Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting

Oliver Spycher[1,2] and Melanie Volkamer[3] and Reto Koenig[1,2]

[1] Bern University of Applied Sciences, CH-2501 Biel, Switzerland
oliver.spycher@bfh.ch, reto.koenig@bfh.ch
[2] University of Fribourg, CH-1700 Fribourg, Switzerland
oliver.spycher@unifr.ch, reto.koenig@unifr.ch
[3] TU Darmstadt, CASED, Mornewegstrasse 34, D-64293 Darmstadt.
melanie.volkamer@cased.de

Abstract. The short history of e-voting has shown that projects are doomed to fail in the absence of trust among the electorate. The first binding Norwegian Internet elections are scheduled for fall 2011. Notably, transparency is taken as a guideline in the project. This article discusses transparency and other measures the Norwegians apply that are suited to establish profound trust, i.e. trust that grounds on the system's technical features, rather than mere assertions. We show whether at all, how and to which degree these measures are implemented and point out room for enhancements. We also address general challenges of projects which try to reach a high level of transparency for others as lessons learned.

1 Introduction

Voting technology comes with many promises. While some see the potential of saving significant time and money, others will hope to increase voter turnout due to easy and flexible participation. Also, voters may expect mechanisms to validate their ballot and avoid casting an invalid vote. Although many stakeholders in voting are likely to benefit from such features in some way, voting technology still faces much opposition. Correspondingly, only few countries introduced internet voting and so far only Estonia has offered their citizens to vote through the internet at nation-wide parliamentary elections. Critics most commonly express their doubts regarding the integrity of the outcome of elections, arguing that citizens need to be able to verify the correct functioning of the electronic procedure based on the processed data. Accordingly, mistrust towards the Irish voting machines culminated in the cancelation of the respective project shortly before going live. For the same reason Germany and the Netherlands have persistently banned their voting machines from use at political elections. Trust in voting technology that lasts can only be established when operating a system that complies with high security standards. On the other hand, even the perfectly secure system alone will hardly increase any trust among the public. In order to avoid the fate of the voting machines in Germany, the Netherlands and Ireland, we must not only ask ourselves how to make systems that are more secure. The focus should rather lie on the primary, superordinate question of how to establish trust itself.

Soon we may add Norway to the list of countries offering internet voting for governmental elections. The Norwegian government's motivation is to increase the availability of the voting system and to reduce costs in the long term. Binding trials of internet voting are planned in ten municipalities for the 2011 local elections in September. Afterwards, the parliament will decide whether to continue the project and enable remote electronic voting for federal elections in the future. The e-voting project called E-valg is currently widely discussed and particularly special due its open information policy. Their motivation for transparency is to increase trust among experts but also among voters in general.

We have taken advantage of the open information policy and expose some implemented techniques that are suited for establishing trust as per [27]. [27] identifies appropriate measures to establish trust not only among experts but also among a non-technical audience. These measures comprise: *transparency*, *implementing separation of duty*, *enabling verifiability*, *enabling vote updating*, *evaluating the system according to international standards* and *test elections*.

This set strongly grounds on the 'Guidelines on transparency of e-enabled elections' published by the Council of Europe in [19], the discussion in [26] on advantages and disadvantages evaluation and certification versus verifiability, and the recommendation on the information that an e-voting project should publish in [24]. The objective of this paper is twofold: On one hand we validate the recommended measures meant to establish trust [27], by analysing a concrete Internet voting project. At the same time we reveal whether and to which degree the Norwegian Internet voting project adheres to these recommendations.

After providing the necessary background on Norwegian Internet voting in Section 2, we will revisit and briefly introduce each measure in the subsequent sections. We summarize how these measures are addressed and expose room for enhancements where it seems applicable.

2 The Norwegian Internet Voting Project and System

The main manufacturer of the voting system is Scytl, a company specialized in Internet voting solutions. The Norwegian project distinguishes itself from other electronic voting projects in many ways: for instance they put an emphasis on verifiability, they address the untrustworthiness of home computers, publish system specifications, security analyses, the source code and many other project related documents. Furthermore, they are working towards an evaluation according to the Common Criteria[1].

The rest of this section provides an overview of the system. The level of detail is meant to suffice for our argumentation in the coming sections.

2.1 System Description from the Voters Perspective

The voters' perspective of the system is rather simple and convenient. They authenticate using their MinID[4] account (two-level authentication). After placing the right mouse clicks to select their preferred parties and candidates and cast their vote, they receive an SMS containing personalized verification codes corresponding with the vote received by the voting servers (one code representing the selected party and one code per candidate position of the party list). If the codes correlate with the expected codes of the voting card they previously received by postal mail, voters may be confident that their vote has reached the servers as intended.

2.2 System Entities

The system comprises the following key components.

1. Voter's Computer: Downloads and runs the voting client application (Java Applet).
2. Electoral Roll (ERoll) Service: Holds information on the electorate.
3. Authentication Service: Holds and sends voter credentials to the voter's computer (upon successful authentication by MinID). The credentials include a private key for signing votes.
4. Vote Collector Service (VCS): Stores encrypted votes.
5. Return Code Generator (RCG): Computes the information required by the voter to verify the correct inclusion of her vote in the ballot box. She receives that information by SMS.
6. Key Management Service (KMS): Creates and distributes keys. It is also in charge of establishing the private key used for decrypting the votes. The keys form VCS are generated on KMS-VCS, the ones for RCG on KMS-RCG.
7. Cleansing Service: Discards electronic votes (e-votes) of voters that cast a paper vote (p-vote).
8. Mix-Net (as described in [18]): Mixes and re-encrypts the encrypted votes signs the output. The mix-net consists of four nodes that form a LAN.
9. Decryption / Counting Service: Decrypts and counts the votes.

[4] MinID is a well established service in Norway. It can be used to access more than 50 online services from various Norwegian public agencies [11]

Except for the ERoll service (developed by Ergo), they all run software developed by Scytl.

The main task of the Electoral Board (EB) is to securely store shared of the decryption key and to initiate the Decryption / Counting Service. There are also auditors involved to verify the integrity of the ballot. The RCG is operated by The Directorate for Civil Protection and Emergency Planning (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 Brønnøysund Registry Centre, which is subordinate to The Ministry of Trade and Industry. The isolated components of the system (KMS, cleansing service, mix-net and decryption service) are located in the Crisis Support Unit, a high security facility subordinate to The Ministry of Justice and located in Oslo, but the servers are managed by security cleared representatives of The Ministry of Local Government and Regional Development (KRD).

2.3 Setup

The following steps are conducted prior to the voting phase.

1. Establish Electoral Register: Eligible voters are included in the ERoll.
2. Key Generation:
   (a) The KMS generates and distributes RSA key pairs for all components to sign messages.[5] Voters' key-pairs denoted as (h_{voter}, s_{voter}) are saved in the KMS.
   (b) It also generates ElGamal key pairs for VCS (h_{VCS}, s_{VCS}), for RCG (h_{RCG}, s_{RCG}) and for EB (h_{EB}, s_{EB}). These are used with respect to encrypting, decrypting and partially encrypting and decrypting votes (voters encrypt their vote using the public key of the electoral board h_{EB}). The private keys must satisfy $s_{VCS} + s_{EB} = s_{RGC}$, accordingly the public keys $h_{VCS} \cdot h_{EB} = h_{RGC}$. VCS and RCG receive their keys from the KMS through a secure channel (each of the two private keys is generated using an individual isolated machine denoted as KMS-VCS and KMS-RCG respectively). Each electoral board member presents one personal smartcard to KMS-VCS to obtain s_{VCS_i} and the other personal smartcard to KMS-RCG to obtain s_{RCG_i}. The values s_{VCS_i} and s_{RCG_i} are chosen such that a majority of all shares suffice to compute s_{EB} (t,n - threshold). The KMS does not persistently save any private keys. The containing storage media are destroyed after the setup phase.
   (c) Finally, the KMS generates private symmetric keys K_{VCS} and K_{RCG} and sends them to VCS and RCG through a secure channel. VCS and RCG decrypt and save these values in the private partition of secure hardware (HSM). Again, the values are separately generated in KMS-VCS and KMS-RCG and the storage media destroyed after the setup phase.
3. Establish public parameters: Election specific public values are established in KMS, including values P (the global value associated with a party), C (the global value associated with a candidate), and T (the global value associated with a candidate position in his party list). These values are chosen within the ElGamal plaintext space.
4. Establish Return Codes (KMS-VCS):
   (a) For each voter, using K_{VCS} and the voter's social security number (SSID), KMS-VCS computes a secret value s.
   (b) For each voter and each of the values P and C, using s KMS-VCS computes the partial values of the long party codes P' as P^s and the partial values of the long candidate codes C' as C^s. [6] P is the global value associated with a party, C the one associated with a candidate. The values P' and C' are sent to KMS-RCG along with information which voter they correspond to.
   (c) For each voter, KMS-VCS sends RCG the value g^s, where g is a publicly known generator of the ElGamal space. RCG will need these values to assess the correctness of VCS computations during the voting phase.
   (d) For each voter, using K_{VCS}, the VCS' generates a list B which maps a random identifier to each SSID. This list is passed to the RCG' for the next step, and to the printing service.
5. Establish Party Return Codes (KMS-RCG):

[5] Outgoing messages are always signed and the signature of incoming messages always verified throughout the voting procedure, even if not explicitly stated here.

[6] Note, that given P' (C'), P (C) can only be computed when knowing s and s cannot be computed unless knowing K_{VCS}.

(a) For each voter, using K_{RCG}, P' and the voter's SSID, KMS-RCG computes the long party codes P'' and the short party codes P''' (return codes to be sent by SMS).
(b) A hash of each long party code P'' is mapped to an encryption of its corresponding short party code P''' under key P''.
(c) All mapped pairs in random order per voter are sent to RCG along with information which voter they refer to. (RCG does not learn the return codes P''', since they are encrypted.)
(d) All return codes P''' are associated with the random identifier of list B and sent to the printing service.
(e) The storage media of KMS-RCG are destroyed.

6. Establish Position Return Codes (KMS-RCG):
   (a) For each voter, using K_{RCG}, P' and the voter's SSID, KMS-RCG computes the long candidate codes C'' (return codes to be sent by SMS).
   (b) For each voter and each value T, using K_{RCG} and the voter's SSID KMS-RCG computes the short position codes T''' (return code to be sent by SMS). T is the global value associated with a candidate position in any party list.
   (c) A hash of each long candidate code C'' is mapped to an encryption of its corresponding short position code T''' under key C''.
   (d) All mapped pairs are further processed like the party return codes.
7. Print Voting Cards (Printing Service):
   (a) A first process of the printing service prints the return codes P''' and T''' (received from KMS-RCG) onto each voter's voting card. The voting card is labeled with the random identifier obtained from KMS-RCG.
   (b) A second process (involving a second printer) uses the list B obtained from KMS-VCS to interpret the random identifier of the voting cards and label them with the home address of the voters. The second process only sees the random identifier of the voting cards. Thus, the printing service should not be able to learn which voters the return codes are associated with.

Note, that after the setup phase no single entity can elicit which voter a return code corresponds with. Furthermore, no single entity can elicit which party or candidate position a return code refers to. Possible attack scenarios require for instance VCS colluding with RCG, information being copied from KMS-RCG and retained prior to the destruction of storage media or the printing service combining the information of both processes.

2.4 Voting

The voting process contains the following steps.

1. The voter accesses the e-voting web-site and a session request is sent to the authentication service. The voter redirected to MinID and prompted to enter her MinID user name and password. Upon successful authentication on the MinID system, the authentication service sends the voter her voting credentials if she is enlisted in the ERoll. These include her private key s_{Voter} for signing her encrypted vote, the public key of the electoral board h_{EB} for encrypting her vote and the values P and C that represent the competing parties and candidates, mapped to the corresponding party and candidate names.
2. The browser displays the ballot. The voter makes her choice.
3. The voting client application computes an ElGamal encryption $E_{h_{EB}}(\hat{P})$, $\hat{P} \in P$ representing the selected party, and one ElGamal encryption $E_{h_{EB}}(\hat{C}_i)$, per selected candidate $\hat{C}_i \in C$. Further, it signs the encryptions using her private key s_{Voter} and generates one zero-knowledge proof ZKP_1 per encryption to prove that they are not deduced from an other voter's submission. The values generated in this step are sent to VCS.
4. VCS verifies the voter's zero-knowledge proofs ZKP_1 and the signatures to ensure that the vote has been cast by an eligible voter. Upon successful verification, from each encryption it computes the encryptions $E_{h_{RCG}}(\hat{P}^s)$, and $E_{h_{RCG}}(\hat{C}_i^s)$, by partially encrypting with s and partially decrypting with s_{VCS}.[7] This is easily done knowing the secret value s associated with the voter, knowing the ElGamal private key s_{VCS}, exploiting the relation $s_{VCS} + s_{EB} = s_{RCG}$, as well as the homomorphic property of the ElGamal crypto system. Finally, it computes two

[7] VCS cannot decrypt the values since it does not know the required private key s_{EB}.

zero-knowledge proofs ZKP_2 and ZKP_3 to prove the correctness of its computations. All received values, along with the values generated in this step are sent to RCG.[8]

5. RCG performs the same verification steps as VCS. Additionally it uses the values g^s to verify VCS's computations. Upon success, it uses its private keys s_{RCG} and K_{RCG} to compute the long party codes $\hat{P}''$ and the long candidate codes $\hat{C}_i''$. It computes the hash values to look up the encrypted return codes $\hat{P}'''$ and $\hat{T}'''$ in the map established in the setup phase and uses $\hat{P}''$ and $\hat{C}_i''$ to decrypt them. If the corresponding entries are found, RCG sends the decrypted $\hat{P}'''$ and all $\hat{T}_i'''$ to the voter via SMS. It also sends a signature of approval (voting receipt) to VCS to confirm that the vote is accepted and the SMS has been sent. Upon reception, VCS permanently stores the vote and forwards the voting receipt to the voter for confirmation. RCG saves its signature of approval for the purpose of verification during the tallying phase.
6. The voter compares the codes sent to her by SMS with the values on her voting card.

2.5 Tallying

The tallying phase contains the following steps.

1. The ERoll and data stored by VCS and RCG during the voting are signed by the corresponding entity and imported in the cleansing service on a physical storage media (e.g. DVD), i.e. the encrypted votes as sent by the voter, her signature, the data stored by RCG, including its signature of approval. The cleansing service thus verifies that the votes recorded in the databases of VCS and RCG are valid and consistently correspond with each other. The latest valid votes of VCS per voter are further processed.Auditors can verify that this process is performed correctly by performing the same steps themselves and comparing their output with the output of the cleansing service.
2. Paper mark-offs from the polling-stations reach the ERoll Service to indicate which voters have cast a paper vote. The digitalized data from the ERoll is imported in the cleansing service from a physical storage device. The cleansing service removes e-votes by voters that cast a paper vote. The cleansing service signs the resulting set of mere votes and transfers them to the offline mix-net. Similarly as above, auditors can verify this process and even import the output into the mix-net themselves on a physical storage media.
3. The first node of the mix net receives the votes from the cleansing service as its input and each node forwards its output to the next one. After the final node has produced its output, the mixed and re-encrypted votes along with the signatures can be accessed by the the auditor through a designated terminal connected to the LAN.
4. The auditor computes and sends a challenge to each mix node. Corresponding with the challenge, each mix-node computes a zero-knowledge proof to prove that it did not alter any votes at mixing. The proofs along with all inputs and outputs of each node data are signed and stored on a DVD to allow verification by the auditor using their own equipment. If the signatures and the proofs hold, the auditor import the DVD in the Decryption / Counting Service.
5. The members of EB provide their shares s_{EB_i} of the private decryption key s_{EB} to the Decryption / Counting Service. The Decryption / Counting Service reconstructs s_{EB}, decrypts the votes and generates a zero-knowledge proof of correct decryption. After the auditor has verified the proof, the votes are counted and the result is published.

3 Transparency

This is the key-measure for the successful application of the subsequent ones. The more information is withheld, the less the public will appreciate the added value gained by applying the remaining measures. As per [27] the idea behind establishing trust among IT-literates is to publish the full logical and technical system documentation - *voting protocol, components, software documents including the source code, all involved parties at development and operation, evaluation reports* - and relate its analysis to a *security concept*. 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. The public should be informed as early as possible and be able

[8] The obtained encryptions allow RCG to obtain the values $\hat{P}^s$ and $\hat{C}_i^s$. However, RCG cannot compute s and thus learns nothing regarding the selected party and the candidates.

to participate in an open discussion. It should be possible to comment on the project, ask questions and request for more information or clarification.

Transparency in the Norwegian project. At the point of writing this article, the project is still in its development stage, i.e. the public documentation has not been finalized yet. Although we were able to learn much from the information on the project site, we required further explanations from E-valg and Scytl. Both were very active at providing us with additional detailed information through pre-versions of documents yet to be published, shared documents and personal discussions.

The available documentation shows high quality and is presented in a logical, accessible structure on the Web-site of the Ministry of Local Government and Regional Development. [6] and [2] give an introduction to the project, in [16] technical documents can be found. In [7] the security objectives of the project are stated based on a security domain model and a threat analysis. They formulate technology independent, high level requirements for a secure, transparent and verifiable e-voting system. [21] contains the description and an analysis of the voting protocol that underlies the implemented system. The described mechanism aims at sidestepping single points of failure regarding privacy and the integrity of the ballot. Under [13] the requirements specification, tenders, evaluation and contract documents can be accessed. On the Web site one may also find presentations and videos that document the project.

Documents describing the implemented system were not yet published when writing this article. However pre-versions of the documentations were made available to us without any complicated NDA procedure. In the meantime the source code [12] and system documentation including Common Criteria Security Targets have been published [15]. They explain in [4] that they publish the source code hoping to get useful comments from the public for making improvements. However the auditing software to verify the tallying process is not yet implemented. That will actually be done through a properly open source ("free software") project during the summer.

Recently E-valg have published a couple of more documents in both English and Norwegian. Thus in the short time of preparing this paper, it was hard to get an overview and link theses different documents to each other, e.g. which is a refinement of which document or which document has been taken as input for other documents. However, a very valuable document is the one providing a summary of the threat assessment [17]

There is a Web-site to explain the system in a simplified fashion [5]. According to [27] 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.

There is a blog [4] where people from the public can ask questions and place comments on the system. On the same site, the responsibles of the project are introduced. E-valg are also active on the social network *twitter* [3]. In order to address concerns from technical experts appropriately, for the future they consider using their issue tracking tool on [12].

4 Separation of Duty

By distributing secrecy-critical duties, one can exclude the event of a single entity being able to break secrecy, i.e. compromise the voters' privacy or elicit partial results prior to the tallying phase. Under separation of duty, secrecy is only broken if a whole group of entities fail (or choose not) to follow their respective procedures correctly.[9] Since it is effective and easy to explain, [27] captures separation of duty as a measure suited for trust establishment.

Responsibilities can be separated on various levels, i.e. organizational (enforcing restricted access to information within an organization), architectural (physically and logically separating information) and evolutionary (having the organizations in charge use their own equipment, particularly use self-developed or independent 3rd party software). The potential to gain trust heavily relies on the selection of the responsible parties, their ability to perform their duties independently and to confirm to the public that they have done so truthfully.

Separation of Duty in the Norwegian system. Separation of duty will widely be implemented throughout the voting procedure of the Norwegian system. The efforts are summarized as follows.

1. The three respective environments that run RCG, the remaining online components (VCS, authentication service), and the isolated components (KMS, cleansing service, decryption service) are operated by independent governmental departments. Violating secrecy requires that information kept by at least 2 of the 3 sites be shared. The fact

[9] Apart from secrecy, separation of duty can also be employed similarly in order to circumvent the violation of a vote's integrity. This aspect is discussed in the context of verifiability in Section 5.

that all departments operate at least 100 km apart from eachother, induces additional trust in their independence (organizational and architectural separation).
2. The secret key s_{EB} required to decrypt votes is not kept anywhere during the vote casting phase. (It is not even explicitly computed during the setup phase, since its creation is distributed among KMS-VCS and KMS-RCG in the KMS.) Thus, a potentially malicious member of the electoral board EB cannot break the secrecy of the ballot or prematurely elicit partial results even if he gets hold of encrypted votes (e.g. through VCS, RCG, or from malware running on voters' computers).
3. The mix-net consists of four nodes. Including the mix-net service in breaking the voter's privacy thus involves convincing four players (each operator in charge of a mixing node) in participating in an illegal action. Given that the nodes are operated independently from eachother, each of their operators can strengthen public trust in privacy just by officially confirming their independent participation.

These precautions are explicitly outlined in the system documentation and therefore likely to have a positive influence at creating trust among the electorate. We believe that their influence will additionally be strengthened by publicly identifying the responsible of each duty, explaining to which degree they are independent (organizational, architectural, evolutionary), and having them confirm to the public that they have acted truthfully.

The following points summarize potential for further enhancements.

1. Key Generation: The key-generation service creates secret keys for all system players. In particular, all information needed to compute the private key s_{EB} used at the decryption of votes is established at KRD. Unfortunately it is inherently difficult for independent auditors to verify that the information is not persistently stored, i.e. that it is not copied before the destruction of the storage media. Having the system players independently compute their own keys can increase trust. Such an enhancement grounds on the mechanism introduced in [23]. Nevertheless, we point out that the secrecy critical keys for VCS and RCG are generated on independent machines of KMS (KMS-VCS and KMS-RCG).
2. VCS / RCG: Since s_{EB} is shared among the members of EB, it is unlikely that any of them can assist any other component at breaking secrecy. However, s_{EB} is also shared among VCS and RCG, due to the relation $s_{VCS} + s_{EB} = s_{RGC}$. Thus, if one of the two players reveals its private key to the other, the latter learns all the information it takes to prematurely decrypt votes and find out who voted how, even without the assistance of KMS. Just as with s_{EB}, trust can be gained by establishing and sharing the keys s_{VCS} and s_{RCG} among multiple entities within the respective organization. Clearly this would yield additional complexity and costs.
3. Mix-Net: Separating the duty of mixing votes among four mixing nodes holds much potential of increasing the public's confidence. However, the documentation suggests that each node is kept in the same physical environment (KRD). To build trust, it would be beneficial to outline how the independence of the node is enforced, i.e. whether they are meant to be independently maintained, supervised or operated (organizational) and whether they should run independent software (evolutionary). We point out that the E-valg project management and Scytl are in favour of including more independent nodes for mixing at some point.
4. Malicious software running on the voter's computer, potentially even the voting client application downloaded from the authentication service itself, could forward the voting choices entered by the voter to a third party in plain-text. E-valg have studied the option of having voters enter personalized codes as their voting choices, i.e. not only have them use codes for verification, but also use codes for expressing their will. However, such an approach has been conciously outruled, due to the inherent loss of usability.

5 Verifiability

In verifiable voting systems voters can verify that their vote is *cast as intended* and *stored as cast* (individual verifiability [22,20]) by accessing the relevant data collected by the voting servers. They can even verify that all collected votes were cast by eligible voters and that all these votes are correctly counted, i.e. one per voter (eligibility and universal verifiability [22,20]).[10] If all processed data can be verified as correct, it becomes obsolete to trust in any system

[10] Note that in internet voting systems one must weaken the notion of eligibility verifiability. In this article therm captures the ability to verify that all collected votes have been cast *using the credentials* of eligible voters.

players at preserving the integrity of the vote. Verifiability has been identified as a measure for trust establishment in [27].

Verifiability in the Norwegian System. The SMS received upon casting a vote distinguishes the Norwegian e-voting system from others. It confirms to the voter that her vote has reached VCS as intended. Note, that employing an independent channel for the purpose of verifiability, the event of a corrupted computer is addressed, who potentially may display misleading information to the user (trusted platform problem). In this respect, Evalg do not only comply with point 16 of the Council of Europe in [19], they also exclude the need to trust one's own platform with regard to verification.

On the other hand, the solution comes with a price. Since the voter has no possibility of accessing any public information from the ballot-box, she will inherently need to trust system players regarding the storage of her vote (individual verifiability). Accordingly, she has no means of verifying herself that the tally includes all and none but authorized votes (universal and eligibility verifiability).[11] Separation of duty thus comes in to play again, this time with respect to verifiability. On the positive side, some separation of duty is actually in place.

5.1 Individual Verifiability

Due to the return codes sent to her by SMS, the voter is able to verify that her first vote has been cast as intended and reached the VCS. She can not verify that VCS actually stores her vote. Nevertheless, this is mitigated by the fact RCG is supposed to store its signature of approval (voting receipt) as pointed out in Section 3. If only one of both refuses its duty, the auditors will observe the inconsistency during the first step of the tallying phase and include that finding in the report addressed to the authorities of their municipality. Just as in the traditional polling-station elections, the municipality will use the report to decide whether the inconsistency is acceptable or whether they need to fail the election.[12]

When casting subsequent votes, voters have to bring forward some more trust: If voters cast a subsequent vote that contains some repeated choices, the computer can cast a different value for these choices and inform RCG which ones these are. RCG then re-sends the codes as expected by the voter. A similar attack can be performed by a computer that colludes with the device receiving the SMS.

Thus, voters are reassured that their vote is stored as cast when they trust either RCG along with one of the two user devices, or VCS along with the computer. Further, they need to be given at least one report from a trusted auditor that states no inconsistencies.

In the meantime the aim is to enhance the system and have RCG store the votes as well and have a vote counted if at least one out VCS and RCG holds it along with a corresponding voting receipt issued by the other party. Thus, if the voter trusts in the independence of VCS and RCG despite running software from the same vendor, and if she believes in the trustworthiness of at least one of both environments of operation, she can be confident that her vote reaches the tallying stage (despite inconsistencies detected by an auditor). Further, it has been discussed whether to have VCS publish the voting receipts received from RCG. Thus after verifying that the receipt is published, even voters who trust neither VCS nor RCG only need to confide in at least one honest auditor reporting voting receipts that do not correspond with any vote in VCS or RCG. Counterarguments to this approach include usability concerns (how do voters verify that the receipt is published) and the fact that this would yield vote buying by individuals from the public more feasible.

5.2 Universal and Eligibility Verifiability

Universal and eligibility verifiability are not granted to the voter. Nevertheless, the system foresees the auditors to perform verification tasks. In that sense, the voter delegates verification. Clearly, the more trustworthy and the more

[11] Not offering a public bulletin board is an intentional measure, aiming at circumventing vote buying by individuals from the public.

[12] We point out that the auditing service running in Brønnøysund Registry Centre would detect the inconsistency in real-time and allow action prior to the audit. Yet, taking this as the solution would still require full trust in Brønnøysund Registry Centre (since VCS is also run there) and thus offers no mitigation regarding the lack of individual verifiability in terms of *stored as cast* under the organizational and architectural separation of VCS and RCG.

independent the voter believes an auditor to be from the rest of the system, the more will she trust in the integrity of the final tally. For the sake of public trust, we encourage to employ multiple independent auditors (in a strong sense of separation of duty, i.e. operating on their own equipment and running own software) for verifying the necessary tallying steps and have them confirm to the public that their verification was successful.

As shown in Section 3, All steps of the tallying phase can be audited - the voter merely needs to trust at least one auditor, i.e. believe that he would publicly reveal failing verification steps. Since anybody can ask to be an auditor and use own equipment to perform verification, the auditability of the system becomes comparable to traditional polling station elections.

6 Further Measures to Establish Trust

In this section we discuss vote updating, standardised security evaluations and test elections as measures to establish trust.

6.1 Vote Updating

According to [27] vote updating increases trust in the Internet voting system for many reasons, e.g. to overcome family voting, vote buying or problems with the PC. However, [27] also mention that it is important to ensure that the 'last' vote is the one that is counted.

Vote Updating in the Norwegian System. In the Norwegian system vote updating is possible. Voters can repeat the electronic voting procedure several times or cast a paper vote at the polling station, where the latter overrules any electronic vote. This holds in particular if voters do not get the success message on their screen or if they do not get the SMS containing the expected codes.

One point that could be improved is that voters cannot verify whether their electronic vote has been replaced by a paper vote cast by collaborating poll workers in the polling stations. There should be some way for voters to be informed whether their electronic vote has been overwritten by a paper vote. Further, vote-updating protects the system from vote-buying initiated by non-system players. However, vote-buying can still be performed by any entity who sees the vote as encrypted by the voter's computer or the collection of decrypted votes.

6.2 Evaluation

Evaluating the system according to international standards increases trust in the system according to [27]. This is meant to confirm to voters that the developed system corresponds to the one that is documented and that experts analysed it according to widely accepted standards including the formal voting protocol analysis, Common Criteria, ISO 27001, the k-resilience value [25], process observation, and usability standards.

Evaluation in the Norwegian project. According to the procurement[14] ' The supplier shall in the development process create the necessary documentation for a formal review process and Common Criteria certification to EAL4+[13] of all components directly related to e-voting, including counting and returning of members. [..] 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.' It has been decided that for the test run the availability of corresponding documents is sufficient while before using the system after the test election again, the documentation and the system will be undertaken a Common Criteria (CC) evaluation. For average voters these documents are meaningless. While they might know that in general people could now evaluate, they do not know whether a single person/institute has done this.

With respect to CC documentation, the following Security Targets (ST) are available on the Internet

- Election Administration software according to EAL2 [8]
- Electronic counting of paper votes software according to EAL2 [9]
- Electronic Voting Software according to EAL4+ [10]

[13] EAL means Evaluation Assurance Level; while level 1 is the lowest one and 7 requires the most thorough evaluation.

These documents seem to be pre-documents yet to be evaluated. [10] does not base on the existing Protection Profile defining basic requirements for Internet voting [28]. One difference is that [10] other than [28] does not include the assumption of trustworthy computers at the voters' side. However, whether this is acceptable by the CC evaluators is questionable, since one might assume that voters will generally not update their votes, which would permit manipulated PC's to elicit who voted how. Other CC documents like the high level system description are also not yet available.

The data centers seem not to have a formal ISO 27001 certificate, However, they are owned by the government and run other critical applications. It is also planned to compute and illustrate the k-resilience value of the whole system according to [25] in order to show more precisely than in section 4 which entities need to be trusted regarding which security property. A description of the protocol and its analysis exists [21]. However it would be interesting to see an analysis of the implemented system, i.e. without assuming ideal functionality.

Currently there is no information on how the observation of the security critical processes is organized. It is also unclear how the process is defined that ensures that the systems in use for the election correspond to what has been documented and announced on the Web. While we are also not aware of classical user test, the test elections (see section 6.3) can be seen as such. In addition, the reason for using T was based on usability argumentations.

6.3 Test Elections

Test elections were included in the list of trust establishment measures in [27] as it allows voters to experience the full voting process beforehand. Thus, voters' doubts and concerns that emerge from the act of casting their vote itself can be addressed without requiring them to simultaneously question the success of a real election.

Test elections in the Norwegian project. It is very hard to describe the technical delta for 10 pre-pilots performed from October of last year up until mid May of this year, and with continuous development in between. However, all 10 pre-pilots have used MinID, and two have in fact used return codes on SMS (in the first test 78% of voters reported checking their code). The last pre-pilot in Re (from May 13-19) used a near-complete system, where all proofs etc. from the protocol were generated.

Using pre-versions of the software may have disadvantages. Voters might be confused about different interfaces and the SMS having not being relevant for the test elections while very important for the legal binding election. However, maybe this is all clearly communicated to those who participated in test elections but we are not aware of this as this information is only available in Norwegian. In principal, one could also define the election in September as test with the full system and all processes implemented.

7 Conclusion

We have described the Norwegian Internet voting system with respect to the measures for trust establishment proposed in [27].

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. Taken from the published information, as well as from the discussions with the people in charge, it became obvious that being transparent is no easy task even if there is much willingness and even if the legal premises are given. Document management and version control becomes even more important.

Although we identified some possible enhancements to the system, we do not claim by any means that our additional propositions need to be implemented in order for the project to find acceptance among the Norwegian electorate; in particular not for the elections in September. They are rather meant to expose further possibilities that may also be found useful and relevant in the context of Internet voting projects for future large scale deployments as well as in other countries and as a proactive means to address concerns among the public that may arise due to irregularities at operation in the future.

Regarding transparency, one might get the impression that E-valg concentrate very much on the experts while this might also be the case as documents and information for the voters are only available in Norwegian. From our understanding, information regarding the remaining risks, the trust in different entities, and the restrictions of the verifiability are hardly communicated to the public.

With this analysis, we also validated the trust established measures proposed in [27] and demonstrated that it is possible to address all of them in one project.

8 Late Remarks

Since the Norwegian project is still very new, not all information is yet available in the documentation. Also parts of the system naturally tend to change during the initial development process. At least we would like to point out two relevant aspects that we became aware of only at a very late stage of our research.

- RCG accesses MinID to obtain the voters' mobile number in order to send the SMS containing the verification codes. By indicating a wrong mobile number, MinID alone can cast votes without the voters noticing. With regard to individual verifiability, voters will additionally need to trust in MinID not launching any such attacks.
- As described in this paper, the system has been designed and implemented to send voters an SMS containing codes relating to the selected party and the selected candidates, i.e. their position in the party list. However, the SMS's in the fall elections will only contain one code representing the party. Thus, the exposition of verifiability as described in the corresponding chapter only relates to the selected party, not the selected candidates.

References

1. Common Criteria for Information Technology Security Evaluation. Version 3.1, Revision 3, Final (July 2009), available at: http://www.commoncriteriaportal.org/cc/ Retrieved: 07.06.2011
2. About the e-vote project @ONLINE (May 2011), http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658
3. E-valg 2011 (krd_evalg2011) on twitter @ONLINE (Jun 2011), http://twitter.com/$#$!/krd_evalg2011
4. e-valgbloggen @ONLINE (Jun 2011), http://www.e-valgbloggen.no/
5. E-valglosningen @ONLINE (Jun 2011), http://www.regjeringen.no/nb/dep/krd/prosjekter/e-valg-2011-prosjektet/e-valgsystemet1.html?id=597799
6. E-vote 2011-project @ONLINE (May 2011), http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658
7. e-vote 2011 security objectives @ONLINE (May 2011), http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/tekniskdok/Security_Objectives_v2.pdf
8. Election administration software according to eal2 @ONLINE (Jun 2011), http://www.regjeringen.no/pages/16539918/SecurityTargetforElectionadministrationsoftwarev1_0.pdf
9. Electronic counting of paper votes software according to eal2 @ONLINE (Jun 2011), http://www.regjeringen.no/pages/16539918/SecurityTargetfore-countingofp-votesv1_0.pdf
10. Electronic voting software according to eal4+ @ONLINE (Jun 2011), http://www.regjeringen.no/pages/16539918/SecurityTargetforElectronicVotingSoftware.pdf
11. Minid @ONLINE (Jun 2011), http://minid.difi.no/minid/minid.php?lang=en
12. source.evalg.stat.no @ONLINE (Jun 2011), https://source.evalg.stat.no
13. Specification, tenders, evaluation and contract @ONLINE (May 2011), http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/tekniskdok/Security_Objectives_v2.pdf
14. System requirements specification @ONLINE (May 2011), http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/System_Requirements_Specification1.pdf
15. Systemarkitektur @ONLINE (Jun 2011), http://www.regjeringen.no/nb/dep/krd/prosjekter/e-valg-2011-prosjektet/kildekode/dokument.html?id=645240
16. Technical documents @ONLINE (May 2011), http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/technical-documents.html?id=612104
17. Threat assessment summary e-voting, admin, and pvoting toe's @ONLINE (May 2011), http://www.regjeringen.no/pages/16539918/ThreatAssessmentSummary.pdf
18. Allepuz, J.P., Castelló, S.G.: Universally verifiable efficient re-encryption mixnet. In: Electronic Voting. pp. 241–254 (2010)
19. Directorate general of democracy and politcal affairs: Guidelines on transparency of e-enabled elections. GGIS (2010) 5 E, Council of Europe (2010)
20. Gharadaghy, R., Volkamer, M.: Verifiability in electronic voting - explanations for non security expert. In: Robert Krimmer and Rüdiger Grimm (ed.) Electronic Voting 2010 - 4^{th} International Conference. LNI, vol. 167, pp. 151–162. Gesellschaft für Informatik, Bonn (2010)

21. Gjøsteen, K.: Analysis of an internet voting protocol. Cryptology ePrint Archive, Report 2010/380 (2010), http://eprint.iacr.org/
22. Kremer, S., Ryan, M., Smyth, B.: Election verifiability in electronic voting protocols (2010)
23. Pedersen, T.P.: A threshold cryptosystem without a trusted party. In: Davies, D.W. (ed.) EUROCRYPT'91, Workshop on the Theory and Application of Cryptographic Techniques. LNCS 547, vol. 547, pp. 522–526. Brigthon, U.K. (1991)
24. Volkamer, M.: Evaluation of Electronic Voting - Requirements and Evaluation Procedures to Support Responsible Election Authorities (2009), volume 30 of LNBIP, Springer
25. Volkamer, M., Grimm, R.: Determine the Resilience of Evaluated Internet Voting Systems. In: First International Workshop on Requirements Engineering for E-Voting Systems. pp. 47–54. IEEE CS Digital Library, doi: 10.1109/RE-VOTE.2009.2, Atlanta, GA, USA (2009)
26. Volkamer, M., Schryen, G., Langer, L., Schmidt, A., Buchmann, J.: Elektronische Wahlen: Verifizierung vs. Zertifizierung. In: Fischer, S., Maehle, E., Reischuk, R. (eds.) Informatik 2009: Im Focus das Leben, Beiträge der 39. Jahrestagung der Gesellschaft für Informatik e.V. (GI). LNI, vol. 154, pp. 1827–1836. Gesellschaft für Informatik, Bonn (2009)
27. Volkamer, M., Spycher, O., Dubuis, E.: Measures to establish trust in internet voting. In: ICEGOV. ACM International Conference Proceeding Series, ACM (2011)
28. Volkamer, M., Vogt, R.: Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte (BSI-PP-0037), common Criteria Protection Profile, http://www.bsi.de/cc/pplist/pplist.htm, 2008