting environments, like Internet voting, cannot guarantee that the voter is not put under undue influence as the vote is cast.

Complicating an already significant challenge in this respect is the use of return codes by the Norwegian Internet voting system. While the use of return codes provide voters with a degree of confidence that their Internet votes have been recorded accurately by the Internet voting system, these codes can be seen as a proof of how voters cast their ballots and therefore facilitate voter coercion and vote-buying.

The analogy of postal voting, where many of the same concerns exist as for Internet voting, is useful in assessing whether the Norwegian Internet voting system meets this fundamental electoral standard. However, the use of postal voting is restricted in Norway to overseas voters, and the concern might be that extending the use of remote voting mechanisms, such as Internet voting, increases the potential for voter coercion and undemocratic practices.

The Norwegian Internet voting system implements a number of mechanisms that are aimed at addressing these concerns – repeat voting and the primacy of the paper ballot. The repeat voting facility allows voters to cast as many Internet votes as they wish to, with only the last one being counted. Additionally, there is always the possibility for the voter to cast a paper ballot, either through the extended period of early and advance voting or on Election Day at the polling station. Importantly, any paper ballot supersedes an Internet ballot, even if the paper ballot was cast before the Internet vote.

This ensures that if a voter is observed, or even coerced, while casting an Internet vote, the observer will never know if this Internet vote will be included in the count or not. A subsequent Internet vote may be cast or a paper ballot may be cast, either of which will supersede the observed Internet ballot. This also deals with the problem of the return code and its potential use as a voting receipt. While the return code can be considered as a proof of the content of the vote, only the voter knows if it represents the vote that will be included in the count. Furthermore, it is impossible for the voter to prove to anyone else that it represents a vote that was counted.

In the opinion of this assessment, these measures successfully reduce the risks associated with remote Internet voting to acceptable levels and the Norwegian Internet voting system is in compliance with secrecy and freedom of the vote aspects of the Council of Europe Recommendations. This argument is supported by the fact that postal voting is already permitted in the Norwegian electoral system and that the Norwegian Internet voting system provides additional protection for the secrecy and freedom of the vote that postal voting cannot provide.

Invalid Ballots

An invalid ballot is normally caused either by not having been properly authorised by the election administration or because the intention of the voter cannot be determined. In principle, invalid Internet votes should not exist as voting software should be designed so that making invalid ballot choices is not possible. In fact, the ability to eliminate the possibility for invalid ballots (but not blank ballots, which are a legitimate expression of voter choice) is seen as one of the big advantages of using electronic voting.

Despite this, the Norwegian Internet voting system recorded nine invalid ballots for the municipal and local election pilots and one ballot, which was submitted after the end of the 30 minute voting session window. The nine invalid ballots contained choices for multiple candidates, making the intention of the voter impossible to determine, and neither the invalid or out of time ballots were included in the results.

Scytl, the supplier of the core Internet voting system, was asked to investigate how these invalid votes could have been generated. While many possible causes were considered, Scytl was unable to determine which of two possible causes led to the submission of the invalid ballots. Scytl concluded that the invalid ballots were either due to an attempt to hack the system by the voter or due to a voting applet error when casting the vote.

The existence of these invalid and out-of-time ballots, as well as the way in which they were processed by the system, had implications for the assessment of the system's compliance with a number of Council of Europe Recommendations. The fact that these invalid and out-of-time ballots did not produce an error message to the voter, and in fact resulted in return codes being sent, led to all three findings of non-compliance with the recommendations in this assessment.

The existence of the invalid ballots also led to three out of four cases where the assessment could not determine whether the Norwegian Internet voting system had complied with the recommendations or not. This was because the two possible causes identified by Scytl would result in different findings with respect to compliance, especially in relation to whether the will of the voter was accurately reflected in the recorded vote.

While the issue of invalid Internet ballots was the largest cause of non-compliance in the assessment, as well as being the cause of several recommendations for which an assessment concerning compliance was not possible, the issue needs to be put into perspective. This issue only affected 10 votes, split across a number of elections. The impact was negligible, and did not affect the results in any way. It is also worth noting comparisons with paper voting, remote and in person, which do permit the submission of invalid ballots and do not inform the voter that this is the case upon submission.

The existence of these invalid and out-of-time ballots is a concern though, and they ultimately resulted in a failure to comply with some of the recommendations. The Ministry and Scytl are now aware of the issue and a modification to the system has been identified which will deal with this issue in the future. It is to be hoped that this modification will implement some form of coherence check, as the Geneva Internet voting system does, against every vote that is received in order to verify that the ballot meets the validity rules. Where this is not the case, the voter should be informed of the failure to cast a valid ballot so that another attempt can be made to vote.

Audit

When compared to paper based voting from controlled environments, electronic voting and especially remote Internet voting, suffer from a lack of transparency that is difficult to compensate for. Electronic voting systems need to provide additional mechanisms to ensure that the results produced are accurate and generate stakeholder trust in the process. Audit mechanisms play a significant role in this assurance process, both internally within the election management body but also with voters, political parties, candidates, media, and observers. The ability to audit the functioning of an electronic voting system is also very prominent in the Council of Europe Recommendations.

The need for transparency and the possibility to audit the correct functioning of the system have been central to the design of the Norwegian Internet voting system, which is designed to allow E2E verification. Unlike other E2E verifiable systems, the verification mechanisms are divided between various stages of the system, with the voter conducting the first component of verification by checking the return codes they receive after voting. Subsequent stages of the verification process have to be conducted by IT experts but can be done by independent organisations.

When considered in their entirety, the combination of verification of the different stages of the voting and counting process ensures that votes are received as cast, recorded as received, remain unaltered through the counting process, and only authorised votes are included in the results.

Despite the audit requirements included in the Council of Europe Recommendations being extensive and detailed in nature, the Norwegian Internet voting system has managed to implement mechanisms which, in the opinion of the IFES team, manage to fully comply with these audit requirements. Not only was this audit of the process possible, but it was conducted by an organisation which was in principle independent. While the organisation that conducted the audit was contracted to do so by the Ministry, this was only because no other organisation indicated that it would conduct the audit (which had been the expectation of the Ministry). Faced with the prospect of either having to do the 'independent' audit themselves or having no entity to do the audit, the Ministry chose to contract Promis AS to for the task.

Conclusions

As a package, the Council of Europe Recommendations represents a very comprehensive and detailed set of standards for the conduct of electronic voting. In many ways, these standards establish a higher benchmark for electronic voting than for paper voting in controlled environments. This is somewhat expected given the inherent lack of transparency with electronic voting and the need to compensate for this with additional mechanisms to ensure the integrity of the process and the confidence of stakeholders.

For the Norwegian Internet voting system to fully comply with 85 of the 102 relevant recommendations and only be non-compliant with three recommendations is a significant achievement given the exacting nature of the Council of Europe Recommendations. Even the three non-compliant recommendations and the 10 partially compliant recommendations should be carefully considered within the relevant context.

Firstly, this was a pilot of a new Internet voting system in Norway. The nature of a pilot is that it is used as a learning exercise. While it is hoped that the system piloted comes close to meeting all of its requirements, and certainly has to meet minimum standards, the purpose of a pilot is to learn lessons and improve the system. Areas of improvement have been identified by the pilot process, and not solely related to the issues identified in this assessment.

In this context, findings of non-compliance need not be seen as a failure of the Internet voting system. Certainly some of the issues raised by this assessment are very important for the integrity of the electoral process, but the issues identified were small in impact (as with the nine invalid ballots) or were part of an issue which was largely well dealt with but could still see some improvement (as with the access to information and transparency issues). In fact, many of the issues identified in this assessment would be relatively easy to remedy in any future implementation of Internet voting in Norway. The one technical issue identified, invalid ballots, already has a solution identified, which the Ministry has tested and believes will resolve the problem in the future.

The use of remote Internet voting from uncontrolled environments will always present challenges when it comes to issues such as secrecy and freedom of the vote. Voting from uncontrolled environments, including postal voting, can never provide the same protection for these principles as paper voting from controlled environments. However, it must be recognised that the use of Internet voting, and other forms of electronic voting, can help elections better achieve other basic international electoral standards, such as providing better access to voters in general and especially voters with disabilities (who may actually be able to vote unassisted, and secretly, with electronic voting).

It is important to note, in this regard, that every election system represents a country specific attempt to balance the range of different electoral standards. It is sometimes the case that the better achievement of one standard can only be achieved at the expense of others, secrecy and transparency being a good example. Each country and election administration body will need to find the most appropriate balance of these standards given the country's electoral, political, social and legal environment.

References

Caarls, S. (2010) E-voting Handbook: Key steps in the implementation of e-enabled elections, Council of Europe Publishing: Strasbourg

Carter Center (2007) Developing a Methodology for Observing Electronic Voting, see http://www.cartercenter.org/documents/elec_voting_oct11_07.pdf [last accessed May 9, 2012]

Council of Europe (2004) Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and Explanatory Memorandum, at http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/Key_Documents/Rec percent282004 percent2911_Eng_Evoting_and_Expl_Memo_en.pdf [last accessed November 3, 2011]

Council of Europe (2011a) Certification of e-voting systems: Guidelines for developing processes that confirm compliance with prescribed requirements and standards, Council of Europe's Directorate of Democratic Institutions, "Good Governance in the Information Society" Project

Council of Europe (2011b) Guidelines transparency of e-enabled elections, Council of Europe's Directorate of Democratic Institutions, "Good Governance in the Information Society" Project

European Commission (2006) Methodological Guide to Electoral Assistance, see http://ec.europa.eu/europeaid/multimedia/publications/documents/thematic/ec_methodological_guide_on_electoral_assistance_en.pdf [last accessed May 9, 2012]

OAS (2010) Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions, General Secretariat of the Organization of American States (GS/OAS), see www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf [last accessed May 9, 2012]

OSCE (2005) Challenges of Election Technologies and Procedures: Final Report, Supplementary Human Dimension Meeting, PC.SHDM.GAL/5/05

OSCE (2008) OSCE/ODIHR Discussion Paper in Preparation of Guidelines for the Observation of Electronic Elections, ODIHR.GAL/73/08

Pran, V. and Merloe, P. (2007) Monitoring Electronic Technologies in Electoral Processes: An NDI Guide for Political Parties and Civic Organizations, National Democratic Institute for International Affairs, see http://www.ndi.org/files/2267_elections_manuals_monitoringtech-preface_0.pdf [last accessed May 9, 2012]

Signe Bock Segaard, S. B. and Saglie, J. (2012) Evaluering av forsøket med e-valg 2011: Tilgjengelighet for velgere, tillit, hemmelig valg og valgdeltagelse, Institutt for Samfunnsforskning, Oslo

Smith, E. (2011) "Secret Electronic Elections?", provided to the Ministry as a legal opinion on the Internet voting project. The paper was further developed and published in the law review Lov og Rett, Vol 49(6), page 307-323

Tjøstheim, I. and Fuglerud, K. S. (2011) “Easy E-voting?”, at http://www.forskning.no/artikler/2011/september/298728 [last accessed January 11, 2012]

U.S. Election Assistance Commission’s (2005) Voluntary Voting System Guidelines (http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx [last accessed May 9, 2012]

Venice Commission (2004) Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe, Strasbourg: European Commission of Democracy Through Law, at www.venice.coe.int/docs/2004/CDL-AD percent282004 percent29012-e.asp [last accessed October 28, 2011]

Annex – Assessment of Council of Europe Recommendations

Appendix I

Legal standards

A. Principles

I. Universal suffrage

FC / 1. The voter interface of an e-voting system shall be understandable and easily usable.

The explanatory memorandum elaborates on this recommendation, saying that it is not possible for a voting system to be understandable and usable for every voter, but there is a requirement that "the voter interfaces of e-voting systems are usable and understandable by as many people as possible."

This assessment did not include a specific evaluation of the usability and ease of use of the Norwegian Internet voting system, but these issues were covered by other aspects of the evaluation of the Internet voting system. A representative survey from the 10 pilot municipalities conducted by the Institute for Social Research (ISF) as part of this broader evaluation asked Internet voters the reasons why they voted over the Internet. Of the 891 respondents, 95 percent indicated that a 'very' or 'somewhat' important reason for using Internet voting was that 'it was an easy way to vote' (Segaard and Saglee 2012: 68).

Exploring this finding further, the survey asked Internet voters about the ease of use of different aspects of the Internet voting system. The percentage of respondents who found the following aspects of the system to be 'very' or 'somewhat' easy to use are as follows: understanding which passwords and pin codes to use – 97 percent; entering passwords and pin codes – 99 percent; casting your vote – 100 percent; and, understanding what the return code received by SMS meant – 99 percent[72] (Segaard and Saglee 2012: 69).

These findings make it clear that Internet voters found the system easy to use and understandable.

The Norwegian Internet voting system complies with this recommendation.

FC / 2. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.

The Norwegian Internet voting system allows three authentication mechanisms for Internet voting: MinID, BuyPass and Commfides. These three mechanisms are multipurpose authentication mechanisms, and are used both for this Internet voting trial and for other goals, namely for accessing different public and private services.

All citizens of voting age have an online MinID account allocated to them, but not all have activated it. The activation of the online MinID account, the most widely used authentication channel, is relatively simple. MinID and the other authentication mechanisms all require that a mobile phone number be

[72] There were fewer respondents to this question as not all Internet voters actually checked their return code.

recorded for the voter. This does not present a significant impediment to the use of Internet voting taking into account the penetration rate of mobile phones in Norway. BuyPass and Commfides also include additional procedural steps to complete the registration, but again not to the extent of being an impediment to the voter.

The Norwegian Internet voting system complies with this recommendation.

FC / 3. E-voting systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities.

The explanatory memorandum recognizes that using electronic voting solutions may not be practical for all voters with disabilities, but where electronic voting systems are implemented they should maximize the potential for accessibility for such voters. As part of the ISF evaluation of the Norwegian Internet voting system, the Norwegian Computing Centre observed 30 voters with disabilities casting their votes for municipal and county elections on a copy of the Internet voting application[73]. On one ballot they were required to also cast personal votes for candidates. Participants were interviewed after they had cast these votes to evaluate their experience of using the Norwegian Internet voting system.

The research indicated that as a group these voters did experience challenges in using the Norwegian Internet voting system. Voters with disabilities experienced difficulties in updating Java on their computers, logging on to the Internet voting solution, screen contrast, problems with font size and magnification and difficulties in casting personal votes. Some users also found that the Internet voting system was not compatible with the assistive technology used by voters with disabilities (such as screen readers), and they were not able to vote by Internet.

However, these difficulties need to be put in the perspective of these voters' interactions with the paper balloting process at polling stations. Some of these voters experienced significant challenges in voting in polling stations. They often have to vote with assistance, meaning that the secrecy of their vote is compromised; they need to secure transportation to the polling station and often need assistance to get into the polling station.

Overall, the majority of respondents in the survey of voters with disabilities was positive about the use of Internet voting and supported the use of Internet voting in the future. Voters with disabilities were especially appreciative of the sense of control, dignity and independence that voting over the Internet provided them (Segaard and Saglee 2012: 139-140). The research conducted by ISF and the Norwegian Computing Centre did indicate, however, that there are still improvements that can be made to the Norwegian Internet voting system relating to usability for voters with disabilities.

The Norwegian Internet voting system complies with this recommendation.

FC / 4. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

[73] It is important to note that they did not observe their actual votes being cast; the votes observed were cast on a copy of the Internet voting application for the purposes of the study only.

Internet voting was only used as a supplementary and optional channel of voting for the pilots in the Norwegian local government elections. There is no indication that the Norwegian approach will change to Internet voting in this respect.

The Norwegian Internet voting system complies with this recommendation.

II. Equal suffrage

FC / 5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box.

It may seem that the ability to cast repeat Internet votes means that the Norwegian system is not compliant with this recommendation. However, the explanatory memorandum makes it clear that this recommendation does not preclude the casting of repeat ballots by the voter if they are allowed to do so, and mechanisms are in place to ensure that only one of the ballots is included in the count. The Norwegian system does ensure that only one vote for a voter is counted. While a literal interpretation of the wording of the recommendation would seem to indicate non compliance with this recommendation, the explanatory memorandum makes a more liberal interpretation applicable. Norway complies with this more liberal interpretation of the recommendation because it ensures that only one vote per voter is counted.

The second sentence of the recommendation would also seem to be problematic for the Norwegian Internet voting system, due to the possibility of repeat voting. However, using the same argument based on the explanatory memorandum it is clear that as only one vote per voter is counted, the system complies with the recommendation.

The Norwegian Internet voting system complies with this recommendation.

FC / 6. The e-voting system shall prevent any voter from casting a vote by more than one voting channel.

As in recommendation 5, the literal reading of the recommendation would seem to entail a conclusion that the Norwegian Internet voting system is not in compliance as it allows Internet votes to be cast as well as paper votes. Using the same reasoning as recommendation 5 though, as long as only one of these votes is counted then the system is in compliance. This is the case with the Norwegian Internet voting system – the latest Internet vote is counted, or a paper ballot if one was cast.

The Norwegian Internet voting system complies with this recommendation.

FC / 7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.

Again a teleological approach is required to properly assess this recommendation. The explanatory memorandum adds little of substance to interpret this recommendation, and therefore an initial analysis would have to find the Norwegian Internet voting system not in compliance as not every vote deposited in the electronic ballot box is counted. Votes are 'cleansed' from the ballot box during the counting process if a subsequent Internet vote was cast by the same voter or if a paper ballot was cast by the voter, and these votes are not counted in the results.

However, reference must be made to recommendations 5 and 6, and the fact that casting multiple ballots is permissible as long as only one ballot for each voter is counted. Therefore, it is appropriate that not every vote which is deposited in the ballot box is counted in the Norwegian Internet voting system, as this is exactly what is required by recommendations 5 and 6.

So the fact that repeat votes can be submitted by voters does not entail non compliance with this recommendation as long as only one of them is counted. The recommendation also requires that all of the remaining votes are included in the count. This aspect of the recommendation is ensured through the E2E verification mechanisms that are put in place for the Norwegian Internet voting system and prove that each vote that is deposited in the ballot box is either cleansed (due to the reasons above) or continues through the counting process unaltered and is included in the results. More details of these E2E verification mechanisms can be found in the audit section (recommendations 100 to 111).

The Norwegian Internet voting system complies with this recommendation.

PC / 8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.

While some tasks are carried out locally (e.g. marking the roll with people using paper votes, publication of the final results etc.), others are conducted centrally (e.g. the counting of Internet votes). Legally speaking, the Ministry is only a technical facilitator as the final responsibility for elections rests with each municipal electoral committee. The coordination of central and local election administration bodies is clearly defined in electoral regulations and the Ministry's Election Manual, but obviously its implementation can face problems especially where new systems are being used.

Internet voting was not the only new system in use for the 2011 local elections in Norway, the pilot municipalities were also trialing a new election management system. In one pilot municipality the final results issued for the county election, Finnmark county, were subsequently found to have not included the Internet votes cast in Hammerfest municipality. This was due to a human error in the Finnmark County administration.[74] However, control procedures in the county picked up this omission and the final results were subsequently changed to include these votes on October 4, 2011. This resulted in a change in the distribution of seats between the Labor party and the Sami People's Party.

While the mistake was eventually discovered and corrected, this error represents a partial failure to ensure that a reliable method existed to aggregate all votes in the election and calculate the correct results.

[74] Email from the Ministry, dated October 21, 2011.

The Norwegian Internet voting system partially complies with this recommendation.

III. Free suffrage

FC / 9. The organization of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.

Internet voting itself, when used in uncontrolled environments, cannot completely avoid undue influence and coercion of the voter. Given that the voter will vote within private areas (e.g. at home), any Internet voting system should foresee this drawback and implement mitigating measures. The explanatory memorandum also assumes such a problem: "where remote e-voting channels are provided, special attention has to be given to the provision of facilities that allow the voter to exercise the right to cast a vote in a supervised environment."

In the Norwegian case, the voter can cancel an Internet vote with another one. Moreover, any paper ballot, whether postal or not, supersedes an Internet vote even when the former is cast before the Internet vote. Such flexibility might be a good measure against family voting since voters could easily accept the coercion when voting through Internet because they know that this ballot will never be counted and that they can cast another Internet ballot later. Therefore the deployment of unsupervised voting channels may not enhance family voting provided the repeat voting option is included.

However, if the coercion of the voter occurs during the final minutes of the Internet voting period, then voters will have no chance to revote by Internet means. They may have already voted by paper means, but even if this is not the case there is still the opportunity to go to the polling station and use a paper-based procedure. However, family voting has strong social and cultural roots that cannot be totally addressed by IT means. In some neighborhoods, it will be extremely difficult to freely cast a paper ballot since, as stated by Prof. Eivind Smith, "(other) members of the social structure that is the source of the problem would easily be able to discover and report attendance at a polling station" (Smith 2011: 12). Therefore, in such cases, paper ballots, even when cast in different constituencies, would not completely guarantee the freedom of vote. Voters could prefer not to cast a paper ballots because the coercer will know that s/he is attempting to supersede the Internet vote.

Whereas these previous concerns should be taken into account by Internet voting developers, it is worth recalling that traditional paper based procedures also face similar risks. First of all, postal voting, which is accepted for Norwegians living abroad, can also be submitted to undue influences and it does not include the cancellation options already seen for Internet voting. Moreover, the Venice Commission's report on remote voting makes a comparison between postal and Internet voting concluding that, if some conditions are accepted, both channels may comply with the Council of Europe's standards. Second, we should not forget that cellular phones also allow the possibility for undue influence even using voting booths as vote coercers can require that voters take a photo of their ballot. Western democracies seem relatively unconcerned about these issues. Even if it may theoretically happen, the amount and political significance of these pressures have not generated complaints so far.

Unsupervised voting channels cannot exclude the possibility of undue influence being exercised over the voter, as also happens with postal voting. However, some additional features of the Norwegian Internet voting system, which are not foreseen for postal voting, like repeat voting and the supremacy of paper ballots, weaken these pressures. If we introduce more voting channels, we simultaneously weaken the chances for coercers because we are multiplying the options for the voter.

Legally speaking, the fact that postal voting is only admitted for Norwegians abroad during elections has no impact because theoretically every voter should be granted voting rights with the same level of legal guarantees. If a Norwegian living abroad may accept a voting channel that is clearly less protected than a polling station environment, there is no reason not to implement another remote voting channel that with similar or better chances to fight against undue influences.

The Norwegian Internet voting system complies with this recommendation.

FC / 10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.

The Explanatory Memorandum provides little additional guidance to help interpret this recommendation. The Norwegian Internet voting system requires voters to select their voting options and then to confirm that these selections are correct before the vote is cast. This confirmation process seems to be sufficient to ensure that Internet ballots are not prematurely cast by voters. Additionally, the possibility for repeat voting, whether by Internet or paper, means that there is always the possibility for the Internet voter to subsequently change their vote if they vote without adequate reflection.

The Norwegian Internet voting system complies with this recommendation.

FC / 11. Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.

The Norwegian Internet voting system allows voters to alter their choices as many times as they wish to do so before confirming their choices and submitting their ballots (although they must complete their voting choices in 30 minutes as the voting session times out after 30 minutes). Voters may also cancel their voting session at any point, before casting any or all of the ballots available to them.

Any options made by voters, but not confirmed through the voting application are not sent to the voting server, and therefore not recorded on the server. However, as voters cast ballots from PCs in uncontrolled environments, it is possible for these PCs to record in some way the content of a voting session. The Ministry stated that it had considered implementing a technical solution which would try to mitigate this potential threat to the secrecy of the vote. However, this solution was only available on one operating system/web browser combination and conflicted with mechanisms to make Internet voting accessible for blind and visually impaired voters.

This apparent non compliance with the recommendation needs to be considered in the context of the possibility for casting repeat Internet votes. See the discussion below on recommendations 16-19 for an assessment of the ways in which repeat voting mitigates the challenges of the secrecy of the vote with Internet voting.

Due to the possibility for repeat voting and the casting of a paper ballot, it will never be possible to know if a vote cast through a voting session which was recorded by a PC was the one that was included in the count. Because of this possibility for repeat and paper voting, the secrecy of the vote is not seen to be violated as only the voter knows the content of the ballot which is included in the count.

The Norwegian Internet voting system complies with this recommendation.

FC / 12. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.

The explanatory memorandum elaborates on this recommendation, indicating that the e-voting system should be designed to exclude all forms of manipulative influence, and that this is targeted at computerized manipulative influences, such as sounds associated with the candidate and pop-up screens.

Compliance with this recommendation is again a challenge for voting from uncontrolled environments, environments in which any activity could be taking place during the casting of a vote. However, the recommendation and the explanatory memorandum talk about the ‘design of the e-voting system’, which can be seen to limit the environment that is being discussed to that present on the device being used to vote (most likely a PC), and not the more general environment in which voting takes place in uncontrolled environments.

There are two components to the environment on the PC used for voting, the voting software developed for the Ministry and the environment provided by the PC. The voting software provided by the Ministry for Internet voting does not provide any of the manipulative influences discussed by the memorandum, and therefore present a neutral environment in which the voter can cast a vote. In fact, even the order of the party lists presented to the voter through the Internet voting system are randomized so that no party benefits from always being presented at the top of the list of options.

The PC environment is a different matter. The Ministry and the voting applet have no control over this environment, and there would be little that could be done to stop messages being displayed to voters by the PC as the voter was casting a vote. The impossibility of controlling this PC environment and ensuring that such manipulative influences are not present may lead to concluding that the Norwegian Internet voting system is not compliant with this recommendation.

However, again a more contextual assessment is appropriate. The recommendation and explanatory memorandum are not clear about whether this recommendation relates to only the voting applet or the more general voting environment on the PC from which the vote is cast. Given the uncertainty over how to interpret this recommendation and the differing conclusions to be reached from these interpretations, this assessment assumes the interpretation leading to compliance. This interpretation is also consistent with Venice Commission findings on the compliance of Internet voting with international electoral standards (Venice Commission 2004), which must inherently assume that these environments cannot be fully excluded from manipulative influences.

The Norwegian Internet voting system complies with this recommendation.

FC / 13. The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.

The Norwegian Internet voting system allows for the possibility for voters to cast a blank ballot.

The Norwegian Internet voting system complies with this recommendation.

NC / 14. The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.

Once the voter has confirmed their vote choices the vote application submits the vote to the vote server. This involves a number of steps, during which the voter is informed that the vote is being processed. First the vote received by the vote server is re-encrypted and passed to the RCG. The RCG checks the re-encryption, sends a return code to the voter's mobile phone and stores a hash of the re-encrypted vote. When the RCG has done this it informs the vote server that it has sent the return code and the vote server stores the vote. The voting application then informs the voter that the vote has been cast. The return code acts as an additional confirmation to the voter that the vote has been received as cast.

This process makes it clear to the voter that the vote has been cast and received by the vote server.

However, there were a number of Internet votes cast which were invalid (9 votes) or rejected (1 vote). In the case of the invalid votes, the recorded preferences were invalid because more than one vote was recorded for a party list. Scytl, the Internet voting solution provider, investigated how such invalid ballot choices were possible and concluded that it could either have been a successful attempt to manipulate the system or an error in the voting applet allowing invalid choices to be submitted. The rejected ballot was received just before the end of the 30 minute voting session time limit, but so close to the end that it was processed just after the end of the 30 minute period and was rejected during the cleansing phase of the counting process.

In both cases voters casting these ballots received a return code and were informed by the voting application that their votes had been successfully submitted.

Despite the small number of ballots involved, the extemporaneous ballot clearly represents a failure to comply with the recommendation because the system wrongly informed the voter that his/her vote had been successfully cast. Moreover, if we understand the recommendation as requiring both a time confirmation and a proper substantial casting of a ballot, then the nine invalid ballots would also fail to comply with this recommendation.

Therefore, the Norwegian Internet voting system does not comply with this recommendation.

FC / 15. The e-voting system shall prevent the changing of a vote once that vote has been cast.

Given that the Norwegian Internet voting systems allows repeat voting, this requirement should be seen as referring to the prevention of changes made to stored votes. Completely eliminating any possibility for stored vote values to be changed is not feasible. Administrators of the Internet voting process require access to the system in order to manage it.

The Norwegian Internet voting system has procedural and security controls to mitigate any attempts to alter stored vote data. More importantly it employs E2E verification mechanisms so that any manipulation of vote data can be identified. The Internet voting system used a series of zero knowledge proofs and other checks for different stages of the procedure and employed an independent contractor to check that ballots passed through the counting process unaltered.

Therefore, the Norwegian Internet voting system complies with this recommendation.

IV. Secret suffrage

FC / 16. E-voting shall be organized in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.

This requirement generally refers to the principle of secrecy and the following recommendations split the principle into different aspects. The explanatory memorandum also includes a general reference to secrecy encompassing all the voting procedures.

However, authentication is specifically mentioned in this recommendation. Given the remote and unsupervised nature of the Norwegian system, any authentication scheme must simultaneously send to the relevant servers both the voter's ID and the vote's value. Linking both data may only be avoided by computerized means and should be analyzed within the audit / certification procedure.

Finally, an uncontrolled environment always entails a risk for the secrecy of the vote because undue influences could force the citizen to reveal the content of his/her vote. Repeat votes and the supremacy of any paper ballot cast intend to overcome this problem. Please see comments on recommendation 9 for further assessment of this issue.

The Norwegian Internet voting system complies with this recommendation.

FC / 17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.

Encrypted ballots are stored using a double envelope strategy similar to that used for postal voting. The outer envelope consists of the voter’s digital signature for the ballot, with the inner envelope being the encrypted vote. The outer envelope, with the ID credentials, is removed during the cleansing stage of the counting process. Ballots are then mixed, to make it impossible to determine the identity of the voter due to the order in which ballots are stored. The inner envelope, with the vote's value, is then decrypted at the final stage of counting where results are tabulated.

This schema is similar to the one used by other Internet voting projects, but the Norwegian system includes an additional feature consisting in return codes that intend to provide individual verifiability. Each eligible voter is receiving a polling card that links each candidature with a code. The set of codes for the candidates is different for each eligible voter. Such codes entail a link between voters' ID and a code representing vote values. In principle then, there is a link between the voter's ID and the value of the vote through the return code. However, the possibility for repeat Internet voting and for the casting of a paper ballot at any time during the voting period mean that only the voter will know if a specific return code represents the vote that will be counted.

The set of return codes is also a concern, as the generation of these codes requires that a link be made between the voter ID and the return codes in order to print them. The return codes are generated before the election through a computerized protocol that links the voter's ID with his/her codes for each candidature. If this link is not broken afterwards, the servers that collect the vote and send back the return codes would be able to disclose the identity of a single voter and link it to a vote. According to the explanations received from the Ministry, the generation of codes is conceived as a highly critical step and different physical and organizational measures are established to ensure that once these codes are generated, the link between the voter ID and return codes cannot be accessed.

Finally, it may seem that the Internet voting system must maintain the link between the voter and value of the vote in order to be able to send the return code to the voter. However, the design of the system ensures that this link is not possible. While the VCS has the ID of the voter and the encrypted vote value, it re-encrypts the vote before passing it to the RCG. The RCG uses the re-encrypted vote to generate the return code and it does so without knowing the value of the vote, just that the re-encrypted value X results in a return code value of Y.

The Norwegian Internet voting system complies with this recommendation.

FC / 18. The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.

According to the explanations provided by the Ministry, "if there were less than 20 e-votes in an electoral area, then these e-votes are added to the second smallest electoral area, and then the third smallest electoral area, until you'd reach at least 20 votes. These e-votes would then be marked as belonging to 'Area 0000', to avoid that a one of the electoral areas will be registered with more e-votes than it actually had."

This solution does not completely solve the problem since, if we are dealing with municipal elections, merging electoral areas would only be feasible within the same municipality and it is possible to imagine a small municipality with only one electoral area and a small number of voters. However, Internet voting does not seem to increase the problems that already exist in this regard with traditional paper based voting.

The Norwegian Internet voting system complies with this recommendation.

FC / 19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

As already mentioned, the order of the ballots will be randomized at the end of the voting period and meanwhile the votes are encrypted.

Return codes obviously require information on the voter and the value of the vote, but this concern has already been discussed in the assessment of recommendation 17.

The Norwegian Internet voting system complies with this recommendation.

B. Procedural safeguards

I. Transparency

FC / 20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.

If we interpret “understand . . . the e-voting system” as the ability to perceive and monitor the technical functionality of the voting system, it is quite evident that probably no electronic voting systems would be able to meet the recommendation. The German Constitutional Court decision (BVerfG, 2 BvC 3/07, March 3rd 2009) found German electronic voting machines, which did not have a voter verified paper audit trail, as failing to meet the constitutional requirement for all citizens to be able to understand and supervise the voting process, without the need for specialised technical knowledge.[75]

On the other hand, if we assume that “understand” refers not to the core technical details, discussion about the compliance remains open. “Understand” might refer to those organizational measures that could be analyzed by an average voter and that are conceived to create enough confidence in the electronic voting system. To understand everything would not be a goal in itself, to understand would only be a path to generate sufficient confidence in the system. This confidence need not be a result of personal knowledge and understanding of the technical details of the voting system, but could be based on an understanding of the oversight mechanisms and trust in the competence and integrity of those providing this oversight function.

The explanatory memorandum seems to accept this second position when it mentions that, regarding e-voting procedures, “voters will be less familiar with the electoral process and perhaps less able to understand the safeguards built into the e-voting system.” Such a mention to both the system and the safeguards seems to be linked to the concept of procedural trust, that is to say, a confidence that is not based on direct supervision by the voter. It could be based on an assessment of how the voting system is managed, the oversight mechanisms provided and the trust placed in the institutions providing that

[75] § 109 - *jeder Bürger muss die zentralen Schritte der Wahl ohne besondere technische Vorkenntnisse zuverlässig nachvollziehen und verstehen können* (translation: each citizen would have to be able to understand and supervise main electoral phases without a specialized technical knowledge); similarly stated at § 119, 148 and 149.

oversight. Moreover, the last paragraph of the memorandum seems to strengthen this approach with the following statement: "Confidence can be enhanced by providing voters with as much information as possible about the method of e-voting being used." Information, and perhaps not a direct supervision, might be enough for a voter to become confident as he understands how Internet voting is organized.

The analysis of this recommendation assumes this second meaning of "understand" and assesses whether the Norwegian voting system is transparent enough to provide to the voter the relevant data that s/he needs to enhance electoral confidence.

It is worth stating that confidence is a subjective perception that cannot be evaluated by theoretical means and that a survey would be required to determine levels of confidence. What can be analyzed theoretically are the measures undertaken by the government in order to enhance public confidence. The Ministry has disclosed the source code, implemented E2E verifiable mechanisms and published all relevant documentation on the Internet voting system. Clear regulations regarding audit mechanisms and proactive involvement of other key stakeholders have also helped to provide a high level of transparency.

Finally, it should be noted that the recommendation indicates that Member states shall not ensure, but only take steps to ensure this goal. Although not completely clear, this wording might have intended to include a nuance weakening the commitments endorsed to Member states.

The implementation of the Norwegian Internet voting system has taken many significant steps to ensure that voters understand and have confidence in the system.

The Norwegian Internet voting system complies with this recommendation.

PC / 21. Information on the functioning of an e-voting system shall be made publicly available.

Transparency has been a guiding principle in the Ministry's implementation of the Internet voting system. The Ministry's website has many pages with information on the Internet voting project. This includes technical documentation, including the source code for the voting system, as well as presentations on the features of the Internet voting system.

While all relevant information seems to have been publicly available, timing constraints led to some limitations in the availability of this information. The first version of the source code was published on the Ministry's website on June 7, 2012, and the Ministry made it clear that there may be updates to this version. Updates were in fact made subsequent to this as bug fixes were made to the system. Crucially, the final version of the source code was not made available on the website until October 7, 2012, nearly one month after the election. The Ministry indicated that anyone who wanted to see the final version of the source code before it was posted online would have been provided access, but many would have expected the version on the website at the time of the election to be the final version.

The source code is a vital component of the information related to the functioning of the Internet voting system. There is no indication that the failure to publish this information prior to the election was an attempt to mislead stakeholders in any way. In fact, the Ministry made significant efforts to provide as much access to information as possible. The complexity of the Internet voting system and late changes that had to be made to it meant that the Ministry was focused on making the election happen at the expense of immediately publishing the new version of the source code.

Nevertheless, the failure to have the source code published represented a failure to provide key information on the system in a timely manner and provide those stakeholders with an opportunity to review this key information before the election took place.

The Norwegian Internet voting system is partially compliant with this recommendation.

PC / 22. Voters shall be provided with an opportunity to practice any new method of e-voting before, and separately from, the moment of casting an electronic vote.

The Ministry provided a number of opportunities for voters to test the Internet voting system before they used it in the local government elections. The Internet voting system was used in trial ballots in each of the pilot municipalities in the 12 months preceding the local government elections. These ballots were for youth councils and for local consultations. Not all of the features of the Internet voting system were available in earlier trials, but later trials used the full functionality of the Internet voting system, including return codes. Obviously not all voters in the pilot municipalities would be eligible to participate in youth council elections. However, voters in the pilot municipalities were also provided the opportunity to experiment with the Internet voting platform through a test Internet voting website established by the Ministry. This website was an authentic copy of the actual Internet voting website, including the use of third party authentication mechanisms (such as MinID) and return codes, and was available from July 20 to August 1.[76]

In addition to the general requirement to provide opportunities to practice the use of Internet voting, the explanatory memorandum indicates that "special attention should be paid to any voters who are not familiar with the e-voting method, for example the elderly." It does not appear that the Ministry made any special efforts to familiarize such voters with the Internet voting system.

In view of this omission, the Norwegian Internet voting system is found to be only partially compliant with this recommendation.

FC / 23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.

A number of points concerning this recommendation are worth making at the outset. This recommendation only requires that the legal framework allow observers to observe and comment on the e-elections, and does not require that such observation take place. Therefore the failure of any observers to monitor an e-election would not result in a failure to meet this obligation as long as any interested observers were able to observe and comment if they had chosen to do so. This is relevant for the Norwegian Internet voting pilots as there were no domestic observation organizations accredited for

[76] The test website did not have the proper political party names.

the 2011 local government elections. While the OSCE did observe certain aspects of the Internet voting pilots, they were not present for all stages of the process.

The explanatory memorandum for this recommendation indicates that clear legal provisions on observer access to e-voting documentation and access to software should be provided for, as well as the viewing of electronic and physical security measures, and observation of the entry of votes into the electronic ballot box. The Ministry's Regulations Relating to Trial Electronic Voting make no special provisions for observation of the Internet voting process. However, the general provisions of the Election Law also apply to Internet voting unless otherwise stated. The Ministry's Election Manual, which elaborates on Chapter 15-10 of the Election Act, discusses the general provisions relating to the role of observers in elections. The Manual states that, "The electoral authorities ... shall for their part ensure that the observers have unrestricted access to all stages of the electoral process. They shall also have the possibility of assessing the part of the election that proceeds electronically, use of new technology etc" (page 106).

Therefore, it is clear from the general provisions of the Election Law that observers are able to be present to observe all aspects of the electoral process, including the Internet voting process. In fact, the Ministry made additional efforts to enable observation of election activities related to Internet voting, inviting the OSCE to monitor the printing of polling cards and return codes. It also conducted a special event for the cleansing, mixing, decryption and tallying of Internet votes at the end of polling, to which many stakeholders were invited.

The Norwegian Internet voting system complies with this recommendation.

II. Verifiability and accountability

PC / 24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.

The Ministry required the full disclosure of the source code in the Regulations Relating to Trial Electronic Voting (art. 28.2) and it also uploaded to the website the documentation generated during the tender, including the technical specifications presented by the suppliers. The regulation also foresees the publication of "the requirements relating to the solution (infrastructure, servers, data in the system, procedures, guidelines for deleting return codes, roles, access, technical documentation, testing, time plans, security copying procedures, etc.)" (art. 27.1) as well as the "documentation relating to how the system has been built up and how it works, including detailed specifications and architectural documents" (art. 28.1).

However, some technical components, like the authentication mechanisms, remain outside the scope of this policy as they are managed by other institutions that did not disclose details of their systems to the Ministry. This recommendation could be considered as having been met if we considered the authentication mechanisms as not being "components of the voting system." However, as the authentication of voters is an inherent and critical component of the Internet voting system, this option does not seem acceptable.

The failure to provide access to the components of these authentication mechanisms does need to be contextualized. The other Ministries and agencies responsible for the authentication mechanisms, MinID, BuyPass and Commfides, are all subject to regulation and are audited on a regular basis. Therefore, while the components of these systems are not made available to the competent electoral authorities, as required by the recommendation, they are subject to oversight.

The Norwegian Internet voting system partially complies with this recommendation.

N/A / 25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.

According to the Regulations Related to Trial Electronic Voting (art. 27.5), this recommendation is not applicable.

FC / 26. There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.

A recount is always possible in any Internet voting system, but it has limited value if conducted by the same organization and with the same means as the previous count. Such a count does not achieve the main goal of this recommendation, to verify the correctness of the vote tally. The Norwegian solution intends to overcome this barrier by the means of E2E verification of the process. As foreseen by article 27.3 of the Regulations Related to Trial Electronic Voting, “the system shall enable independent third parties to verify the integrity of the election by using cryptographic proofs.”

The E2E verification mechanisms implemented allow a complete software independent assessment of the various stages of the vote counting process. However, such independent verification relies on specialized technical knowledge and expertise. Once an average voter cannot verify him or herself, the correctness of the results, the legitimacy and public confidence depend on the transparency mechanism and the involvement of relevant stakeholders. If anyone with computer knowledge can completely verify the voting platform and conduct a second recount with his/her own means, as the Norwegian case claims to allow, then this will significantly enhance citizen confidence and the legitimacy of the system.

In fact, no independent organization did conduct such a verification of the results. Promis AS conducted a verification of each stage of the processing of Internet ballots, but this was funded by the Ministry and therefore its independence could be questioned. Nevertheless, the fact that no organization took up this opportunity to independently conduct this verification function does not mean that the recommendation has not been complied with. The recommendation only requires that the possibility for recount exists and that other features influencing correctness of the results be verifiable. This is the case with the Norwegian Internet voting system.

The Norwegian Internet voting system complies with this recommendation.

FC / 27. The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.

The Norwegian Internet voting system does not have any design features which would prevent the partial or complete re-run of an election or referendum, either by Internet voting again or by paper balloting.

The Norwegian Internet voting system complies with this recommendation.

III. Reliability and security

FC / 28. The member state's authorities shall ensure the reliability and security of the e-voting system.

The explanatory memorandum states that e-voting measures should be as reliable and secure as paper-based ones and that election management bodies should not avoid their responsibilities by giving a disproportional role to private suppliers. It is difficult to objectively compare the reliability and security of Internet voting systems vis-à-vis paper balloting systems, as the different systems face different kinds of threats to their security and issues with reliability. It must also be understood that paper balloting entails issues with respect to reliability and security.

In terms of the reliability of the Norwegian Internet voting system, it is worth noting that there were two data centres actually established for the VCS and two data centres established for the RCG to ensure a back-up in case one server experienced problems. Having two data centres for the VCS and RCG updated in real time, when a single data centre could have managed the anticipated load by itself, ensured that a significant level of protection was provided for the reliability of the service.

In terms of the security of the Norwegian Internet voting system, the list of measures includes at least the following ones:

- The VCS and RCG servers were located on different servers in different Ministries, 700 miles apart, making it more difficult to manipulate data. Such manipulation would have to be conducted on both servers to be consistent (differences in the content of the two servers would be apparent through the E2E verification mechanisms implemented)
- Both servers were under constant video surveillance
- The Ministry had no direct access to the VCS and RCG servers during Internet voting, both being located at other Ministries
- All access to the VCS and the RCG was authorized personally by the Chief Security Officer for the E-Vote Project
- All transactions on the VCS and RCG were logged, the log for voter authentication mechanisms was held in external locations (depending on which authentication mechanism was used)
- The Ministry employed a commercial application for analysis and monitoring of the transaction logs on the different servers

- The logs that were generated were immutable, which means that they were protected from tampering and erroneous insertion of entries. This was achieved by each entry in the transaction log containing a hash of the entire previous entry in the transaction log
- The Ministry established and monitored a separate dashboard which checked for attacks on the Internet voting system. Not only were attacks on the application itself monitored, but also attacks on the infrastructure of the system. This dashboard was capable of sending alerts if serious attacks were detected

In terms of the suppliers' roles, it seems clear that final legal responsibility is assumed by the electoral authorities. The Regulations Relating to Trial Electronic Voting emphasize this in the section entitled "Ownership and operational responsibility." This section states that "the e-election system and the electronic election computer system are owned, operated and administered by the Norwegian state" (art. 26).

Taking into consideration all of the issues and measures listed above, it can be seen that the Ministry has implemented many measures to ensure that the Norwegian Internet voting system is reliable and secure, and that these measures have done much to ensure that a high level of reliability and security has been achieved with the system. However, a computer-based assessment would be needed to obtain a more definitive assessment of such security and reliability issues.

As far as can be determined by the assessment team, the Norwegian Internet voting system complies with this recommendation.

FC / 29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.

Although the wording is very compelling, the explanatory memorandum adds nuances to this requirement by admitting trade-offs between security measures and other key items such as usability. Consequently this general recommendation is only requiring that appropriate measures be taken to mitigate the risks of fraud and unauthorized intervention.

According to the data provided by the Ministry, "risk assessment was initially performed by Veritas, and this was updated regularly during the project. All risk reports was presented to the steering committee. The trade-off between security and usability was considered in the risk assessment." Again, it can be seen that the Ministry constantly monitored risks and mitigation strategies throughout the project. An IT based assessment would be needed to definitively assess whether the measures taken to mitigate fraud and unauthorized intervention in the system were sufficient.

As far as can be determined by the assessment team, the Norwegian Internet voting system complies with this recommendation.

FC / 30. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.

In evaluating this issue, the assessment made for recommendations 29 and 70 are relevant. Although recommendations 29, 30 and 70 foresee different issues, they all deal with risk assessment and mitigation strategies, which are inherently technical in nature with Internet voting systems, and would require an IT based assessment to definitively determine whether adequate measures were taken to address these issues.

As far as can be determined by the assessment team, the Norwegian Internet voting system complies with this recommendation.

FC / 31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.

The explanatory memorandum links this recommendation to the 24th, where the suppliers are asked to disclose at least those e-voting components that are necessary for verification purposes. Once this disclosure occurs, Member States are required by the current recommendation to verify that the e-voting system being used is the correct and approved one.

According to the data provided by the Ministry, "the server was already on, and the same server was used during the pre-pilots. The software was installed by the operators responsible at the *Brønnøysundsregistrene* (website: brreg.no) and DSB (website: dsb.no). Final configuration was performed by KRD [Ministry] representatives with assistance from Scytl. The production software was intensively tested before making the system available to the public . . . The installation packages were digitally signed from Ergo, so these could not be replaced."

The Norwegian Internet voting system complies with this recommendation.

PC / 32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.

Any Internet voting system should rely upon established procedures that have to be previously described in an operational manual. These procedures must identify critical steps in the management of the system and describe appropriate measures to deal with these steps. According to the data provided by the Norwegian authorities, "the sum total of all procedural steps, are covered in a numbers of documents such as project plans (high level and detailed), configuration and counting scripts, user manuals, and installation guides, backup plan."

The Ministry informed IFES of the following procedures for access to the different components of the Internet voting system:

- The BRREG (Brønnøyssundsregistrene) e-voting infrastructure, where the VCS was located, was managed by a single person (which was contrary to the specification of requirements), but this person could not physically access the servers without a second person (the person managing the administrative system) being present. This person also did not have any access to the Hardware Security Modules in the system. Access to the operator cards was controlled by the BRREG's Chief Security Officer, and access was only provided on a case-by-case basis and on the authorization of the e-vote Chief Security Officer. This procedure was applied once (on August 4, so strictly speaking before the election, when one piece of hardware was returned after warranty repairs).

- In DSB, where the RCG server was located, the teams were rotated. There were two operators who were contracted from a company called Atea. Sometimes they worked together as a team, but most of the time they worked alone, under the supervision of a DSB representative. Additionally, the DSB infrastructure was installed with the help of a representative from Scytl.
- The counting infrastructure was also managed by rotating teams. An outside contractor from Red Pill Linpro, and representatives from Scytl worked on installing the infrastructure – always under supervision by a representative of the Ministry. Later a contractor from Ergo managed the system under the supervision of a project security officer.77

While clear procedures seem to exist for the management of the Internet voting system, the fractured nature of the documentary evidence for this and the failure to publish some of this documentation makes it difficult to independently check this assertion by the Ministry.

It must be recognised that the use of Internet voting for the Norwegian local elections in 2011 was only a small pilot, and that therefore it may be reasonable to expect the procedural guarantees required by the recommendation to only be fully developed and properly documented for a full scale implementation of Internet voting. Nevertheless, the absence of coherent and collated procedural guidance for the management of the Internet voting system is an omission, although it is recognised that other aspects of the recommendation are met.

The Norwegian Internet voting system is partially compliant with this recommendation.

PC / 33. While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and any election observers.

This recommendation is seen as covering any authorized intervention during the one month period of Internet voting. The Ministry informed IFES that there had been, "one authorized system change during the voting period (on the early morning of august 31st). The upgrade was scheduled and planned well ahead (even prior to the opening of the election). It was first installed and tested in the QA environment, which resulted in a test report."

The change in the production environment was authorized and monitored by a representative of the Ministry, and performed by one representative each from the Brønnøysund Register Centre and from the Directorate for Civil Protection and Emergency Planning where the VCS and RCG were hosted.

[77] Email from the Ministry on May 2, 2012.

Details of the upgrade were recorded on the log file monitoring system, although no formal report was written concerning the upgrade.

There was no other “intervention” in the Internet voting system during the voting period. The Ministry is certain that this is the case because any system change would have required a server restart. This would both have triggered an alert to Ministry staff through the log file monitoring system and required the Ministry to re-send the passwords.[78]

While the Norwegian Internet voting system has complied with parts of this recommendation, there are significant aspects that it does not seem to have complied with. The failure to write a report on this intervention is one such issue. It could, arguably, be considered that the transaction logs for this intervention would constitute such a report.

Less debatable is the failure of the Ministry to inform observers about this intervention in the Internet voting system, and allow access to observe it. The explanatory memorandum makes it clear that such observation of the intervention should be allowed when stating that, “if election observers are allowed by domestic law, then they should have access. Security measures for telephone or Internet voting may make it necessary to prohibit the presence of observers in the computer room. In that case measures should be taken in order to give the observers the opportunity to monitor the intervention.”

On balance, it would have to be said that while some aspects of the recommendation were complied with, others were not, and therefore a finding of partial compliance is appropriate.

The Norwegian Internet voting systems partially complies with this recommendation.

NPTD / 34. The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.

The last component of this recommendation is the easiest to deal with. Votes cast through the Norwegian Internet voting system do pass through uncontrolled environments, but they are encrypted by the voting applet before being communicated to the VCS. This ensures that it is not possible for anyone to intercept and read the vote as it is communicated to the VCS.

At first glance the Norwegian case may appear to struggle to comply with the following statement included in the explanatory memorandum: “from the moment the vote is cast, no one should be able to read or change it or relate the vote to the voter who cast it.” Return codes could be seen as violating this by linking the vote value to the voter who cast it while generating the return code and sending it to the voter.

However, as discussed in recommendation 17, the design of the system ensures that this link is not possible. While the VCS has the ID of the voter and the encrypted vote value, it re-encrypts the vote before passing it to the RCG. The RCG uses the re-encrypted vote to generate the return code and it

[78] Email from the Ministry dated April 27, 2012.

does so without knowing the value of the vote, just that the re-encrypted value X results in a return code value of Y. As also previously discussed, the return code itself is not seen as a violation of the confidentiality of the vote because only the voter knows whether a specific return code relates to a vote that will be included in the count.

The first part of the recommendation concerning the integrity of the votes cast is also somewhat problematic. Subsequent to the announcement of results, but prior to the finalization of the results, Scytl reviewed the logs for the Internet voting system and discovered that of the 53,916 Internet votes which passed through the various stages of the process to be counted, nine votes could not be interpreted after decryption. These Internet votes in fact had more ballot selections than was permitted under the election rules, and therefore were not included in the count of Internet votes.

The votes were distributed amongst the various local government elections in the following manner:

Figure 7 – Distribution of Invalid Internet Votes[79]

Election	Number of Invalid Votes
Rogaland County	1
Sogn og Fjordane County	1
Møre og Romsdal County	2
Nordland County	1
Sandnes Municipality	1
Bodø	2
Hammerfest	1
Total	**9**

The generation of such invalid Internet votes should not have been possible and is indicative of a flaw in the Internet voting system.

Scytl, the supplier of the core Internet voting system, was asked to investigate how these invalid votes could have been generated. The Scytl report[80] into this issue considered several possible sources for the generation of invalid Internet votes, including:

- A configuration error when specifying or assigning the voting areas to the voters
- An attack by the same voter that cast the vote by forging a vote containing more than one selection for the same candidate or party
- An error in the applet that included the same party or candidate twice in the encrypted vote81

After exhaustive analysis, the possibility of a configuration error was discarded by Scytl, "[t]herefore, the final conclusion is that the votes were generated by including more than one selection for the same

[79] Data provided by the Ministry in email of October 21, 2011.

[80] Ergo Group/Scytl (2011) "Audit Report of the 2011 Municipal and County Council Election Results", version 0.1, October 17, 2011, provided by the Ministry in an email dated October 24, 2011.

[81] *Ibid*, p.5.

candidate due an attack or an applet error when casting the vote."[82] When considering these two possibilities Scytl concluded that:

> *Unfortunately, both cases generate the same type of invalid vote and it is not possible to distinguish which one has generated it. Furthermore, both cases occur in the voting side and therefore, are impossible to detect*.[83]

It was noted that these invalid votes had been detected as invalid during the counting process and therefore not included in the count. However, the voters who submitted these votes would have believed that a valid vote had been submitted at the time of voting, as these invalid votes were accepted by the RCG and would have led to a return code being sent to the voter.[84]

Scytl identified a number of improvements that would be made to the Internet voting system to resolve this problem in the future, and to report it to the voter when they submit the vote.[85]

The cause of the invalid ballots is fundamental in determining whether this recommendation has been complied with. If the cause is due to a deliberate attempt by the actual voter to try and manipulate the voting system, then this would not entail a corruption of the intention of the voter when casting the ballot. However, if a corrupted voting applet or an attempted hack by someone other than the voter was the cause, then the Internet system would have allowed the choice indicated by the vote to be corrupted and the integrity of the vote to be violated in these nine instances. This would lead to a conclusion that the Norwegian Internet voting system was not in compliance with this recommendation.

As Scytl cannot determine the actual cause of the invalid ballots and the cause will determine compliance with the recommendation, it is not possible to determine whether the Norwegian system has complied with the first part of this recommendation. Despite the latter two parts of the recommendation being complied with, this leads to an overall finding that it is not possible to determine compliance with this recommendation.

It is not possible to determine if the Norwegian Internet voting systems complies with this recommendation.

FC / 35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.

This recommendation raises the same concerns as the previous one, but it also adds that votes and voters' ID should be handled separately. While it would be understandable to wonder how votes and voters ID can remain separated and sealed, but simultaneously be used to send back to the relevant

[82] *Ibid*, p.5.

[83] *Ibid*, p. 10.

[84] The return code for these nine invalid ballots would have indicated a code for the party choice selected by the voter as well as the number of personal votes cast by the voter. However, the number of personal votes indicated in the return code SMS would have been one more than actually cast. This slight anomaly would have provided no indication to the voter to believe that the overall vote would be considered invalid.

[85] *Ibid*, p.5.

voter return codes that contains votes' value, this issue has already been dealt with in the assessment of recommendation 17.

Votes are encrypted by the voting applet before being submitted to the VCS, and they remain encrypted until the last stage of the counting process. The first stage of the counting process, the cleansing stage, makes the vote anonymous by stripping out the voter identification details. Votes are then mixed to randomize the order of the stored votes, and only then decrypted. The decryption key is split into 10 parts and distributed to 10 political party representatives, with six parts of the decryption key being required to decrypt the votes. Therefore votes are sealed for as long as the vote value and the voter’s identity can be linked.

The Norwegian Internet voting systems complies with this recommendation.

Appendix II

Operational standards

I. Notification

FC / 36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.

The timetable for Norwegian elections at all levels is clearly established in the Election Law and well summarized in the Ministry's *Election Manual – Overview of Election Rules*. These detail not only the dates of elections, but also the timelines for all stages of the elections.

The explanatory memorandum makes it clear that an e-election can differ in many ways from a paper based election and that the election management body has a responsibility to ensure that voters are aware of any such differences. Therefore, assessing the voter information measures implemented by the Ministry in the pilot municipalities is an important part of assessing compliance with this recommendation.

These measures began in spring 2010 when the E-vote Project visited the Electoral Committees in all the pilot municipalities. Local media were also invited to these meetings, and wrote about the visit and the pilot. In addition, a letter to editors regarding the pilot, signed by the Minister of Local Government and Regional Development, was sent to the local media in some of the pilot municipalities.

All the pilot municipalities had pre-pilots in the autumn of 2010 or the spring 2011. The municipalities were informed locally about the pre-pilots in different ways, for example via brochures and schools' web sites. The pilot was covered in social media by the Ministry on Facebook, Twitter, YouTube and in the e-voting blog.

A test version of the Internet voting system became available in the pilot municipalities late in July 2011. The municipalities were informed about this locally and in the local news. The Ministry informed voters on its web site.

From the beginning of July, the Ministry increased its efforts to inform voters about the Internet voting pilot. A training/instruction video on how to vote using the Internet was made available in the beginning of July. A link to the video was provided in the e-voting client, on www.e-valg.dep.no and www.valg.no. In the first two weeks of August, a sealed polling card with return codes was distributed to all voters in the pilot municipalities. This polling card told voters when and where it was possible to vote online and at the polling stations, information about MinID, about the option to vote several times online, how to vote using the Internet, the purpose of the return codes and how to use them. In the second week of August a brochure on Internet voting was sent to all households in the pilot municipalities. The brochure informed voters about all aspects of the option to vote by Internet, including the need to vote in secret.

It is clear that significant efforts were made by the Ministry to inform voters in the pilot municipalities about their option to vote by Internet.

The Norwegian Internet voting systems complies with this recommendation.

FC / 37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote e-voting, the period shall be defined and made known to the public well in advance of the start of voting.

The timetable for Norwegian elections at all levels is clearly prescribed by law, and occurs every four years for each level of election. Therefore, voters are aware well in advance when an election is scheduled to take place, making the formal notification of an election less relevant than in other countries.

The period allowed for Internet voting in the Norwegian Internet voting pilots was exactly the same as for the conduct of advanced voting by paper. As such, Internet voting was provided at a time when voters were well aware that voting was possible. As can be seen by the assessment of recommendation 36 above, significant measures were taken by the Ministry to inform voters of the opportunity to vote by the Internet and the ways in which they could do so.

The Norwegian Internet voting systems complies with this recommendation.

FC / 38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the e-voting will be organized, and any steps a voter may have to take in order to participate and vote.

The assessment of recommendation 36 above outlines the significant efforts made by the Ministry to inform voters about the opportunity to vote by Internet in the pilot municipalities and the steps required to do so.

The only additional step required of voters to utilize the option of voting online was that they be registered with one of the three online identification services approved for use with Internet voting (MinID, BuyPass or Commfides). Many Norwegians have already registered to use at least one of these portals, MinID being the most popular with some 2.6 million voters having activated their online MinID out of a total of 3.8 million eligible voters (68 percent).[86] For those that have not activated their MinID account before voting, the process is quick and simple, and can be completed when they log on to vote.

The explanatory memorandum also indicates that, “Consideration should also be given to offering the voter the opportunity to try the suitability of his/her equipment before he/she decides to use a specific electronic voting channel.” This relates to the suitability of the voter’s personal computer to run the Internet voting application. The Ministry did provide ample opportunity for voters to test this through

[86] This figure is taken from the Agency for Public Management and Egovernment (Difi) website – see http://www.difi.no/elektronisk-id/about-the-use-of-electronic-id [last accessed February 12, 2012].

the trial elections that were held in each pilot municipality and also through the test election site established by the Ministry.

The Norwegian Internet voting systems complies with this recommendation.

II. Voters

FC / 39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him/her on the register, and request corrections.

The Election Manual (page 12) states that, "The Population Register forms the basis for the municipality's electoral register, cf. Section 2-5 of the Act. Registration in the Population Register is required pursuant to Act No. 1 of 16 January 1970 relating to the Population Register and regulations for registration were issued by the Tax Directorate on 9 November 2007. The regulations contain detailed rules for regarding a person as being a resident. Election authorities may not make decisions concerning registration in the electoral register that are contrary to population registration rules. Pursuant to Section 2-5 the Population Register is responsible for providing the municipalities with information concerning who is to be entered in the municipal electoral register."

The electoral register is based on persons entered in the Population Register on June 30 on the year of the election, and this data is provided by the Population Registry to Electoral Committees. In order to identify and correct mistakes, and also to account for any changes between this date and the September election date, the Electoral Committees are required to display the electoral register and accept corrections. There is no timeline established for this display of the electoral registers, but the Election Manual makes it clear that it should be done as soon as practical after receipt of the data from the Population Registry (Election Manual, p. 14). The Election Law requires that the Electoral Committee announce the time and place for the display of the electoral register (Election Law, Section 2-6).

Therefore, it is clear that a voter's register does exist. This register is regularly updated by the Population Registry, and additional opportunity is provided by law for voters to check and amend their entries on the electoral register in advance of the election.

The explanatory memorandum, however, adds an additional aspect to this voter registry requirement. The memorandum states that, "It is necessary to check whether or not a specific person has the right to vote and whether or not a specific voter has cast a vote." As this recommendation concerns e-voting, we will not consider how the Norwegian system checks that multiple paper ballots are not submitted and counted for a voter, we will only consider the Internet voting component of this requirement.

The design of the Norwegian Internet voting system means that there is no need to ensure that Internet voters have not already cast any other ballot. In fact, the system requires that repeat ballots can be cast, with mechanisms in place to ensure that only one ballot for each voter is counted. Therefore, this additional requirement outlined in the explanatory memorandum is not applicable in the Norwegian case.

The Norwegian Internet voting systems complies with this recommendation.

N/A / 40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.

According to the Regulations Related to Trial Electronic Voting (art. 27.6), this recommendation is not applicable.

N/A / 41. In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.

According to the Regulations Related to Trial Electronic Voting (art. 27.6), this recommendation is not applicable.

III. Candidates

N/A / 42. The possibility of introducing online candidate nomination may be considered.

This is not part of the current election management system, and as the focus of this assessment is Internet voting, is seen as beyond the scope of this report.

FC / 43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.

The Election Law requires that both the preliminary list of candidates and the final list of candidates for each party list are displayed for inspection. The way in which this publication takes place is up to the municipality electoral committee, and therefore varies from municipality to municipality. The Ministry's Election Manual states that approved lists can be put on the Internet, and municipal electoral committees do publish the lists on their websites. The SSB also publishes the list of all parties and candidates on its website, as does the Ministry.

The recommendation refers to other (than electronic) means also being used, and the explanatory memorandum indicates that the candidate lists should not only be published through the Internet. Municipality electoral committees do in fact use a range of other mechanisms to inform voters about the parties running for election and the lists of candidates. Each municipality uses means which are most appropriate for its voters, but these means will typically include publication in a newspaper, and display in public government offices and libraries. Therefore a range of means are used to publish the lists of candidates.

The Norwegian Internet voting system complies with this recommendation.

IV. Voting

FC / 44. It is particularly important, where remote e-voting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.

Internet voting was not possible on the main day(s) of voting for the local government elections. The period of Internet voting saw voters also able to cast paper ballots by mail and in advanced polling stations in limited locations in each municipality. Therefore if this recommendation is read literally, then the Norwegian Internet voting system is not compliant.

However, it is possible to argue that the wording of the recommendation has become outdated due to developments in the field of Internet voting. The explanatory memorandum talks specifically about permanently updating the voter register with details of those voters who have voted and preventing voters voting both in polling stations and by other means. In fact, the intent of this recommendation can be better read to mean that voters should not be able, due to the various voting channels available, to cast and have counted multiple ballots.

The Norwegian system does not prevent voters from voting more than once. Repeat Internet voting is a deliberate design feature of the Internet voting system and voters can always cast a paper vote which will supersede any Internet votes. However, the system is designed to ensure that only one ballot from each voter is counted and that paper ballots are always counted instead of Internet ballots when both are cast by a voter.

With this interpretation of the recommendation, the Norwegian Internet voting system complies with this recommendation.

FC / 45. Remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.

Internet voting in Norway was only possible during the advance voting period, with the Internet voting period ending at midnight on the Friday before the election. After this time, it was not possible to use the Internet voting website to vote.

The Norwegian Internet voting system complies with this recommendation.

FC / 46. For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.

The assessment of recommendation 36 above outlines a number of relevant measures which were taken by the Ministry to inform voters about the use of Internet voting. Some of these, such as the instruction video, the brochures and the Frequently Asked Questions posted on the website, helped to guide voters through the use of Internet voting.

In addition to this, the Ministry operated a telephone helpdesk to support the use of Internet voting. The helpdesk was actually established for the trial Internet elections held in each of the pilot municipalities in advance of the pilots. During the local government elections, the lessons learned from this experience was used to update the helpdesk procedures. During the elections, the helpdesk operated from August 10 to September 9, from 08:00 – 23:59 on weekdays and 08:00 – 21:59 on weekends.

The Norwegian Internet voting system complies with this recommendation.

FC / 47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.

The Norwegian Internet voting system randomizes the order in which political party lists are presented to the voter, ensuring that no party list is favored by the use of Internet voting. The exception to this is that the option to cast a blank ballot is always presented at the end of the party list options.

The Norwegian Internet voting systems complies with this recommendation.

FC / 48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The e-voting system shall avoid the display of other messages that may influence the voters' choice.

The explanatory memorandum explains this recommendation as follows, "During the casting of the vote, the voter's immediate environment should be free from objects and information that could influence his/her choice in a partisan way. In the case of the Internet, this environment includes, in particular, the screens that are generated on a voter's computer when accessing the e-voting website. These screens should not contain more information about the choices than paper ballots, such as pop-up screens that promote a specific candidate or audio elements that are associated with a particular candidate or point of view."

The Norwegian Internet voting application is designed in such a way that no information about political parties or candidates, except that which is required for the ballot, is presented to voters while they are voting. Only the same information that is presented on the paper ballot is provided on the electronic ballot.

However, remote Internet voting in uncontrolled environments means that voters may use a wide variety of electronic devices, operating systems and web browsers to cast their ballots. Most of them are multi-task platforms that allow casting the ballot and simultaneously using other applications. While the Ministry can ensure that the voting application itself does not include undue information, it seems difficult, if not impossible, to guarantee that the client side system does not display information which may in some way influence the voter as they cast their Internet ballot.

It is also worth noting that if postal voting is admitted, as is the case with Norwegians living abroad, such voting is also not able to ensure that voting actually takes place in an environment which is guaranteed to be free of messages which may influence the voter's choice.

It is clear then that although the Internet voting application itself does not provide any information likely to influence the ballot choices of the voters, the environment from which they are voting, including the machine on which they are voting, may be presenting them with such information. There seems little that can be done to mitigate this issue while voting takes place from uncontrolled environments.

However, again a more contextual assessment is appropriate and similar arguments can be used as for recommendation 12. The recommendation says that the e-voting system shall avoid the display of messages which may influence the voter. Again, it is not clear if this relates only to messages displayed by the voting application or also to the computer on which voting takes place. Given the uncertainty over how to interpret this recommendation, and the differing conclusions to be reached from these interpretations, this assessment assumes the interpretation leading to compliance. This interpretation is also consistent with other Venice Commission findings on the compliance of Internet voting with international electoral standards (Venice Commission 2004), which must inherently assume that these environments cannot be fully excluded from manipulative influences.

The Norwegian Internet voting system complies with this recommendation.

N/A / 49. If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.

According to the Regulations Related to Trial Electronic Voting (art. 27.6), this recommendation is not applicable.

FC / 50. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.

The Ministry did establish a test Internet voting site, available to registered voters in the pilot municipalities, which was available before the Internet voting period. The actual Internet voting website made it clear which electoral races were being voting for, although it did not specifically inform them that it was a 'real' election. In contrast, the test election site clearly indicated that it was not a real election. While it looked very similar to the actual voting website, it stated that it was a test election site and all party names were changed to names such as "the football party." No return codes were sent from the test voting platform, and voters were clearly informed about this with the message, "in this test election you will not receive a return code."

The Norwegian Internet voting systems complies with this recommendation.

FC / 51. A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.

The explanatory memorandum discusses the deletion of information about the Internet voting transaction from the remote device on which the vote was cast. It identifies three layers of components, which might make copies of the transaction in some way – the web application, the browser and external software that can record the transaction. Only the web application is under the control of the Internet voting system, and in the case of the Norwegian system it is not possible through the web application to print, save or store the voting screen information. However, the other two layers of components are beyond the control of the Internet voting solution and it is entirely possible that they could record the voting transaction. In fact, even with paper based voting it is relatively easy to record the transaction through a photo or video taken from a mobile phone.

In addition to this, the Norwegian Internet voting system provides each Internet voter with a "return code" sent to the voter's mobile phone, which provides the voter with a code for the party that they have voted for. Voters need to check this return code against their polling card to see which political party the return code relates to and to ensure that their vote has been received as cast. The set of codes for party lists are different for each voter.

At first glance, it seems clear that the provision of the return code does violate this recommendation, as it provides the voter with "a proof of the content of the vote cast." This is the very purpose of the return code, so that the voter is able to prove to themselves that the Internet voting system has received their vote as it was cast, and is a critical mechanism in enabling trust in the system. It also seems clear that it is not possible to entirely eliminate the opportunity for the Internet voting transaction to be recorded in some way by the browser or some external software, and furthermore, this is not possible for paper based voting either.

However, it would be wrong to conclude discussion of the issue at this point. In fact, a proper assessment of this recommendation is much more nuanced and a full examination of the issue requires an understanding of why this recommendation is included. The purpose of ensuring that voters are not in possession of a proof of how they voted is to eliminate the possibility for voters to sell their votes to political parties/candidates or for voters to be coerced into voting in a certain way. Ensuring the secrecy of the vote, with no proof of how a vote is cast, makes the conduct of such practices unfeasible as the vote coercer or vote buyer will never know how the voter actually voted.

In this context, it is important to note that while the return code does prove how the voter voted, it does not prove the value of the vote that will be counted for that voter. Voters are able to vote as many times as they want using the Internet voting system, with only the last Internet vote being counted. Therefore, a return code could be superseded by a subsequent return code, and a vote-buyer or coercer will have no guarantee that the return code that they are shown represents the vote that will be counted for the voter. Internet voters can also vote using paper ballots on Election Day or in the advance voting period, and any paper ballot will be counted instead of an Internet ballot.

Such uncertainty will remove the incentive to engage in practices such as vote-buying and voter coercion. The same arguments are equally valid for the possibility of the web browser or other external components recording the Internet voting transaction. While the voting transaction can be recorded, there is no guarantee that this actual voting transaction represents the vote that will be counted.

This is one of the more difficult recommendations to assess. A literal interpretation of the recommendation's wording would necessarily lead to a conclusion that the Norwegian Internet voting system does not comply, because the voter is left with a receipt about the way in which they have voted and the environment could record the voting transaction. However, if the recommendation is seen in the context of measures to ensure that voter coercion and vote-buying do not take place, then the Norwegian Internet voting system meets this standard as any receipt provided/recorded need not represent the vote which is actually counted. It is this second, more contextual, interpretation of the recommendation which is used here.

The Norwegian Internet voting systems complies with this recommendation.

N/A - 52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.

According to the Regulations Related to Trial Electronic Voting (art. 27.6), this recommendation is not applicable.

V. Results

FC / 53. The e-voting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.

Internet votes in the Norwegian Internet voting system are encrypted by the voting applet on the voter's computer and it is not possible to determine the content of the vote until they are decrypted. This decryption of votes only takes place during the Internet vote counting process, which was on the evening of September 12, after polling was completed. Therefore, no information about the number of Internet votes cast for different ballot options was available until after the close of regular polling, and this was after the end of Internet voting.

The Norwegian Internet voting systems complies with this recommendation.

FC / 54. The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.

See the previous assessment of recommendation 18 as to the measures that are taken to ensure that the counting of a small number of Internet votes could violate the secrecy of voter's choices.

The Norwegian Internet voting systems complies with this recommendation.

FC / 55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.

The counting of Internet votes takes place immediately after the end of the paper voting period on Election Day.

The Norwegian Internet voting system complies with this recommendation.

FC / 56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.

The counting of Internet votes is inherently less observable than the counting of paper votes. Nevertheless, the local government elections in 2011 saw a range of observation mechanisms provided by the Ministry with respect to the counting of Internet ballots.

On the day before the election, the Ministry held a conference to explain the Internet voting system to observers and also to explain the processes that would take place during the counting of Internet votes. Then on the evening of the election, after the close of polls, observers were invited to watch the various stages of the counting process take place. In addition, the Ministry contracted an independent IT firm, Promis AS, to conduct a series of checks on the integrity of the counting process, and these checks were done publically as the counting ceremony proceeded. Finally, the actual decryption of the votes was conducted in an open and transparent manner, with all of the 10 encryption key-holders, representing political parties, being invited and called at random to provide the 6 parts of the key required to decrypt the votes. The entire ceremony was conducted by staff from the Ministry.

The only caveat that should be made to this assessment is that no observers actually observed the final count of Internet votes. The preliminary count of Internet votes was observed, as this took place shortly after 9pm on the evening of the election. However, the final count of Internet votes was only possible after municipalities had updated their electoral registers with all voters casting a paper ballot. Therefore, the final count of Internet votes did not take place until individual municipalities had completed updating their electoral registers with this data, and in effect did not take place until the early hours of the day after the election at the earliest. By this point all of the election observers had left the Ministry.

The Ministry did perform a “final final count” on September 20, 2011, in order to perform a final verification of the entire process. This was performed in the presence of the verifier, who subsequently verified the proofs for all stages of the counting process.[87]

Nevertheless, the Ministry did provide observers the opportunity to observe the counting process, from the preliminary to final count of Internet votes, and it was the choice of the observers not to remain for the entirety of the process.

[87] Data provided in email from the Ministry on May 2, 2012.

The Norwegian Internet voting system complies with this recommendation.

FC / 57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.

A number of records were kept by the Ministry of the Internet vote counting process. Each of the servers used for the different stages of the vote counting process generated a transaction log which could be analysed by the commercial software used by the Ministry for monitoring and analysing all of the transaction logs generated by the Internet voting system. In addition, the entire counting process was webcast and can be viewed again on the Ministry's website (at http://media01.smartcom.no/Microsite/dss_01.aspx?eventid=6316). Data was also produced about the counting process in order to report the total numbers of cast Internet votes, how many votes were removed during the cleansing process, the reasons for cleansed votes, and the numbers of Internet votes included in the final count for each election.

The Norwegian Internet voting system complies with this recommendation.

NC / 58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.

The receipt of irregular votes, i.e. invalid ballots, should not be possible with electronic voting solutions, and the casting of such ballots should be precluded by the voting interface. This was thought to be the case with the Norwegian Internet voting system. However, after the completion of the cleansing, mixing and decryption processes for Internet votes on the evening of the elections, the decrypted votes were then counted for their relevant elections. Subsequent to the announcement of results, but prior to the finalization of the results, the Scytl reviewed the logs from this process and discovered that of the 53,916 votes which passed through these stages to be counted, nine votes could not be interpreted after decryption. These Internet votes in fact had more ballot selections than was permitted under the election rules, and therefore were not included in the count of Internet votes (see recommendation 34 for more details on these invalid ballots).

The receipt of these invalid Internet ballots was not discovered until later in the process when the logs were reviewed, indicating that there were no mechanisms established for reporting on invalid ballots when they were processed during the count.

The Norwegian Internet voting system is found to be non-compliant with this recommendation.

VI. Audit

FC / 59. The e-voting system shall be auditable.

Full details of the audit mechanisms implemented in the Norwegian Internet voting system are provided in the Audit section of the recommendations (numbers 100 – 110). This recommendation, however, only requires that the Norwegian system be auditable, not that any actual audits take place. As the

Norwegian Internet voting system has implemented E2E verification mechanisms, these provide the information necessary to conduct an audit of the operation of the system.

The Norwegian Internet voting system complies with this recommendation.

NPTD / 60. The conclusions drawn from the audit process shall be applied in future elections and referendums.

The audit of the Internet voting pilots is still ongoing in Norway, so it is too early to say whether the conclusions drawn from the audits will be applied in future elections. It is also worth noting that the future implementation of Internet voting in Norway is a political issue and there is no guarantee that the audit recommendations will be incorporated into political decisions about the future or Internet voting in Norway.

At this stage it is not possible to determine if the Norwegian Internet voting system complies with this recommendation.

Appendix III

Technical requirements

The design of an e-voting system shall be underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election or referendum. The e-voting system shall include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified. Service failure or service degradation shall be kept within pre-defined limits.

A. Accessibility

FC / 61. Measures shall be taken to ensure that the relevant software and services can be used by all voters and, if necessary, provide access to alternative ways of voting.

This recommendation specifically deals with voters' impairments such as visual impairment or dyslexia, which are quoted in the explanatory memorandum. In line with this, the Norwegian system complies with the WCAG 2.0 AA-level success criteria from the Web Accessibility Initiative (WAI). To ensure access to Internet voting for visually impaired voters, the decision was made not to implement a technical solution that would have prevented a PC running Internet Explorer on Windows to record the voting session, as this solution would have blocked some of the software used to read out loud the content of web pages.

Another important accessibility measure is represented by the fact that the voting web site was available in seven languages: Norwegian Bokmål, Norwegian Nynorsk, English, Polish, Russian, Somali, Serbian/Bosnian/Croatian.

The use of MinID to identify voters is coherent with the previous development of eGovernment in Norway. Some 2.6 million people hold a MinID out of a total of 3.8 million eligible voters, or 68 percent of the electorate. While this is clearly short of 100%, it must be remembered that all Norwegian citizens received a PIN code and an invitation to activate their MinID account. Therefore, we can consider that the citizens who have not created an account have exercised a form of "opting out", which is not in contradiction with this recommendation. It must also be underlined that it was also possible during the advanced voting period to activate one's MinID account and vote online.

Regarding disabled voters, however, in the article "Enkelt E-valg?" [88] reporting on their study on vote accessibility for visually impaired voters in the municipalities of Re, Sandnes and Ålesund, Ingvar Tjøstheim and Kristin Skeide Fuglerud write: "We have seen a lot of cases where voters have not understood what to do to be able to vote electronically. Some will need help to register as MinID user. They cannot read PIN codes, or can not combine passwords and pin codes correctly." And Tjøstheim and Fuglerud continue: "The threshold for using e-voting would certainly be lowered if the sign-in solutions were more user friendly and accessible" (Tjøstheim and Fuglerud 2011). This may be linked to the fact that the majority of visually impaired persons in Norway are in the 60+ age group.

[88] See http://www.forskning.no/artikler/2011/september/298728, [last accessed February 26, 2012].

While challenges exist in providing full access to voters with various disabilities, it is clear that significant efforts have been made to do so. The WCAG compliance is a clear indication of the success of these efforts. Beyond the actual accessibility degree of the Internet voting platform, it is worth noting that voters also have other voting channels with paper ballots both during an advanced period and during Election Day.

The Norwegian Internet voting system complies with this recommendation.

FC / 62. Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.

This recommendation underlines the need to include users in the development of the solution in order to achieve the goals of recommendation 61. The interface development for the Norwegian Internet voting application started in 2009, when a preliminary study was done on the prototypes of the e-vote client[89]. The Norwegian project group worked in close contact with a reference group and representatives from the different organizations for disabled people, and users with disabilities were involved in the testing.

With a view to testing and refining the e-voting solution, pre-pilots were conducted throughout autumn 2010 and winter 2010/2011 in the municipalities participating in the trials. In the last two pilots, the system of return codes was also tested. By 19 May 2011, all of the 10 pilot municipalities had tested Internet voting online either in a youth council election or by arranging local referenda on various issues. Evaluations, consisting of voter surveys and in-depth interviews among the voters and non-voters, were carried out in all the pre-pilots.

In the summer of 2011, a large-scale test-election, open to all of the voters was conducted in the pilot municipalities. Delays in the deliveries from a subcontractor prevented a separate user test on the final version of the Internet voting client with a sample of disabled people. However, two researchers from the Norwegian Computer Centre conducted an observation study with 28 disabled people during the advance voting period and this can be used as a basis for further improvements for the Internet voting client.

The Norwegian Internet voting system complies with this recommendation.

FC / 63. Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).

As stated under recommendation 61, the Norwegian system was developed bearing in mind the WCAG 2.0 AA-level success criteria from the Web Accessibility Initiative (WAI). However, the specificities of the

[89] "Accessibility and usability evaluation of E-vote prototypes", available at www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/report_evoting_usability_accessibility_eval_nr_iter2_final.pdf [last accessed November 16, 2011].

electoral system, especially the possibility to add candidates from other parties to one's list, complicate the task to make the system WAI compliant.

The study conducted by Ingvar Tjøstheim and Kristin Skeide Fuglerud in the municipalities of Re, Sandnes and Ålesund prior to the 2011 municipal election has shown that casting a party vote without amendments was easy for visually impaired voters. Adding candidates from other parties was difficult, however. Yet, taking paper-based votes as a benchmark, the objective of this recommendation is fulfilled. It is worth nothing that enhanced accessibility to the voting process was one of the main objectives and rationales for the Internet voting project.

The Norwegian Internet voting system complies with this recommendation.

FC / 64. Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.

There are two aspects to this recommendation. One is the system's compatibility with the devices aimed at enabling disabled people to access the web, the other deals with the system's compatibility with the most common operating system/browser configurations.

The compatibility with devices for disabled voters has been examined under recommendations 61 and 63 and the system was found to be compliant. For the second aspect, the supported browser/OS combinations were chosen based on the most common configurations in the country. The selection of common configurations was based on statistics provided by a private company, Finn.no (website: labs.finn.no), which operates Norway's largest online marketplace and is hence well placed to observe the distribution of hardware and software among the Norwegian population.

In addition, feedback from reference groups like the Norwegian Association of the Blind and Partially Sighted and The Norwegian Labour and Welfare Administration was used to determine which browsers persons with disabilities were using. A total of 40 configurations were fully supported and another 25 had limited support.

Finally, the authentication through MinID was built on an existing and widely used solution.

The Norwegian Internet voting system complies with this recommendation.

FC / 65. The presentation of the voting options shall be optimized for the voter.

The explanatory memorandum explains this recommendation as follows, "Products and services must be adaptable to the users' functional restrictions and specific circumstances without infringing the equality principle. This can be achieved by offering different versions of the same product, changes to key parameters, modular design, ancillaries or other methods."

In our understanding, this recommendation is a reformulation of recommendations 61 to 64 and is more specifically intended for voting machines and calls for solutions such as enlarged fonts on the screen or read aloud devices for visually impaired people. In the framework of Internet voting, offering different versions of the same product, changing key parameters or adopting modular design could create security breaches in the system and would add complexity to an already complex platform.

The only “customized” item in the Internet voting system was the candidates’ list: each municipality and province had its own and the list displayed to the voter was determined by her address as known to MinID. Yet, as these lists are data but not executable functions, there are neither technical nor security issues in having different ones in the system.

The Norwegian Internet voting system complies with this recommendation.

B. Interoperability

FC / 66. Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, inter operate.

This recommendation aims at avoiding dependency of the electoral authorities towards a vendor which would be in a position to impose technical solutions of its choice. In the Norwegian system, all components communicate over the Election Markup Language[90] (EML version 5.0), and the authentication system uses SAML (Security assertion markup language).

According to its conceivers, EML is a set of data and message definitions covering a wide range of transactions that occurs during various phases and stages of the life cycle of an election. EML has been defined by the OASIS (Organization for the Advancement of Structured Information Standards) consortium, a not-for-profit organization that develops open standards[91]. EML is focused on defining open, secure, standardized and interoperable interfaces between components of election systems and providing transparent and secure interfaces between various parts of an election system. Conceptually, EML simply enables the exchange of data between the various end-to-end election stages and processes in a standardized way.

The solution outlined in EML is non-proprietary and works for any election scenario using electronic systems for all or part of the process. The objective is to introduce a uniform and reliable way to allow election systems to interact with each other. The OASIS EML standard is intended to reinforce public confidence in the election process and to facilitate the job of democracy builders by introducing guidelines for the selection or evaluation of future election systems.

SAML is an XML-based open standard for exchanging authentication and authorization data between an identity provider (here, MinID) and a service provider (here, the electoral authorities). SAML has been developed by the OASIS consortium.

The Norwegian Internet voting system complies with this recommendation.

FC / 67. At present, the Election Markup Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-

[90] http://en.wikipedia.org/wiki/Election_Markup_Language [last accessed February 26, 2012].

[91] www.oasis-open.org/org [last accessed February 26, 2012].

referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this recommendation, and supporting documentation are available on the Council of Europe website.

As explained in recommendation 66, the Norwegian Internet voting system uses EML version 5.0.

The Norwegian Internet voting system complies with this recommendation.

FC / 68. In cases which imply specific election or referendum data requirements, a localization procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.

This recommendation deals with the possibility to adapt the EML standard to local needs. More specifically, it calls for an EML implementation that allows for interchange of the Internet voting system's components without having to modify neither the system's structure nor other components.

In Norwegian, all Internet voting system components communicate using EML.

The Norwegian Internet voting system complies with this recommendation.

C. Systems operation

(for the central infrastructure and clients in controlled environments)

PC / 69. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.

The Ministry published more information regarding its Internet voting system than any country which has so far used Internet voting. We know for instance that the system comprises the following key components:

- Voter's Computer: Downloads and runs the voting client application (Java Applet).
- Electoral Roll (ERoll) Service: Holds information on the electorate.
- Authentication Service: Holds and sends voter credentials to the voter's computer (upon successful authentication by MinID, BuyPass or Commfides).
- Vote Collection Service (VCS).
- Return Code Generator (RCG).
- Key Management Service (KMS): Creates and distributes keys. It is also in charge of establishing the private key used for decrypting the votes.

- Cleansing Service: Discards electronic votes (e-votes) of voters that cast a paper vote (p-vote) and all but the last e-votes in the case of voters having cast more than one online vote.
- Mix-Net: Mixes and re-encrypts the encrypted votes signs the output.
- Decryption / Counting Service.

Except for the electronic electoral roll service (developed by Ergo), all of the systems listed above run software developed by Scytl.

The source code for the Internet voting system and its licence has been published (although the code available online at the time of the election was not the final version), as well as all documents regarding the tenders (the tenders themselves, their evaluation and the auditions of the tendering companies as webcasts), the contracts, the system's specifications and the description of critical components (system's interface with the ID portal, interface for transfer of results to the Election night system, etc.).

The installation date of the various software components is available from the documents accessible on the web page.[92] An issue tracking tool is also online at https://source.evalg.stat.no/. Therefore, it can be said that Norway has done much to comply with this recommendation.

Yet, as Spycher, Volkammer and Koening rightly note[93], "trust among the full population will be supported by publishing a simplified system documentation that explains and if applicable quantifies the remaining measures for trust establishment. Independent experts who have assessed the full documentation would need to confirm that the simplified documentation has been derived correctly." However, Spycher, Volkammer and Koening note that "it would be beneficial to additionally relate the explanations to a security concept and underline how and to which degree the security requirements are met."

The last point of the recommendation stating: "a procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time" does not appear to be covered in the Norwegian case, especially as the explanatory memorandum makes it clear that this should be possible for authorities and citizens alike.

It is clear that while significant efforts have been made to meet this recommendation, there are still some additional steps that could be taken.

The Norwegian Internet voting system partially complies with this recommendation.

FC / 70. Those responsible for operating the equipment shall draw up a contingency procedure. Any backup system shall conform to the same standards and requirements as the original system.

[92] See www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/technical-documents.html?id=612104 [last accessed May 24, 2012].

[93] "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting", available at www.regjeringen.no/upload/KRD/Prosjekter/e-valg/vedlegg/paper_transparency_and_technical_measures.pdf [accessed February 26, 2012].

The pertinence of this recommendation is underlined by the bomb attack that took place in early July 2011 in the administrative area of Oslo, next to the building of the Ministry of Local Government and Regional Development which organized the local and municipal elections.

The hardware for the Internet voting system is located in the premises of the Directorate for Civil Protection and Emergency Planning (dsb.no) and the Brønnøysund Register Centre (brreg.no). The RCG was hosted by DSB, which is subordinate to The Ministry of Justice and located in Tønsberg (about 100 km from Oslo and 700 km from Brønnøysund). The VCS and the rest of the online system is operated by the BRREG, a government body under the Norwegian Ministry of Trade and Industry that develops and operates many of the nation's most important registers and electronic solutions. The isolated components of the system (KMS, cleansing service, mix-net and decryption service) were located in the Crisis Support Unit, a high security facility subordinate to the Ministry of Justice and located in Oslo, but the servers were managed by security cleared representatives of The Ministry of Local Government and Regional Development (KRD).

Both VCS and RCG had replicated all hardware in one different location each, and this back-up was fully operative all the time. If one chain of hardware would have gone down, the other would still have been instantly operative. The Ministry of Local Government and Regional Development established Service Level Agreements (SLA) with both hosting entities that ensured adequate response time in case of problems.

The data centers were required to keep licences and protection software up to date. It was possible for the authorities to check the state of protection of the servers at any time.

The counting servers had a local backup. The servers were kept in a single bombproof server room. Manual backup routines for crossing off the electoral register had been developed in case the electronic system became unavailable.

The logs generated by all systems were monitored closely to ensure that the systems were in good health. This commercial monitoring system was configured to send out a text message to certain persons if irregularities happened. The connectivity of the VCS and the RCG with the outside world was constantly monitored, and SMSs were sent if connectivity was lost.

The Norwegian Internet voting system complies with this recommendation.

FC / 71. Sufficient backup arrangements shall be in place and be permanently available to ensure that voting proceeds smoothly. The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.

The explanatory memorandum comments on recommendations 71 and 72 together by placing them under the perspective of level of service for the electronic voting system. Yet, this labelling is debatable, as it is not possible to answer on the level of service without considering contingencies. Besides, the wording of both recommendations belongs to the universe of contingency rather than to that of level of service. We therefore examined them as aspects of contingency planning.

Prior to each pre-pilot and also prior to the 2011 elections, the ministry produced an emergency procedure, which was handed out to all relevant staff. The emergency procedure sheet contained contact data for all relevant staff (including backup staff), along with procedures for the escalation of potential problems. As this scheme was tried and tested during all pre-pilots, the Ministry says it knew that it worked well.

According to the procedure sheet that was handed to IFES, each member of the crisis cell had a precise role to assume in case of an incident on the system. Further to the Ministry staff, this sheet also lists staff from the various public entities hosting the hardware and the private companies (Ergo and Scytl) that developed the solution.

Both data centers had built in redundancy, with two servers established at the VCS and the RCG (in other words, contingency planning by design). The data centers also had in place their own disaster recovery plans, and have performed their own risk assessments.

The Norwegian Internet voting system complies with this recommendation.

FC / 72. Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. The backup services shall be regularly supplied with monitoring protocols.

There is considerable overlap between recommendations 70-72, and therefore much that could be said in the assessment of this recommendation has already been done so in the previous two recommendations, which were both found to be fully compliant. Additionally, it should be noted that the principle and backup VCS and RCG servers were fully monitored through the audit log monitoring system employed by the Ministry, and alerts were sent to Ministry staff in the event that service levels dropped below certain standards.

The Norwegian Internet voting system complies with this recommendation.

PC / 73. Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with technical specifications. The findings shall be submitted to the competent electoral authorities.

There is no prescription in the Norwegian legislation regarding testing and certification of the Internet voting system. However, the “Security objectives” mandate that, “The Contractor shall […] prepare the required documentation for the specified Common Criteria assurance levels.” This document further states, “The supplier shall in the development process create the necessary documentation for a formal review process and Common Criteria certification to EAL4+ of all components directly related to e-voting, including counting and returning of members”, and, “The supplier shall in the development process of Election System components not directly related to e-voting create the necessary documentation for a Common Criteria certification to EAL2.”

The “Security objectives” also foresee that “the Contractor shall describe their test strategy including methodology and tools for testing (usability testing, unit testing, accessibility testing, system testing, regression testing, volume testing, performance testing, security testing, acceptance testing) bug reporting and change management”, implying therefore that such testing has to take place before the system is used. Although it is not the “competent electoral authorities” who draft the testing protocol, as requested by recommendation 73, the requirement made to the Contractor has the purpose of enabling these authorities to validate or request additions to the this protocol. Therefore, this aspect of the recommendation can be considered to be met.

According to information received from the Ministry, all modules of the system were extensively tested before production, and all test phases of the project included a test protocol. The test protocols were quite high-level, and detailed test results were documented continuously in Redmine, the ministry’s bug tracking tool.

A predictive test that verifies the correct counting of electronic votes was also performed using a predefined protocol. This test was performed just before the opening of the election and it was a prerequisite for going live.

According to the Ministry again, the system was not common criteria certified for the municipal and county council elections. This certification will be considered by the Ministry before a bigger roll out of Internet voting.

An unofficial evaluation against the common criteria has been performed by three external experts, Melanie Volkammer, Oliver Spycher and Reto Koenig. One can summarize their conclusion with this quote: “Transparency and the technical measures we discuss imply significant extra costs and complexity for the project. We may conclude that E-valg make significant extra efforts in trust establishment although a high degree of public trust is assumed towards the central election administration.”[94]

Further, the explanatory memorandum to this recommendation states that: “A clear distinction should be made between checking done on a regular basis after each election or referendum, and the checking done whenever the system is modified in any respect. In the first case, employees of the entity running the election or referendum system might do the checking. However in the second case an external body should do the checking, as the check is closer to being a certification procedure.”

The second kind of checking is most appropriate for the Norwegian Internet voting system as the system had never been used before for a binding political election. Therefore, the project has gone in the right direction with respect with recommendation 73, but lacks a formal requirement that would translate the recommendation in the set of rules governing e-voting in Norway.

The Norwegian Internet voting system is partially compliant with this recommendation.

[94] www.regjeringen.no/upload/KRD/Prosjekter/e-valg/vedlegg/paper_transparency_and_technical_measures.pdf [last accessed March 3, 2012].

PC / 74. All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be notified.

The Regulations Relating to Trial Electronic Voting do not include any provision regarding access to the system during operation. Further, the explanatory memorandum to this recommendation states that "The electoral authorities must be made aware of all critical changes made on the system in order to anticipate any consequences and choose the appropriate policy to communicate such changes." In the case of county and municipal elections, the "electoral authorities" legally in charge are the county and municipal election commissions; however, these commissions had no involvement in the administration of the Internet voting project as this was conducted by the Ministry.

Before and during the election period, system access was strictly limited. Only two representatives from the Ministry could authorize changes on the system, and only two people in the Brønnøysund Register Centre and two people in the Directorate for Civil Protection and Emergency Planning in Tønsberg (a total of four people) were authorised to perform the changes. These roles were enforced by access rights on the servers.

The system was designed in such a way that certain passwords were not known to the system administrators in Brønnøysund and Tønsberg. These passwords were uploaded by the Ministry over VPN, and stored in the server memory. Any change in the Internet voting application would require a restart, and the passwords to be re-uploaded. No system change would have been possible without the Ministry noticing. Also, all commands entered in the system (including commands to upgrade the system) were logged.

In addition to these controls, the Ministry designed an ambitious, advanced chain-of-trust based on a TPM (Trusted Platform Module) and AIDE (Advanced Intrusion Detection Environment). These components would regularly monitor the system for any change in any file, and alert the log monitoring system. However, the Ministry had to scale down its ambitions due to time constraints: there was not time to properly test the implementation of these tools, and it was decided to leave them out for the pilot. They will be tested as part of acceptance testing, and will be used in any further pilots.

To summarize, procedures were in place to implement this recommendation, as well as a division of duties, which is central to a proper monitoring of the system. The automated tools that should have supplemented these procedures could not be implemented before the election. And the municipalities, which were the owner and the legally responsible entity for the election, were not involved. Therefore, while much was done to implement the recommendation there are additional steps required for it to be fully implemented.

The Norwegian Internet voting system partially complies with this recommendation.

FC / 75. Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from any person. During the election or referendum period a physical disaster recovery plan shall be

in place. Furthermore, any data retained after the election or referendum period shall be stored securely.

As stated in the assessment of recommendation 70, the hardware used in the system was split between different locations, some of it in highly secure rooms, and each piece of hardware was duplicated. The Internet voting servers were housed in secure zones, where special electronic locks required the presence of two authorized individuals for entry. These locks were positioned in such a way as to make it physically impossible for a single person to operate them.

The counting servers were located in the Crisis Support Unit (CSU), and were subject to very stringent access controls. After the July 22 attack, they were relocated to the Ministry's premises. Even if this location was less suitable, access was still strictly controlled. All hardware in this infrastructure was redundant, and there are logs of all software changes (which were all supervised).

The data centers have their own security manuals, based on ISO27000. There was no particular security handbook created for this project. However, the requirement specifications detail a number of procedures for dealing with the system.

The Norwegian Internet voting system complies with this recommendation.

FC / 76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.

As stated in the assessment of recommendation 71, there existed a crisis plan where each staff member had a precise role to assume in case of incident with the Internet voting system. In addition to the Ministry staff, this cell comprised staff from the various public entities hosting the hardware and the private companies (Ergo and Scytl) that developed the solution.

Contingency plans were drafted and a monitoring of the availability of the system performed.

It must be also underlined that, Internet voting being a supplementary voting channel, service disruption is not as problematic as it would be for a networked electronic system installed in polling stations. Citizens prevented from voting online always had the opportunity to go to the polling station on September 12. There was no risk that a citizen lost his voting right due to Internet or online voting failure, because this option ended on September 9.

There remains the problem of defining who the authorities are, as stated in recommendation 74.

The Norwegian Internet voting system complies with this recommendation.

D. Security

I. General requirements

(referring to pre-voting, voting, and post-voting stages)

FC / 77. Technical and organizational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.

See the assessment of recommendations 57, 70, 71, 72 and 75 for contingency procedures and backup procedures.

The Norwegian Internet voting system complies with this recommendation.

FC / 78. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained.

At first sight, this recommendation is unclear, because its uses the words “privacy” and “confidentiality.” The first, evoking the private sphere or the right to vote in private, may refer to polling station arrangements. The second seems to refer to vote secrecy. What is therefore exactly meant here?

This recommendation is hardly better understood through the explanatory memorandum, which states, “Depending on national practices there may be further confidentiality requirements with respect to the candidate's decision. In that case those requirements must be met. “ The word “candidate” makes the recommendation even harder to understand. The key to understanding this recommendation may be found by the mention of the voters' register. The target of this recommendation then appears to be that of preserving the secrecy of the voters' register and of the information on who has cast a ballot and who has not.

In the Norwegian case, information on who has cast an Internet vote is not recorded on the electoral roll as these voters always retain the right to cast a paper ballot in the advance voting period or on election day. Even at the completion of the counting process a list of those voters who cast an Internet ballot is never produced, and cannot be produced as this data is never decrypted.

The Norwegian Internet voting system complies with this recommendation.

FC / 79. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.

The scope of this recommendation has already been covered with recommendations 70 to 76. Recommendation 79 brings however a novel element: the system's self-monitoring. Whereas recommendations 70 to 76 scrutinised the level of service and contingency plans, this recommendation mandates that a monitoring system observe the proper functioning of the system and its availability.

The Norwegian Internet voting system did utilise a system monitoring tool which checked the availability of the system and the existence of any intrusions. The monitoring tool was designed to alert key staff when certain critical situations occurred.

The Norwegian Internet voting system complies with this recommendation.

FC / 80. The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.

As stated under recommendation 74, before and during the election period, system access was strictly limited, based on a division of roles and duties. These roles were enforced by access rights on the servers. The system was designed in such a way that certain passwords were not known to the system administrators in Brønnøysund and Tønsberg.

On the voter side, the strong authentication process based on MinID, BuyPass and Commfides made sure that only eligible voters could access the voting system. In accordance with this recommendation, voters had to register and be recognized by the authentication portal before being allowed to cast a ballot.

The Norwegian Internet voting system complies with this recommendation.

FC / 81. The e-voting system shall protect authentication data so that unauthorized entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.

The possibility for a single voter to cast several online votes makes this recommendation important in the Norwegian context as an attacker who obtained voter authentication data during the voting procedure could use it to cast another ballot, cancelling the citizen's legitimate vote. On the other hand, the use of one-time password sent to the voter's registered mobile phone offers protection to the citizens, as the attacker will always miss one crucial element of authentication.

It should also be noted that the Regulations Relating to Trial Electronic Voting mandate that an "authentication solution with a minimum level of 3 shall be used, as specified in the Guidelines for Public Enterprises that govern electronic services and online trading - The Framework for Authentication and Non-repudiation in Electronic Communication with and within the Public Sector (FAD 2008)" (article 27 §4).

According to the document "Study on Mutual Recognition of eSignatures: update of Country profiles, Norwegian country profile" published in 2009 under the auspices of the Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC)[95], level three authentication can take the following forms:

- Password calculator protected by a PIN-code, where the first PIN-code is sent by a separate mail

[95] http://ec.europa.eu/idabc/servlets/Doc14e9.pdf?id=32349, [last accessed May 9, 2012].

- One-time passwords on cellular phone, where the cellular phone is registered with an own registration code distributed to the address registered with the National Registry
- Person-Standard pursuant to the ”Requirement Specification for PKI for the Public Sector”
- List with one-time passwords, used together with a static password and user name.

According to this document, there are, in Norway, four authentication levels. Buypass and BankID fulfill the requirements of level four. MinID is compliant with level three. Yet, MinID uses cryptography and therefore the following condition set in the recommendation “in uncontrolled environments, authentication based on cryptographic mechanisms is advisable” is fulfilled.

The Norwegian Internet voting system complies with this recommendation.

FC / 82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.

The Regulations Relating to Trial Electronic Voting foresee that the electronic electoral roll shall be set up on the basis of the constituencies. The polling cards voters receive must contain the following information (§23 of the “Regulations relating to parliamentary and local government elections”)[96]:

- the election and year for which they are valid,
- the elector’s name, registered address and year of birth,
- the name and address of the Electoral Committee in the municipal authority area in which the elector is registered in the electoral register,
- polling district, rode, page, line, the number of the municipality’s electoral register and the municipal authority area number,
- the address and opening hours of the polling station on the Election Day(s),
- the space where the returning officer shall write down the time and the place where the vote was cast and sign for receipt of the vote.

It must be also noted that the authentication does not take place on the voting system, but on one of the three available authentication portals. The procedure for MinID authentication (when accessing the MinID web page, voters are asked for their social security number and a password they have previously themselves defined, before receiving by text message a one-time password on their mobile phone) make it very unlikely that two voters would share the same ID as this would mean, among other oddities, sharing the same social security number.

This recommendation also aims at avoiding that people having a role in the voting system’s operation could perform it using their voter’s ID. This would, for instance, be the case of an administrator being able to log him or herself directly on one of the system’s server using their voter ID. As the authentication system and the voting system are separate, this should not be possible. Furthermore, the authentication systems are not owned by the same administrative entity owning the eVote system.

[96] http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Regulations_2003_EN_170609.pdf [last accessed May 24, 2012].

At least with MinID, each citizen provides his/her national ID number and therefore the identification relies upon the national register that keeps this database up to date. Given that the census is built up from this database and uploaded to the voting servers, discrepancies, double records and other mistakes will be the same as in traditional paper based elections.

The Norwegian Internet voting systems complies with this recommendation.

FC / 83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.

A correct understanding of this recommendation should make a clear distinction between the generation of data to enable observation and actual observation of/access to such data. The recommendation only requires a reliable and sufficient generation of data, but it is not concerned with who will receive such information and how it will be handled. This difference is important in correctly assessed the compliance of the Norwegian Internet voting system. While the system generated significant observation data, the number of people receiving such information might be seen as inadequate. This second conclusion, however, does not impact the compliance of the recommendation.

In fact, the Norwegian Internet voting system generated significant amounts of data about its functioning, data which could be observed. Every transaction and event on the various components of the Internet voting system generated a log entry. All log entries from the different servers used were consolidated and available for inspection and monitoring through a commercial log file monitoring and reporting system.

Therefore, it is clear that the system does generate reliable and sufficiently detailed observation data. The different servers, which make up the Internet voting system, all use a synchronised time source, as outlined in the assessment of recommendation 84 below. The authenticity of the log entries can also be checked, as a system of immutable log entries is used, where each log entry contains a hash of the entire previous log entry.

The Norwegian Internet voting systems complies with this recommendation.

FC / 84. The e-voting system shall maintain reliable synchronized time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

All of the servers used by the Norwegian Internet voting system connected to an NTP (Network Time Protocol) server to synchronize their internal clocks against a centralized server on regular intervals. This is standard procedure for maintaining synchronized time for audit trails.

The Norwegian Internet voting systems complies with this recommendation.

FC / 85. Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies.

As has been discussed in relation to other recommendations, there are different electoral authorities involved in the implementation of the Internet voting project. Municipal and county electoral committees are, for instance, responsible for conducting the paper based component of the elections and publishing the official results, including those coming from computerized means. However, the Ministry, which has no formal role in implementing the local elections, managed the Internet voting process on behalf of the municipal and county electoral committees. It was the Ministry, therefore, that implemented and monitored the range of security measures enacted for Internet voting. Despite the problems that such combination of different authorities may entail, the recommendation itself only mentions election authorities in a very generic way and it seems that the internal structure of such authorities will not impact the compliance with it.

As to the requirement that independent bodies assess compliance with security standards, we should take into account that the explanatory memorandum points out that the “designation of an independent body shall be transparent.” This feature might at least include the disclosure of the relevant documents regarding this decision (e.g. criteria used to select the independent body, people involved, description of the procedure, scope of its tasks, deadlines, NDAs).

According to the information provided by the Ministry, “auditors/verifiers have very different roles. Veritas performs QA of the project, as an IT procurement and development project. They do not have any role in evaluating or auditing us from a legal or elections technical perspective. Kåre Vollan and his team are specifically tasked with verifying the mathematical proofs of correctness generated in the counting stage. They also verify the integrity of the ballot box that goes into the counting. Kåre also provides some elections specific advice … Veritas and Vollan both won contracts through standard procurement processes. Veritas won the contract for external QA, and they report to the Steering Committee ahead of every Steering Committee meeting (approx. monthly). Vollan (through the consultancy Promis) won the contract for internal QA, into which the verifying was incorporated. Kåre reports ... on agreed dates for delivery … they have not signed any NDAs beyond what was required to be allowed into the high security facility in which the servers were housed (destroyed by the bomb on July 22)”

The Norwegian Internet voting systems complies with this recommendation.

II. Requirements in pre-voting stages

FC / 86. The authenticity, availability and integrity of the voters’ registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.

The voters' and candidates' lists are uploaded to the voting servers with the relevant digital signatures that guarantee that the lists are the ones provided by the electoral authorities. The voters' and candidates' registers should also maintain their integrity during the voting period. The system should guarantee, for instance, that all the candidates are displayed when a given voter is going to cast his/her ballot (see comments to recommendation 90). However, only computerized means might guarantee such integrity and therefore audit/certification measures become essential to know if this goal is correctly achieved. Moreover, as already happens with paper-based elections, potential mistakes could be reported by voters or candidates in order to adopt the appropriate measures.

The Norwegian Internet voting systems complies with this recommendation.

N/A - 87. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.

This seems to only be applicable for online party and candidate registration systems. Such a system was not used in the Norwegian Internet voting pilots and therefore the recommendation is not applicable.

N/A / 88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

The system of voter registration is totally separate from the Norwegian Internet voting system and therefore is seems as not applicable to the compliance of the Internet voting system with the recommendations.

III. Requirements in the voting stage

FC / 89. The integrity of data communicated from the pre-voting stage (e.g. Voters' registers and lists of candidates) shall be maintained. Data-origin authentication shall be carried out.

See the assessment for recommendation 86.

FC / 90. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.

Taking into account the Norwegian electoral system, an authentic ballot means a layout that provides the voter the list of candidatures, with the relevant candidates for each one, and the chance to mark some of them. In local elections, the ballot should also include the chance to add a candidate from other list.

Remote voting from uncontrolled environments makes it very difficult to verify whether the voter is actually receiving an authentic ballot, that is to say, all the information already mentioned. If the data displayed to the citizen does not include a party list, a candidate or the write-in option, the ballot would not be authentic. As mentioned in the explanatory memorandum, the client's PC might be exposed to several attacks aiming to create a fake website or altering the ballot's content. This was one of the reasons why the Ministry decided to use return codes, as a way of validating the receipt of the ballot through a mechanism (the mobile phone of the voter) that was not available to those making such attacks.

A comparison with postal voting could however be an interesting approach to this problem because this remote voting channel can also include mistakes in the documentation sent to the voter. In this case, the solution consists in transferring to the citizen the responsibility to verify whether s/he receives all the correct ballots. Internet voting would not generate a worse scenario but in Norway, postal voting is only admitted for citizens living abroad. Obviously a generalization in Norway of such solutions would be a significant innovation that should be taking into account but, in legal terms, it has no impact. From a legal point of view, there is no barrier to implement in Norway what is already accepted for Norwegians living abroad.

The Norwegian Internet voting systems complies with this recommendation.

NC / 91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.

Time stamps are used to ascertain when each ballot has been cast and whether it has been cast during the advanced voting period. The counting process only allows votes which have been cast within the 30 minute voting session window, as evidenced by the one vote, which was cleansed due to this reason, and within the authorized voting period.

The one ballot, which was cast outside of the 30 minute voting session period, presents a problem for this recommendation as the voter who cast this ballot will have received no indication that the vote would be rejected, and would have received a return code. Therefore, in this very specific instance of a ballot being submitted in the very last milliseconds of the voting session time limit, the fact that the vote has not been cast in the prescribed time limit is not ascertainable. While this is a statistically unlikely scenario, it represents a problem in principle as it is possible to cast a vote which is outside of the permissible time period but which does not lead to the voter being informed that the vote has been cast unsuccessfully.

The Norwegian Internet voting systems does not comply with this recommendation.

NPTD / 92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.

Although the recommendation requires assurances of the integrity of the system itself, the explanatory memorandum only mentions the voters' confidence in the system, stating that, “there are limited means by which the e-voting system can control whether a secure environment exists. Provision should be made to enable voters to have confidence in the system, such as measures to ensure that genuine software is used, or recommendations on how to protect the system environment.”

Citizen confidence and system integrity are two very different issues. While the second one is an objective goal that can be fully assessed, the first one is a subjective perception on the part of the voter.

The reason for referring to voter confidence may be a result of the admission in the explanatory memorandum that there is a limit to the control of the client side environment when using remote voting in uncontrolled environments.

The Norwegian Internet voting system finds a way to resolve the insecurity of the client-side environment with the need to protect the vote from modification through the use of the return code.

These return codes prove to voters that the votes received by the vote server are the same, or not, as the ones which have been submitted by the voters. If the votes have been modified before submission then the return code will indicate a different ballot choice from what the voter expected to find, raising an alarm. The system of return codes not only addresses the integrity of the vote submitted, required by the recommendation, but also the confidence of the voter, addressed in the explanatory memorandum.

Finally, the nine invalid ballots again pose some problems for accepting full compliance of this recommendation. As explained in recommendation 34, the cause of these invalid votes could be explained either by a corrupted voting applet or by a successful manipulation of the voting system. While the former possible cause has no impact on this recommendation, as the problem is not the modification of the vote but the accurate recording of the vote cast, the latter directly influences this recommendation. A successful hack of the Internet voting system would mean that somebody managed to modify a cast ballot. Unfortunately, Scytl was not able identify whether the problem was caused by the applet or a manipulation of the system (by the voter or a third party).

It is not possible to determine if the Norwegian Internet voting systems complies with this recommendation.

FC / 93. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.

The explanatory memorandum provides additional explanation for this recommendation, saying "technically there may be limited means to ensure this in a remote voting environment. Nevertheless, every measure possible shall be taken to delete such residual information when the vote has been cast." Both the recommendation and the explanatory memorandum seems to assume that, in case of remote e-voting, it will be extremely difficult or even impossible to completely ensure the destruction of this residual information. The Recommendation itself asks to provide information on how to delete the residual data only "where that is possible" and the memorandum asks to implement every possible measure once admitted that there may be limited means to achieve this goal.

Despite the difficulties in ensuring that this residual information is removed, the security requirements for the Norwegian Internet voting system make it clear that this is a requirement of the system. The general security requirements of the system state that:

> *"Residual information holding the e-voter's decision or the display of the e-voter's choice shall be destroyed after the vote has been cast. When voting in an uncontrolled environment, the e-voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote (e.g. cookies)."*[97]

[97] This can be found at '7 Security Requirements: OS 4.4" in the document, 'SSA_u_Appendix2B_Requirements_Table' which lists system requirements.

The supplier of the Internet voting system, Ergo Group, confirmed in its tender documents that this requirement was met by the system.

In addition to this, the system provides the possibility for repeat voting and casting a paper ballot making any residual information which may remain worthless. Even if the residual information is used to reconstruct the value of a vote and the voter identification details associated with the vote, there is no way of knowing if this data relates to a ballot that will be counted for the voter.

The Norwegian Internet voting systems complies with this recommendation.

FC / 94. The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.

The Norwegian Internet voting system identifies voters through one of three authentication channels and only allows voters who were registered to vote in one of the pilot municipalities to continue and cast a ballot.

The second part of the recommendation is more problematic. As discussed in previous recommendations, the ability to cast repeat votes in the system does not violate the principle of one person one vote as only one vote is counted for the voter. If the intention of this recommendation is to ensure that multiple votes are not counted for a voter, then the system does comply.

However, the existence of the nine invalid votes calls into question the compliance of the Norwegian Internet voting system with this recommendation. In these nine instances, the voter was able to cast more than one vote for party lists on the same ballot, making the ballots invalid. This may not comply with the section above which states that the e-voting system shall “ensure that only the appropriate number of votes per voter is cast.”

The explanatory memorandum does not provide any guidance on how to interpret this component of the recommendation. Therefore, parallels with paper balloting are useful. On a paper ballot it is possible to cast votes for more than one political entity, but again the ballot will be found to be invalid. The important point to note is that the paper balloting system, as the Internet voting system, ensures that these multiple votes for political entities are not counted.

The Norwegian Internet voting system complies with this recommendation.

NPTD / 95. The e-voting system shall ensure that the voter’s choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.

There is a definitional challenge related to the assessment of this recommendation regarding the question of what is considered to be the ballot box. In fact, it could be argued that there are many ballot boxes. The VCS is a ballot box, and this is where all of the received Internet ballots are stored. A copy of this ballot box is loaded onto the cleansing server, a subset of the votes on the cleansing server are loaded onto the mixing server, and the results of the mixing process are loaded onto the server which tabulates results. All of these servers could be considered to be some aspect of the ballot box. This is relevant because the recommendation required that all sealed (encrypted) votes enter the ballot box. Due to the possibility for repeat voting, including paper voting, it will not be the case that every sealed vote will enter each incarnation of the voting server. Specifically, votes that are cleansed will not be passed to the mixing or tabulation servers.

While this may appear problematic using a literal interpretation of this recommendation, as outlined when assessing recommendation 5 the explanatory memorandum states that repeat voting is permissible as long as only one ballot per voter is included in the count. It is exactly to exclude the possibility that multiple ballots from the same voter are not included in the count that not all sealed votes are passed to the final stages of the counting process.

Additionally, the requirement that the voter's choice is accurately represented in the ballot box presents a problem when it comes to the nine invalid Internet votes recorded. If these were the results of an error in the voting applet or if they were the result of an attempt to manipulate the voting system by someone other than the voter, then they would represent examples where the voter's choice was not accurately represented in the ballot box. Alternately, the invalid Internet ballots could have been caused by a deliberate attempt by the nine voters themselves to manipulate the system, and if this were the case then the recorded (invalid) votes would represent the voter's choice.

As indicated in the assessment of recommendation 34, Scytl was not able to determine which of the scenarios above were the true cause of the invalid ballots.

It is not possible to determine if the Norwegian Internet voting systems complies with this recommendation.

FC / 96. After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system. However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.

The Norwegian Internet voting system ensures that anyone attempting to cast a vote after the end of the Internet voting period is not permitted to do so. Anyone logged in at the time that the Internet voting period closed was informed that they had a 10 minute period in which to complete the submission of their votes, after which the voting session was terminated.

As the cleansing process looks at the timestamp of when the voter logged into the Internet voting system, and not the time of submission of the vote, the cleansing process would not reject votes submitted within the 10 minute grace period.

The Norwegian Internet voting system complies with this recommendation.

IV. Requirements in post-voting stages

FC / 97. The integrity of data communicated during the voting stage (e.g. Votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.

The Norwegian Internet voting system uses a number of means to ensure that data passed from the voter to the VCS is authentic. The Internet voting system itself does not authenticate the voter, but passes this function to one of three authentication mechanisms (MinID, BuyPass and Commfides) but the ID portal signs the vote which is submitted with its authentication data. This ID portal authentication data is checked to ensure that it has come from a valid authentication mechanism. In addition to this, voters sign the ballot submitted to the VCS with their private key and the authenticity of this private key is checked before votes are accepted.

The Norwegian Internet voting system complies with this recommendation.

FC / 98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.

There are a number of ways in which the Norwegian Internet voting system can demonstrate that the counting process accurately counts votes. Firstly, it publishes the source code for voting system so that those able to analyse the source code can check that the system has been designed to count the votes accurately. In addition to this, the implementation of E2E verification mechanisms can demonstrate that, in practice, votes were processed accurately through the counting process. As discussed in other recommendations, the audit of these E2E verification mechanisms showed that votes were counted accurately.

The counting can be reproduced and, in fact, the Norwegian government conducted both a preliminary count and a final count of Internet votes (although there were differences due to the differences in the data on paper ballots cast). However, the explanatory memorandum indicates that, "to gain confidence, it is most important that the counting process can be reproduced and that this can be done with a *different system from a different source*" (italics added).

Taking into account the publication of the source code, the counting could be reproduced by anyone and with other means. It is worth wondering whether any election management body would be willing to provide vote data, even if encrypted, to 'another source' to replicate the counting process. Compliance with the wording of the explanatory memorandum would appear problematic from a data security and confidentiality perspective. However, the recommendation only requires that the counting of votes be reproducible, not that it actually be reproduced.

The Norwegian Internet voting system complies with this recommendation.

FC / 99. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.

The Norwegian Internet voting system does not have a single server adopting the role of a ballot box. The database used to store votes received by the VCS, as well as the servers used during the counting ceremony, could be considered as ballot boxes because they store the votes at different stages of the process.

Regarding the goal that this recommendation intends to pursue, both voting and counting servers seem affected and their availability and integrity would have to be maintained as long as required. While data coming from the VCS is downloaded in a secure manner that is externally monitored, the three final servers (cleansing, mixing and tallying) can be protected with the same measures undertaken during the election period, that is to say, when they were kept in secured areas and without any outside connection.

The integrity of the data at all stages of the voting and counting process was protected by digital signatures. All of the 'black box' manipulation of the data (for example, the mixnet and the decryption services) generated zero knowledge proofs, which were externally verified.

Finally, the period mentioned by the Recommendation will depend on each nation's legislation, but in Norway all electoral data was destroyed nine days after the results were determined. Log files have not been deleted but, according to the Ministry, such material has no impact on the anonymity and secrecy of the ballots.

The Norwegian Internet voting systems complies with this recommendation.

E. Audit

I. General

FC / 100. The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application.

The Explanatory Memorandum defines auditing of the election process as, "the means by which, in particular, the processes used to collect and count the vote can be examined, in order to confirm the authenticity of the result." The memorandum also adds other interesting features when it states that this audit is to be "independent and extensive." It should also include logical, application and technical approaches.

The Norwegian Internet voting project was designed to be implemented in a transparent manner, and a number of different audit mechanisms were included. On a project level, the Ministry contracted Veritas to conduct on-going quality assurance assessments to the Steering Committee and these assessments focused on the procurement and project management aspects of the pilots. Promis AS were awarded a contract by the Ministry to conduct verification functions for the Internet voting system, including the verification/audit of the processing of ballots received on the VCS through the counting and results process.

The audits that Promis AS performed included the following:

- **Verification of the certificate from the ID portal** – the independent auditor conducted a physical inspection of ID portal certificates obtained through the Ministry and through a second channel independent of the Ministry.

  Both certificates were found to be identical, demonstrating that ID portal certificate matched the certificate used in the cleansing process to verify that all ballots had a valid authentication token from the ID portal and were legitimate votes.

- **Comparison of hashes between the VCS and the RCG** - independent software was developed to verify that hashes of the encrypted votes stored on the VCS were the same as hashes of the encrypted votes stored on the RCG, and that no additional votes were stored on either server. This proves that votes of the same value are stored on each server.

  In fact the comparison of the votes stored on the VCS and RCG found that there were 53 votes stored on the RCG which were not present on the VCS. The Ministry had in fact indicated to Promis AS that between 54 and 57 votes would be found on the RCG with no corresponding encrypted vote on VCS.[98] The Ministry indicated that these entries on the RCG were not problematic as they represented cases where an encrypted vote was not stored on the VCS due to some technical problem. The voters casting these ballots were informed that the vote had not been cast and a receipt was never sent out to the voter.

  All of the other votes stored on the VCS and RCG were identical.

- **Verification of the integrity of the ballot box after data transferred from the VCS to the Ministry's premises** – independent software was developed to check that every ballot stored on the VCS was present and identical in the copy of the ballot box used for the counting process.

  This independent software showed that the contents of the VCS were identical to the contents of the ballot box used for the counting process.

- **Verification that the cleansing process has not injected new votes to the ballot box** – independent software was developed to check that the result of the cleansing process did not contain any votes that were not registered on the VCS.

  All of the votes, which were passed from the cleansing process for counting, were represented in the ballot box from the VCS.

- **Verification of zero-knowledge proofs regarding the correct mixing and re-encryption of the encrypted votes** – the mixing process stage of the counting process creates a zero-knowledge proof to demonstrate that each mix-node has decrypted and encrypted groups of votes it has received as input correctly. Independent software was developed to check these zero-knowledge proofs, and in

[98] The Ministry had anticipated that more would be found than were because it has based its estimate on data which had included a shadow election, run in parallel to the actual election but used only for verification purposes. The audits were not applied to the shadow election, hence the discrepancy between anticipated and actual cases found.

doing this check verify that mixing process output votes as the same value as were input into the mixing process.

All of the zero-knowledge proofs were found to be correct, demonstrating that the mixing process produced a randomized but, accurate copy, of the ballots which entered into the mixing process.

- **Verification of the zero-knowledge proofs regarding the correct decryption of the encrypted votes** – the decryption process for the votes which are to be counted produces a zero-knowledge proof for each vote that is decrypted. Independent software was developed to check the zero-knowledge proof for each decrypted vote.

  All of the zero-knowledge proofs were found to be correct, demonstrating that the correct private key was used to decrypt the votes passed from the mixing process and therefore that the decrypted vote values accurately reflect the encrypted vote values.

In addition to this, every event on infrastructure components and transactions on the various servers used by the Internet voting system (such as the VCS, RCG, cleansing server, mixing server and tabulation server) was logged using immutable logs. These logs were monitored using a professional log monitoring system by the Ministry as the project unfolded, and also reviewed through a comprehensive post-election audit. In addition to this, ongoing monitoring of the functioning of the infrastructure took place, with alerts sent to key staff when issues of concern arose.

The Norwegian Internet voting system complies with this recommendation.

FC 101. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.

As this recommendation refers to sections II to V, below details of the assessment is provided in the sections below. All of the sections below are seen as compliant with the recommendation, therefore this one is also.

The Norwegian Internet voting system complies with this recommendation.

II. Recording

FC / 102. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

As discussed in previous recommendations (see recommendation 100, for example), comprehensive audit mechanisms were implemented for the Norwegian Internet voting system. These audit mechanisms were reported on and reports monitored by Ministry staff. In the event of certain threats or failures in service, the monitoring system was programmed to inform key staff in the Ministry of these events.

The Ministry indicated that the logs produced by the system were available for scrutiny by observers at the Ministry premises if observer groups had requested to view them. While this willingness to provide access to the logs is positive, it is not clear if or how this possibility was communicated to observers. While this information should be clearly communicated to observers at future elections where Internet voting is used, this does not detract from the Norwegian systems overall compliance with this recommendation.

The Norwegian Internet voting system complies with this recommendation.

FC / 103. The audit system shall record times, events and actions, including:
***a*. all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.:**
***b*. any attacks on the operation of the e-voting system and its communications infrastructure;**
***c*. system failures, malfunctions and other threats to the system.**

The audit logs produced by all servers and infrastructure components indicate the date and time of the event, and the activity which is being logged. These event logs were available immediately through the monitoring and reporting tool utilised by the Ministry. Attacks and system failures were also recorded and reported immediately, if serious enough, to the relevant staff. The audit logs do not record the aggregate statistics indicated in the recommendation, such as the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, but most of this data is available by aggregating individual entries on the audit system.

The Norwegian Internet voting system complies with this recommendation.

III. Monitoring

FC / 104. The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.

The analysis of recommendation 102 already indicated that the audit system was open to oversight by observers, if they had wished to do so. The explanatory memorandum indicates that the audit system should allow observers to monitor the real-time progress of the election. The log monitoring and reporting tool utilised by the Ministry does allow such real-time monitoring of the progress of the Internet election.

The recommendations covering the verifiability of the overall accuracy of the Internet voting results have already been discussed with reference to the E2E verification mechanisms.

The Norwegian Internet voting system complies with this recommendation.

FC / 105. Disclosure of the audit information to unauthorized persons shall be prevented.

Openness and transparency are fundamental principles for the way in which the Norwegian Internet voting system has been implemented. Observers are allowed high levels of access to the Internet voting system, and to the real-time audit logs produced by the system. Observers are not required to sign confidentiality or non-disclosure agreements and therefore there are no limitations placed on them by the Ministry concerning their publication of data obtained through observation. Given that there is no limitation on the disclosure of this information, it is not possible for the information to be disclosed to unauthorised persons as no unauthorised persons are identified.

The Norwegian Internet voting system complies with this recommendation.

FC / 106. The audit system shall maintain voter anonymity at all times.

The data that is held on the log files contains personal identification data for voters and the transaction that the voters were conducted, for example, the submission of a vote. However, it is not the actual vote value that is stored in the log entry, but a hash function of the vote value. Such hash functions are one-way functions, meaning that it is not possible to determine the value of the vote from them.

By their very nature, audit logs collect data on the voters and it is clear from the logs whether individual voters have voted, when they voted and the IP address from which they voted. This could be considered as violating the anonymity of the voter. However, when the parallel of paper voting is considered, this process also provides exactly the same information to observers.. Therefore, Internet voting is no different from paper voting in the information it provides to observers of the process.

The Norwegian Internet voting system complies with this recommendation.

IV. Verifiability

FC / 107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.

As discussed in recommendation 100, the Norwegian Internet voting system implemented E2E verification mechanisms, which allow independent verification of the correct functioning of the Internet voting system and confirmation that the results generated are accurate. All votes are signed by the ID portal to indicate that the voter has been authenticated by an approved identification mechanism and are signed with the private key of the voter. The presence and legitimacy of the ID portal certificate and private key are checked by the Internet voting system so that only legitimate votes are accepted by the system.

The Norwegian Internet voting system complies with this recommendation.

PC / 108. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.

At a first glance, there is no major difference between this recommendation and the previous one because both of them require the implementation of a comprehensive audit system. However, the explanatory memorandum provides additional explanation of this requirement. For instance, the system would have "to provide open, standard interfaces with comprehensive observation facilities subject to the needs of confidentiality of the vote." Moreover, "the audit system shall be publicly verifiable . . . This requires the ability to prove to third parties that the results are a true and accurate representation of the authentic votes."

These explanations strengthen the idea that three different elements are required to meet this recommendation - the voting system, the audit system and third parties, i.e. observers. Third parties are not only required to have access to the audit system, but to have open standard interfaces with comprehensive observation facilities. The access provided by the Ministry would not seem to comply with the very comprehensive level of access required by this recommendation.

The Norwegian Internet voting system partially complies with this recommendation.

V. Other

FC / 109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.

The Norwegian Internet voting system uses a system of immutable logs with a hash of the previous log entry being part of the subsequent entry on the log file. This means that any addition, amendment or deletion from the log files can easily be identified. The log-entries are also digitally signed at regular intervals to further block any attempts at tampering.

The Norwegian Internet voting system complies with this recommendation.

FC / 110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

The explanatory memorandum adds further to this recommendation, saying: "It is not enough simply to protect the information gathered by the audit system against unauthorised access. It is also necessary to take legal and organizational measures to control the persons in charge or having access to the audit system. Accordingly, anyone having access to the audit system should be subject to an accreditation process."

The Ministry took measures to ensure that access to the log file information was restricted, with only authorised computers allowed access. Access to these authorised computers was also controlled, although in principle it was open to any observers that wished to view log information. None of the log information could be copied and taken away by observers, and likewise, the vote data was only provided to auditors in controlled and supervised environments.

Promis AS, who conducted the audit of the Internet voting system, was not allowed to take any data from Ministry premises. While Promis AS used its own equipment, it was monitored during the process. In addition, secure deletion of all election data, post-audit, was monitored by the Ministry.

In terms of the accreditation requirements mentioned in the explanatory memorandum, all observers must be accredited by the Ministry in order to observe an election in Norway.

The Norwegian Internet voting system complies with this recommendation.

F. Certification

N/A / 111. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation.

According to the Regulations Related to Trial Electronic Voting (art. 27.7), this recommendation is not applicable.

N/A / 112. In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Co-operation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.

According to the Regulations Related to Trial Electronic Voting (art. 27.7), this recommendation is not applicable.