VALG

KOMMUNESTYRE- OG
FYLKESTINGSVALG

REPORT TO
OSCE/ODIHR

RESPONSE TO OSCE’s EET REPORT OF
2 March 2012
NORWAY

7 FEBRUARY 2013

KOMMUNESTYRE- OG
FYLKESTINGSVALG 2011

INTRODUCTION

During the local government elections in 2011, Norway conducted an Internet voting pilot in ten municipalities. At the invitation of the Norwegian Government, OSCE/ODIHR decided to send an Election Expert Team (EET) to follow these Internet voting pilots.

Electronic voting poses new challenges and requires new approaches when it comes to election monitoring: Therefore, the EET was invited to follow the use of new voting technologies (NVT) from an early stage and through the different stages of the election. The mission was both to assess how the Internet voting pilot was conducted, and to provide recommendations and advices for possible improvements.

Norway's electoral system enjoys great confidence, but new voting technologies gives increased demands for transparency and accountability, amongst other reasons because different stages of the voting process may not be easy to understand or observe for the naked eye. The Ministry of Local Government and Regional Development is therefore very pleased that OSCE had the opportunity to follow the Internet voting pilot during the 2011 elections.

After an initial assessment visit by OSCE, the team conducted six visits during the various stages of the Internet voting, including the setup and configuration, the start and close of the voting, the counting of electronic votes, and data destruction. The report from the EET' was presented and published on 2 March 2012.

It has been very useful and beneficial for the Ministry to cooperate with OSCE's expert team in conjunction with the Internet voting pilots in 2011. We would also like to thank ODIHR office for a useful and constructive follow-up meeting in Warsaw in June 2012, where we received valuable input to the process ahead. Both the report and this input will be important when we now are planning a new Internet voting pilot during the 2013 parliamentary election. The pilot will be conducted in twelve municipalities, including the ten municipalities that participated in 2011.

REQUESTS AND FOLLOW UP

Below is a review of OSCE's requests, advice or recommendations in the EET report and how the Ministry is planning to follow up on these recommendations.

LEGAL FRAMEWORK AND MANAGEMENT (1-2)

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

We agree that it would be favourable to include certain procedures and time plans in the legal framework. However, as it is not common within the Norwegian legal tradition to include formalized procedures and a comprehensive time plans in the legal framework, this will mainly be considered for certain important activities. We will examine closely which activities that should be included in the regulations, based on the experiences from the previous pilot.

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

These are important issues, and they will be assessed.

THE INTERNET VOTING ELECTORAL PROCESS (3-9)

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

The Ministry aim at using the final version of the source code in the open non-binding test election that takes place in July 2013. The test election will be available to all voters in the twelve pilot municipalities.

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

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

In 2013, we aim at publishing the command level protocols prior to the elections. In addition, we have started the process of improving the documentation of the system components. This would make it easier to understand the functioning of the system.

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

The Ministry will improve the routines for the printing of the polling cards, to ensure that the printing process is more resilient against errors. The goal is to ensure that no voters living in the pilot municipalities will receive polling cards containing missing or faulty return codes in conjunction with the parliamentary election in 2013.

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

The Election law defines on which grounds the voter register can be updated, and how to deal with late updating of the voter register is also covered in this law. The affected seven Internet votes were therefore treated in the exact same manner as paper votes would have been treated. We will consider possible amendments to the regulations.

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

The Internet voting software has now been updated, to eliminate the error that affected ten electronic votes in 2011. The update has been tested, and ensures that the e-voting client will refuse a voter to cast a vote that would be unreadable after decryption. The voter will instead get a message stating that something went wrong, and will be asked to try casting an electronic ballot again. We agree that the e-voting regulations should define the grounds for invalidation of votes.

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

We agree with OSCE that formalizing the process of data destruction in both scope and timeframe will increase the transparency of the Internet voting process even more. We therefore aim to include at the very least the time schedule for the process of data destruction in the e-voting regulations for the pilots in 2013.

SECURITY AND SECRECY OF THE VOTE (10- 14)

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

We agree that the routines can be improved in this area, and this recommendation will be given priority in the longer run. During the 2011 pilots many duties were performed for the first time, and unfortunately we were therefore not able to define and document a strict separation of duties at all levels.

For the pilots in 2013, we aim at documenting and defining a strict separation of duties at all levels. In addition, we will consider how we can include the most crucial of these in the electoral regulatory framework.

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

Although it was not possible for the Ministry to construct the decryption key prior to Election night, we agree that the documentation describing this must be better documented.

We will improve the documentation for the management of the secret election keys, and specify detailed procedures showing how the decryption keys will be treated. We will also examine if it would be beneficial to include some of these routines in the legal electoral framework as well.

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

We agree that this would reduce the complexity in set-up, configuration and testing. However, we are not familiar with how this could be done without at the same time conflicting with maintaining a stricter separation of duties.

However, in the long term, other encryption models may arise. If more pilots are conducted beyond 2013, we will re-consider this recommendation and examine if and how the encryption model then could be improved.

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

We will examine how we can increase the voters' awareness of such risks, and to inform them on how to protect their computers against such malicious software. We will consider if it would be sufficient to inform the voters as part of the e-voting client and on the Ministry's web site.

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

As a part of the risk assessment associated with the next Internet voting pilot, we are going to determine how to involve and collaborate with such relevant agencies. We are already in a dialogue with Norway's largest ISP, Telenor, which could assist us during for instance a DDOS-attack. We are also in dialogue with NorCERT (coordinates preventative work and responses against IT security breaches), which could contribute with both monitoring and early warning regarding internet security.

TRANSPARENCY AND ACCOUNTABILITY (15-20)

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

Our goal in 2013 will be to publish the final version of the source code well before the opening of the polls. If any bug fixes are necessary after the publishing date, information about the update, the source code and an explanation of why such an update must be done, will be clearly stated on the Ministry's web site and on the web site where the source code is published.

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

For the pilots in 2013 we will priority to increase the accountability and transparency by other means than certification, like improving the documentation and publishing the final version of the source code at an earlier stage. If the system had not been verifiable, we would have prioritized certification at an earlier stage. Certification of the Internet voting system will be given priority if it will be used on a non-pilot basis beyond 2013.

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

We will examine if the regulations need further clarifications in order to explicitly allow for such audits.

In addition, we aim at improving the way in which third parties and observers can assess that the conduct of the certain crucial processes functions as intended. This may be relevant for, but not limited to, processes such as the printing of the polling cards and generation of the secret keys.

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

To provide further transparency of the Internet voting process, we will publish an election calendar including the dates for the most crucial and important activities in conjuction to the Internet voting pilot. This will be done in advance of the opening of the polls in 2013.

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

Political party representatives and domestic non-partisan observers will be invited to a training session during spring or summer 2013. The training session will include information of the functioning of the e-voting system, as well as information on how the different stages of the Internet voting process can be observed.

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

We agree that a full review of the impact of return codes is of importance, and have already conducted a thoroughly external review of the return codes impacts on the secrecy of the vote. This review is part of the assessment "Norwegian e-voting project: Compliance with International Standards"[1].

The review concluded that the return codes do not conflict with the secrecy of the vote, and that it is still only the voter that knows which vote that will be counted-as-cast. In addition, the assessment concludes that the return codes also comply with the relevant standards on secrecy found in the Council of Europe's legal, technical and operational standards on e-voting.

[1] The assessment is conducted by International Foundation of Electoral Systems (IFES) and can be found at http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic7_Assessment.pdf

On a longer term, if more pilots are conducted beyond 2013, we are also planning to conduct a full review of the return codes impacts on security.

In addition, we aim at conducting the internal universal verification of the count at an earlier stage in 2013 than in 2011. However, when it comes to the timeliness of the external universal verification of the count, it must be up to these external parties to decide themselves when to do this, although we can encourage third parties to perform this verification earlier.