Internet Voting and Individual Verifiability: The Norwegian Return Codes

Jordi Barrat[1], Michel Chevallier[2], Ben Goldsmith[2], David Jandura[2], John Turner[2], and Rakesh Sharma[2]

[1]EVOL2 / eVoting Legal Lab
University of Catalonia / URV
Av. Catalunya, 35, Tarragona (Catalonia) 43002
barratj@tinet.org

[2]International Foundation for Electoral System (IFES)
1850 K Street, NW, 5th Floor,
Washington, D.C. 20006
rsharma@ifes.org

Abstract: The Norwegian return codes, used within an Internet voting project piloted in September 2011, intend to simultaneously achieve both receipt-freeness and individual verifiability. They are delivered as text messages with a code representing the value of a voter's cast ballot, but, according to the Norwegian Government, they would not breach the principle of secrecy, and they are not voting receipts, since the voter could always cancel the vote. However, some international electoral standards, like the *Recommendations on E-voting* from the Council of Europe, clearly forbid an Internet voting system that enables a "voter to be in possession of proof of the content of the vote cast." This paper analyzes the extent to which the Norwegian system complies with this standard and it concludes that there is no contradiction in using a teleological approach.

1 Introduction

Verifiability is one of the key issues that any Internet voting project has to address. As with other remote voting channels (e.g. postal voting), it does not normally provide a voter with any proof that his or her was cast or received as intended. In fact, receipts that can be used to prove the content of a vote are prohibited by some international electoral standards[1], as they facilitate the coercion of voters and vote buying practices.

[1] We will focus our attention on the following recommendation issued by the Council of Europe: Recommendation REC(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 / Legal, Operational and Technical Standards for E-voting. Available at: www.coe.int/democracy [April 24th 2012].

However, voting receipts are still a technically feasible solution and would improve the system's trustworthiness, provided they manage to overcome the problems concerning the secrecy of the vote and the freedom of the voter. While some countries (e.g. the Netherlands) decided to include voting receipts despite their negative effects over such principles, other projects, like the Norwegian one, intend to use voting proofs in a way that does not violate the principles of voter freedom or secrecy.

After a brief outline of the Norwegian Internet voting system (§ 2), this paper will focus on the so-called return codes (§ 3), that is to say, text messages that provide individual verifiability within non-supervised environments. Such mechanisms obviously challenge voting secrecy and freedom principles, but the Norwegian solution intends to overcome both problems with a multiple-voting scheme (§ 4). Finally, this paper will discuss to what extent such codes should be categorized as voting receipts (§ 5) and, therefore, to what extent they meet international electoral standards, like the recommendations from the Council of Europe, which prohibit the provision of such receipts to voters.

2 A Brief Outline of the Norwegian Internet Voting System

Norway piloted Internet voting for the first time during its municipal and county elections in September 2011. It was the first binding and official use of Internet voting after several trials during the period of technical and legal developments. Ten municipalities were selected to conduct the pilot, and after a broad evaluation and a general political assessment are carried out in 2012, the Norwegian Parliament – *Stortinget* – will decide whether or not to continue using Internet voting in future elections.

Internet voting was only used as a supplementary channel for casting a vote and was available for one month during an advance period of voting ending on the Friday before election day. Voters in the pilot municipalities were also able to use traditional paper-based ballots, which were available during the early and advance voting period and on election day (Ri11).

Norwegian electoral authorities conducted detailed assessments on how other countries had addressed the challenges generated by Internet voting and decided to both adopt some of the measures used by other countries and to include new features aimed at improving existing Internet voting solutions. As in Estonia, the Norwegian solution allowed repeat voting, whereby voters could cast repeated Internet votes. Internet voters were also able to cast paper votes during the early and advance voting period or on election day.[2] The final tally of votes only included the last Internet ballot (I-ballot) cast, unless a paper-based ballot (p-ballot) was cast, in which case the paper ballot was counted and the I-ballots discarded.

[2] The Estonian Internet voting system does not allow Internet voters to cast a paper ballot on election day, but apart from this the same possibilities are available in Estonia.

Transparency was another issue that the Norwegian electoral authorities intended to qualitatively improve in regards to previous Internet voting systems [see SVK11]. While other countries face criticism regarding the way they handle electoral information, Norway requires open-source programs, and its Internet voting project is based on a general license that enables anybody to download both the source code and other relevant documentation for non-profit purposes. The government also claims that all the information linked to the project is published.

Finally, the ability to verify that the system accurately reflects the will of the voters in the results that it produces is a common source of concern for Internet voting systems. Norway claims that its Internet voting system can be submitted to a software independent End-to-End (E2E) verification that, *inter alia*, includes Zero-Knowledge Proofs (ZKP) for the final cleansing and mixing stages. Moreover, Norway includes the so-called return codes, whose purpose is to allow individual verifiability that the Internet voting system has received the vote as cast by the voter from the voting client. The next section (§ 3) will describe such codes and the following section (§ 4) will assess how such codes may comply with electoral standards that do not allow voting receipts for remote voting channels.

3 Internet Voting, Individual Verifiability, and the Norwegian Return Codes

The return codes used in the Norwegian Internet voting system were simply text messages sent to the voter immediately after he or she had cast a ballot. The message included a code representing the party list that the voter had cast a vote for and indicated the number of personal votes that had been cast. An SMS message was sent each time an Internet vote was cast. Before the election, each voter received a polling card containing a list of codes for each party list on the ballot for the municipal and county elections. The combination of codes assigned to the party lists on the ballot was unique for each voter. Therefore, when the voter received the SMS message with the relevant code, he or she could refer to the polling card to determine whether the code represented the cast ballot. If the code did not match, representing a clear technical flaw in the system, the overall electoral process could continue because the voter would still be able to cast another I-ballot, which would hopefully be recorded correctly; the option to vote by paper ballot would have also been an option.

Such codes clearly improve the verifiability of the voting system as they provide proof that the system received the vote as cast and that it was cast as intended. However, it is only a partial verifiability because return codes do not prove that the vote is stored as cast or that it is included in the count as it is stored. However, the E2E mechanisms mentioned above intend to complete this sequence of verifiability encompassing all the electoral stages. With the challenges that these return codes generate in mind, the following sections will analyze how the return codes address the protection of the secrecy of the vote (§ 4) and to what extent they comply with the standards that preclude the use of voting receipts for remote voting projects (§ 5).

4 Return Codes and Vote Secrecy

Regardless of whether return codes are used or not, Internet voting always entails serious concerns about the secrecy of the vote and the freedom of the voter. This voting channel is normally used in uncontrolled environments, that is to say, a situation in which there are no means to guarantee that the voter is free from external influence in casting his or her ballot. There is no voting booth to ensure secrecy or official supervision to ensure that the voter is alone when voting, and therefore the vote might be submitted under pressure from external forces, which would breach both to the voter's freedom to vote as well as the secrecy of the vote[3].

Return codes only serve to strengthen these concerns. These SMS messages would simplify the task of coercers and vote-buyers because they need only ask the voter to provide the appropriate proof generated by the Internet voting system itself. Unless the voter manages to send a faked SMS message, which is difficult to do because they are sent by the server itself, the coercer would not be compelled to directly supervise the voting session to know how the voter cast his or her ballot.

Taking these risks into account, most Internet voting projects do not include individual verification means. They assume that the advantages linked to remote voting channels (e.g. easier access to the voting process for some groups) justify not being able to replicate some guarantees that exist in supervised voting environments (e.g. direct supervision). From this point of view, Internet voting can be seen as similar to postal voting. Postal voting is allowed in many Western democracies; despite being unable to guarantee the freedom of the voter and the secrecy of the postal votes cast, it is seen as a legitimate voting channel[4]. Postal voting does not provide any means by which the voter can individually verify that his or her vote has been received or counted as cast. While Estonia and some Swiss cantons (e.g. Geneva) use such an approach, the Netherlands and Norway sought to implement Internet voting with mechanisms for individual verification.

The *Rijnland Internet Election System* (RIES) project was canceled as a result of the overall re-evaluation conducted by the Dutch electoral authorities after weaknesses discovered by an NGO in electronic voting machines previously used in the Netherlands. The cancellation of the Internet voting system was a side effect of these concerns as the main criticism was related to electronic voting machines and not the Internet voting channel.

---

[3] In Norway, such prevention is even more important due to previous incidents where members of some minority groups were thought to have exercised undue influence over some voters. See [Sm10] for a detailed assessment on how Internet voting would not meet electoral principles directly linked to the secrecy of the vote.

[4] The Venice Commission issued a report [Ve04] where both postal and Internet voting, as remote channels, were assessed to determine whether they complied with international electoral standards. The Commission concluded that they did meet international standards provided that certain features were included, but that individual verification was not one of the requirements that any voting channel needed to include.

Despite this, the RIES project's verification mechanisms are worth noting. Once an Internet ballot was cast, the REIS system provided the voter with what was called a 'technical vote', which was an encryption code for the vote cast. When all voting was completed, the election authorities published a list of the codes used with an indication of the ballot option made for each technical vote. This allowed for individual verifiability by the voters, who could see that their vote was recorded correctly, as well as universal verifiability, as anyone could verify the overall results of the Internet votes by tallying the votes for each ballot option.

This feature was seen as a great innovation because it provided the voter with a means to directly verify a process that is normally opaque for the average citizen. However, these advantages also had a critical trade-off with serious implications for the secrecy of the vote. As the OSCE/ODIHR recalled, "if a voter ... discloses his authorization code and his technical vote, anyone can determine his/her actual vote by simply trying all the candidate identities until a match is obtained" [Os06: 15; see also Jo07: 20-25]. The technical vote would no longer be a neutral code as it would reveal the value of a given ballot while also linking the vote to an individual. Therefore, within this schema, individual verifiability would only be feasible when accepting that the secrecy of the vote could be breached in a way that is not possible with postal voting.

The Norwegian project took into account the Dutch experience and tried to address such challenges through repeat voting. The argument is that the voter is able to cast as many ballots as he or she wants, either by Internet or by paper means, with only the last Internet vote or the paper vote being included in the results. The coercer would therefore have no way of knowing if the ballot cast in his or her presence or the return code presented to him or her represented the ballot that was actually counted for that voter.[5]

While Estonia has multiple voting and the Netherlands individual verifiability, Norway mixes both features as a way to simultaneously achieve two goals: a sound protection of the secrecy and freedom of the vote and individual verifiability (or at least a limited version that intends to guarantee that each ballot is received as cast and cast as intended). Return codes do offer proof linked to a certain ballot, but, due to repeat voting, there is no way to check which ballot is included in the final tally [see Bu11: 17-20].

[5] This argument is not without its critics. Repeated Internet ballots might also be tracked by the coercer, as he or she could retain the control over the mobile phone that receives the return code, Internet ballots cast during the very last stage of the voting period would preclude the chance to revoke them by another Internet vote and finally, as recalled by Eivind Smith, the social context may also become a key feature. Although theoretically any voter can freely go to a polling station and supersede a previous ballot, "(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" [Sm10: 12 (edited version)]. Therefore, from this point of view, neither repeated Internet ballots nor paper votes would be good solutions to overcome the problems that return codes create for the secrecy of the vote. However, a comparative perspective, which would take into account how other voting channels (e.g. postal voting, supervised polling stations) protect this legal principle, might emphasize the advantages of having multiple options to cast a ballot.

Moreover, there are also concerns about the anonymity of the vote when return codes are in use. It is worth questioning how the application can send specific data about the value of a voter's ballot while maintaining the anonymity of the vote. Following the explanations of the Norwegian authorities, such a paradox is solved through crypto architectures [see Gj11 and Gj10]. The ElGamal system allows the return code generator (RCG) to establish a dialogue with the vote collection server (VCS), retrieve enough data about a ballot, and send back the relevant code without breaching anonymity. It relies upon an extremely complex crypto systems, but it is worth recalling that even without such return codes, many Internet voting projects also include digital signatures that protect anonymity with double envelope methods. Therefore, ElGamal only represents a more developed crypto system that also allows the delivery of return codes in order to provide a level of individual verifiability.

5 Return Codes as Voting Receipts

Once accepted that the provision of return codes, allowing for individual verifiability in a manner that still protects the freedom and secrecy of the vote, could be a solution for some Internet voting projects, there remains a legal barrier as some international electoral standards prohibit voting receipts when using remote voting channels. The Council of Europe's *Recommendations on E-voting* is a good example as the 51st recommendation states, 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".

While the Council of Europe recommendations are precisely that, only recommendations, they have a special legal status for the Norwegian pilots as they were incorporated into the electoral legal framework through the Regulation Relating to Trial Electronic Voting. Faced with such a clear statement in recommendation 51[6], it is worth wondering to what extent the Norwegian return codes manage to comply with these standards. Although the Norwegian solution might be valid from technical and social perspectives, a legal assessment is always necessary and such standards clearly identify a potential problem[7].

[6] Moreover, other recommendations also seem to reject the use of return codes. The 17th recommendation requires anonymity of the ballots being inserted into the ballot box and "that it is not possible to reconstruct a link between the vote and the voter". The 35th recommendation emphasizes the same goal requiring that "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". Finally, the 19th recommendation includes a general statement regarding the protection of secrecy while managing electoral information. While the 35th only requires conditional ballot secrecy, that is to say, a feature that may be breached under some circumstances, the other two require absolute secrecy [see Jo04].

[7] The Norwegian legal framework also requires an electoral system with "frie, direkte og hemmelige valg" (§ 1-1 Election Act; translation: free, direct and secret elections; see also § 10-5), but the system did not foresee individual veriability for remote voting channels. Citizens using postal voting did not receive a proof of content of his/her vote.

The Council of Europe recommendations are accompanied by an explanatory memorandum, that helps to interpret and contextualize the recommendations. The memorandum does not specifically discuss the option of individual verification for remote voting in unsupervised environments. However, when it analyzes the risks linked to the web application, the browser, and the software, some comments can clearly be applied to the Norwegian return codes: "The web application should not allow the user to retain a copy of his or her vote. This means that the application should not offer the functionality of printing, saving or storing the vote or (part of) the screen on which the vote is visible ... At the very least, there should be no storing of information [by the browser] after the voter has finished casting the vote."

Despite not explicitly prohibiting text messages sent back to the citizen by the voting servers, it seems obvious that the Norwegian return codes are an analogous scenario and it is necessary to assess whether they comply with this recommendation from the Council of Europe.

The Norwegian Government claims that its Internet voting project meets this requirement as return codes should not be understood as voting receipts [Bu11: 20]: they would not be able to provide proof of the content of the vote cast because the voter always has the chance to substitute such a ballot with another I-ballot or with a p-ballot (which may have even been cast earlier than the I-ballot). A return code would not be a voting receipt, whose use is forbidden according to the *Recommendations*, and therefore this recommendation would pose no problem for the implementation of the Norwegian Internet voting project.

To our understanding, such an interpretation is hardly acceptable. As explained in the previous section, a return code is always linked to a set of codes that had been given to each voter in conjunction with his or her polling card. Given that each code refers to a given candidature, the return code is disclosing the content of this ballot and suffices as "proof of content of the vote cast". The fact that such a ballot might not be the final one included in the tally would not be important for the following reasons.

First of all, (i) it is worth noting that the wording refers to the vote "cast" and not to the vote "tallied". A scenario based on repeat voting allows several votes to be cast by the same voter, with only one being finally tallied. Each ballot cast (not yet tallied) will generate the relevant return code that will disclose the value of this ballot. It will therefore function as proof of content of the vote cast.

Moreover, even if we prefer not to make a distinction between votes cast and tallied[8], there is another argument (ii) against the compliance of the Norwegian return codes with this recommendation. Given that the wording only refers to the voter, and not to third parties, it is obvious that the voter will know which one of the votes cast would be the final one included in the tally. Therefore, at least one of the return codes would be a full proof of content of a ballot cast and also tallied.

[8] The system would *receive* several ballots, but only one will be finally *cast/tallied.*

If the voter cast a p-ballot, the return code would never be linked to a ballot finally tallied, but the previous explanation would still be valid for those voters only casting I-ballots and therefore, at least for this group of voters, return codes would offer full proof of the content of a vote cast and also tallied, precisely what the recommendation intends to forbid.

Finally, (iii) if the return codes are not voting receipts, as the Norwegian government states, it is worth wondering what their purpose is. Theoretically return codes are thought to enhance individual verifiability, but, if they cannot provide proof of the vote being cast, there will be no verification, and they become meaningless.

To our understanding, the Norwegian return codes do provide proof of content of the vote being cast and therefore an initial assessment would likely find that they do not comply with the 51st recommendation from the Council of Europe. However, there are other ways to approach this issue and, as we will discuss below, return codes may meet the Council of Europe's recommendations provided we adopt a less literal interpretation of their wording.

Hermeneutic theories argue that literal interpretation is not always the best way to understand the actual meaning of legal rules and that it is necessary to balance literal interpretations with other points of view. Historical, systematic, authentic, and teleological methods are normally used to discover the intended meaning of a rule and to achieve its fairest implementation [in general, see Al83].

Regarding the 51st recommendation of the Council of Europe, where a literal method clearly leads to a breach when using return codes, it is worth using the teleological strategy in order to discover the actual purpose of the recommendation. The key point consists in making a distinction between the role of the voter and that assumed by third parties[9]. As we have seen above, the voter will always know whether the return code is a real voting receipt, that is to say,, proof of content of a ballot cast and tallied, but, thanks to multiple voting chances, third parties will never have the same certainty that a given return code actually represents the vote that will be tallied. They will never know whether a return code has been canceled by another I/p-ballot. Only the voter knows this, and he or she has no way of proving it.

Following this reasoning and taking into account the wording of the recommendation, the Norwegian system does not provide *at least to third parties* a proof of content of the vote cast. The voter does receive such proof but not third parties.

If we follow a literal method of interpretation, such a distinction has no impact because the recommendation only refers to the voter and not to third parties. It forbids providing proof of content to the voter and as we have already seen that return codes only meet this

[9] Please note that this meaning of third parties does not include backend users. They will always be able to reveal the content of a given ballot, but a proper separation of duties as well as other technical safeguards would address this risk. On the other hand, other types of third parties, like relatives or similar potential coercers, may use return codes in order to reveal the value of a given vote, but in this case, both a proper separation of duties and other technical safeguards would be meaningless.

requirement with respect to third parties but not the voter. Douglas Jones reached the same conclusion when assessing whether some e-voting systems may comply with this recommendation: "This rule prohibits cryptographic systems such as that being developed by VoteHere (Andrew Neff and Jim Adler) and SureVote (David Chaum). These systems prove to the voter, in the privacy of the voting booth, that the receipt contains their vote, but they do not provide, to the voter, sufficient information to prove to anyone else how they voted, using that receipt" [Jo04] [10].

However, using a teleological method, we will easily discover that the recommendation does not forbid a proof *only* given to the voter. What it actually rejects is a proof that might be given to third parties in order to verify whether the voter has correctly followed the instructions by someone trying to coerce a voter or buy votes. If the return code only provides information, which is only valuable to the actual voters, its data is not dangerous for maintaining key electoral principles like the secrecy of the vote and freedom of the voter. Obviously return codes can always be given to third parties, but with multiple voting options, they are rendered meaningless to those parties because the return codes do not show further votes or cancellation of the vote. Such limited use of return codes would create no concerns while significantly enhancing individual verifiability[11].

McGaley and Gibson share this opinion and their approach is quite interesting because they intend to restructure CoE's document in its entirety, aiming to minimize its internal contradictions. In their analysis of both the secrecy of the vote and the 51st recommendation, their final suggestion adds slight nuance to the literal wording of the Council of Europe's recommendation. Significantly, Mcaley and Gibson's revision of the 51st recommendation includes the difference between the voter and third parties, which did not exist in the original: "The voter shall not be allowed to retain possession of anything which could be used as proof *to another person* of the vote cast" [MG06: 10, italics added for emphasis]. Although McGaley and Gibson do not comment on such nuances, it seems clear that they interpret this recommendation with a teleological approach that permits some means of individual verification only for the voter.

In our opinion, it makes little sense to consider the Council of Europe's 51st recommendation as being only applicable to the voter because the risk that it intends to avoid only exists if the proof of content can be transferred to third parties. Only when the vote's content can be proven to a third party does a voting receipt make voters susceptible of voter coercion or vote buying. When the voting system includes features

[10] Both systems emphasize that e-enabled remote voting systems might always include a non-remote individual verifiability by using voting booths where each voter will receive data about his or her ballot without being submitted to any external pressure. Note, however, that such solutions have to admit a non-remote stage so that individual verifiability and a fully remote procedure will not be feasible. However, the Norwegian project aims to join both features.

[11] Wolter Pieters adds an interesting nuance to coercion resistance systems that would only exist if people were not "able to prove how they voted, *even if they want to*" [Pi06: 2; italics added for emphasis]. Again, if we apply such meaning to the Norwegian case, the first perception is misleading. At a first glance, return codes would not be admitted by Pieters as proper coercion resistant means because they would allow the voter to prove how he or she had voted. The system does not automatically preclude such an option, what it is envisaged by Pieters, but, even if the voter wants to reveal how s/he voted, the system will always render this decision meaningless because the potential coercer will never be sure whether the voter can be trusted.

such as multiple voting options and the primacy of the p-ballot, which deletes the dangers of a voting receipt being transferred to third parties, the fact that the voter is in possession of a proof of content is not important. Such return codes may breach the literal wording of the Council of Europe's 51st recommendation but using a broader legal assessment that includes a teleological approach, one can reasonably conclude that return codes fall well within the boundaries of the recommendation's goal.

6 Concluding Remarks

The Norwegian Internet voting project aims to improve the management of remote voting channels with some new features: a transparent policy that publishes all the relevant documentation, a software independent verification system that includes E2E tools, and voting receipts that intend to provide partial individual verifiability to each voter. These steps will likely become important benchmarks in the provision of Internet voting systems elsewhere.
This paper has focused on the so-called return codes. The discussion is based on whether such components may breach the secrecy of the vote and whether they comply with international standards that prohibit the use of a voting receipt for remote voting channels. The first issue is resolved by mixing return codes with multiple voting so that potential coercers will never know whether the code links to a counted ballot.

The second problem requires the reinterpretation of such standards concerning e-voting. A literal interpretation may lead to the conclusion that any proof of content provided by a remote voting system to the voter is prohibited. However, a teleological method seems more appropriate in order to discover the actual goal of the Council's recommendations. Applying such an approach leads to the conclusion that what is forbidden is the ability to use a voting receipt to prove to third parties the content of the vote, not proof only of value to the voter. If the return codes are meaningless for third parties, as they are in the Norwegian Internet voting system, they can be considered voting receipts while still fully meeting the requirements of international standards like the Council of Europe's *Recommendations on E-voting*.

Bibliography

[Al83] Alexy, R.: Theorie der juristischen Argumentation: die Theorie des rationalen Diskurses als Theorie der juristischen Begründung. Frankfurt am Main, Suhrkamp, 1978 (translation: A Theory of legal argumentation: the theory of rational discourse as theory of legal justification. Oxford, Oxford University Press, 1989)

[Bu11] Bull, C.: Safety first! Verifiability in the e-vote 2011-system. In: E-voting Conference. Oslo, Ministry of Local Government and Regional Development, 2011.*www.regjeringen.no/upload/KRD/Prosjekter/e-valg/e_vote_conference/ ChristianBull.pdf* [November 30th 2011]

[Gj11] Gjøsteen, K.: The mathematics of Internet voting. Oslo, Kommunal- og regionaldepartementet, 2011. *www.regjeringen.no/upload/KRD/Prosjekter/evalg /e_vote_conference/Gjosteen_evalgskonferanse.pdf* [November 10th 2011]

[Gj10] Gjøsteen, K.: Analysis of an Internet voting protocol. In: Cryptology ePrint Archive - Report 2010/380. *eprint.iacr.org/2010/380.pdf* [February 11th 2012]

[Jo09] Jones, D.: Some Problems with End-to-End Voting. In: End-to-End Voting Systems Workshop. Washington D.C., National Institute for Standards and Technology (NIST). *www.divms.uiowa.edu/~jones/voting/E2E2009.pdf* [December 23rd 2011]

[Jo07] Jones, D.: The Impact of Technology on Election Observation. In: VoCom. Portland, VoComp. *www.divms.uiowa.edu/~jones/voting/vocomp07.pdf* [December 23rd 2011]

[Jo04] Jones, D.: The European 2004 Draft E-Voting Standard: Some critical comments. Department of Computer Science / University of Iowa. *www.divms.uiowa.edu/~jones/voting/coe2004.shtml* [February 11th 2012]

[MG06] McGaley, M.; Gibson, J. P.: A Critical Analysis of the Council of Europe Recommendations on e-voting. In: EVT'06. Accurate / Usenix, 2006. *www.usenix.org/events/evt06/tech/full_papers/mcgaley/mcgaley.pdf* [February 11th 2012]

[NS11] Nore, H.; Stenerud, I.: The good, the bad and the terrible of verifiable electronic voting. In: VoteID11 / 3rd International Conference on E-Voting and Identity. Tallin, 2011.

[Os06] OSCE/ODIHR: The Netherlands. Parliamentary Elections 22 November 2006. OSCE/ODIHR Election Assessment Mission Report. Warsaw, OSCE/ODIHR. *www.osce.org/odihr/elections/netherlands/24322* [24th December 2011]

[Pi06] Pieters, W.: "What proof do we prefer? Variants of veriability in voting", Workshop on Electronic Voting and e-Government in the UK, Edinburgh: e-Science Institute, pp. 33-39. *doc.utwente.nl/65114/1/Verifiability.pdf* [February 11th 2012]

[Ri11] Riise, M.: The Norwegian e-Voting Trials Legal Framework, E-Voting Conference. Oslo, Ministry of Local Government and Regional Development, 2011. *www.regjeringen.no/upload/KRD/Prosjekter/e-valg/e_vote_conference/ MarianneRiiseE-voting_conf_11092011.pdf* [February 16th 2012]

[Sm10] Smith, E.: Hemmelige elektroniske valg? In: Lov og Rett, 49(6), pp. 307-323.

[SVK11] Spycher, O.; Volkamer, M.; Koenig, R.: "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting", VoteID11 / 3rd International Conference on E-Voting and Identity. Tallin, 2011. *e-voting.bfh.ch/app/download/ 5022330961/SVK11.pdf?t=1314955570* [February 16th 2012]

[Ve04] Venice Commission: Report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe. Strasbourg, European Commision of Democracy Through Law. *www.venice.coe.int/docs/2004/CDL-AD%282004%29012-e.asp* [October 28th 2011]