Audit report on pilot electronic voting in municipal elections

Summary

The object of the audit is the piloting of electronic voting in three municipalities in the municipal elections of autumn 2008. This will not be electronic voting taking place at the voters' homes but a trial that, to a considerable extent, imitates conventional elections. Many of the issues of security and trust involved in electronic voting are manifest even in this type of computer-aided elections. The analysis and assessment of such issues is the key objective of this audit.

Based on the audit, the planned trial rests on a solid and secure foundation provided that all parties involved adhere to the prescribed rules. In this regard the system is quite similar to the current practice. With electronic elections, however, the key question is how to ensure that trust is maintained so that none of the parties to the elections will be able to cheat others. In conventional elections, control arrangements are relatively well in place. In electronic elections, this is essentially more difficult in respect of the technical details involved and the actions of the key individuals operating the system. In this regard, the results of the audit suggest that certain details should be made more specific. Particular attention should be paid to the training of election officials and to the fact that multiple control of critical items is required.

However, when considered as a whole, we are of the opinion that the trial can be implemented based on the present plans. In our opinion, the greatest challenge of the project is to ensure that control remains adequate at all times.

1 Introduction

The problems associated with elections arranged through telecommunications networks have been widely researched. In most cases, the goal has been to construct a reliable election system through which everyone could vote at home using either a computer or a mobile phone. This, in turn, is based on the precondition that the system must fulfil at least the following requirements:

1. Only those may vote who are eligible to vote, and each of them may only do so once.

2. The result of the elections must be generally verifiable.

3. The secrecy of the ballot must be preserved.

To meet these requirements, additional 'building blocks' such as encrypted and authenticated data communications connections are required. Other complex cryptographic methods are also needed so that *the preservation of the secrecy of the ballot is not based trust, but instead follows from the inherent characteristics of the system.*

The election system audited herein is based on a different starting point. The objective was to create a system that imitates the current system of secret ballot. The difference is that there will be computers in the polling booths through which the votes are sent to an 'electronic ballot box'. The security of the system is intended to be controlled in a manner similar to that of the present system: by ensuring that there are a number of trustworthy election officials from different interest groups present both at the polling and vote-counting stations. It should, of course, be also ensured that the software applications used for casting the votes and calculating the results operate as intended.

The fulfilment of the above preconditions can be deemed as minimum requirements for the voting system, provided that all officials participating in the elections act honestly. This requirement is met by the system assessed herein. However, for audit purposes, the reliability of the system needs to be assessed also in a situation where some of the officials are fraudulent. In this scenario, the chosen solution also displays weaknesses. A list of general problems is presented below, and a set of potential problem situations is discussed in greater detail in the subsequent chapters.

It should be noted that the purpose of this report is mainly to pinpoint potential problems detected in the audit. Some of them may appear far-fetched, but it is the responsibility of other instances to decide how relevant the postulated risk scenarios are in the pilot.

- It should be emphasised that most of the potential problems mentioned in this report can only occur if an election official acts fraudulently and the physical control exercised by other officials fails. Even though the same problems may also occur in the present secret ballot system, the physical control of officials is considerably more difficult in electronic voting. If the control was to fail regardless of all safeguard measures, the ramifications could be dramatic. Computer skills of at least some degree should, therefore, be required from all election officials in computerised elections. Particularly problematic is a situation where one of the election officials is an expert in the field while the others are novices.

- The election system identifies the voters based on an electronic voting password generated for them. This identifier is recorded on a smart card and handed over to the voter by an official at the polling station. It would thus be possible to obtain several voting IDs from two fraudulent officials who operate together and to use the IDs to vote freely for several times.

- In the system being audited, the voting situation is substantially different from that of the current system. In a secret ballot, the ballots are publicly dropped into the ballot box so that the voter knows and the election officials can witness that the ballot was placed inside the box. In the system under review, the passing of votes into the box is not witnessed by anyone. The system only allows checking the time when a ballot was recorded in the ballot box in the voter's name. The voter thus has no choice but to trust that the officials and the software operate correctly and that the content of the ballot is what the voter intended.

- Several software applications are used in the election system, most of which are supplied by a foreign company that designed the system, while the rest is designed by TietoEnator. A necessary precondition for the reliability of the system is that the software applications function as intended. However, the source code is not open, and only the most critical sections were reviewed. Even if the code had been reviewed in its entirety, it should also be possible to ensure that the code to be executed corresponds with the reviewed code and that the computer executing the code does not run any additional software. Similar problems are certain to emerge in all election systems designed to be implemented though telecommunications networks. For this reason, the voters should preferably be able to personally ensure that their ballot ends up in the ballot box. It should also be possible to generally verify that the election result calculated from the box is correct.

- The digital ballot box is located in the premises of TietoEnator. The system is operated and designed by specialists from TietoEnator under the supervision of the Ministry of Justice. Consequently, the security of the system is based of the ability of the Ministry of Justice to oversee each step of the process. As the same organisation is responsible for all steps of the process, its supervision will be a challenging task.

- It may be worthwhile to consider whether it is sufficient that the designers and 'insiders' of the system are convinced of its security. It should be possible to pass this trust among the voters, too.

More detailed observations on the system being audited are listed below. The limitations imposed on the system by the Ministry of Justice are commented in the following chapter, while the subsequent chapter provides an account of the comments relating to the realisation of the above-mentioned three required characteristics of an election protocol.

Let it again be emphasised that the occurrence of all of the problem situations discussed herein requires that the control has failed to at least some degree.

2 Imposed limitations and problems resulting from them

Based on the Finnish Election Act, it has been decided that no paper printout will be retained or any electronic receipt given from casting a vote. For this reason, the voters cannot in any way ensure whether their vote is correctly registered in the system. They have no choice but to trust that the equipment, software and officials operate as intended, although in unclear situations the election official may check that the voter's right to vote has been marked as used in the system.

Standard PC equipment and an operation system run from a CD are used for the voting. Protecting the PC equipment in a manner that prevents the installation of other equipment or software is a challenging task. A CD can be easily copied without notice, and gaining possession of the disk makes fraud easier. For these reasons, sufficient computer skills should be required from the election officials.

The software to be employed is a business secret that cannot be disclosed. Even though there is no reason to suspect the software to be faulty, the possibility of errors or deliberate weaknesses remaining in it cannot be completely excluded. However, a thorough checking of the entire code would require several man-years of effort.

Continuous connection to the mainframe makes it possible to check people's eligibility to vote in real time during advance voting, but it also exposes the system to denial-of-service attacks. The impact of a denial-of-service attack can be restricted, but the success of such an attack cannot be completely excluded.

3 Voting protocol

3.1 Controlling the right to vote

In our understanding, voters or parties completely external to the elections are not able to cheat the system, i.e. vote for several times.

In the event of failure in the physical control or due diligence exercised by other officials, a fraudulent official may vote on behalf of anyone. An official could, for example, give the voting IDs of several individuals to his or her assistant who comes to vote, or possibly even change his a her personal computer into a voting terminal. For this reason, it is of crucial importance that the officials attend to the control of each other strictly in accordance with the instructions given and take due care of the passwords and other material in their possession.

Voter's access to a polling booth does not guarantee that he or she would actually be able to cast a vote in the booth because a fraudulent official could already have used his or her right to vote in a situation described above. In such a situation, it may be impossible for the voter to convince even honest officials of the true state of affairs, since they would not be able

to know whether the voter him- or herself had already voted or whether someone else had voted in her place.

3.1.1 Prevention of vote-selling

- Observation class: 4

- Corrective measure: The PIN code of the voting card must be better hidden.

If a voter has a card reader with him- or herself in the polling booth and he or she knows the PIN code of the card, he or she might be able to make a copy of the voting card. If the said individually does not vote personally, he or she would then have 30 minutes of time to sell the card to someone else coming to vote. The PIN code can be traced by obtaining one password and a couple of files or in the event that the physical control of the polling station fails.

If the attacker succeeds in writing his or her own voting cards, he or she could also be able to make a card that can be used for voting a candidate from another electoral district.

3.1.2 Control of officials' and voting terminal connections

- Observation class: 3

- Corrective measure: The system could be furnished with automated monitoring that warns of any additional officials' or voting terminals appearing in the system.

A fraudulent individual in the possession of IDs of people entitled to vote, election official IDs of a polling station, password of a client certificate, a couple of files from the CD in the official's terminal, a card reader, and a set of smart cards will be able to prepare cards entitling to vote. If such an individual also has a card and password for opening the voting terminal, he or she will also be able to vote using the cards he or she has made. The risk for the occurrence of this type of fraud is pronounced in respect of the insiders of the system.

The system should also be continuously monitored for other suspicious events. These include too rapidly occurring vote-casting or enquiries on the right to vote.

3.2 Calculation of the election result

- Observation class: 2

- Corrective measure: Internal instructions on the measures to be taken during the calculation. In addition, a sufficient number of specialists representing different interest groups should be present at the vote-counting station, divided into two groups operating in parallel. Both

groups will independently compile the required software and calculate the election result using their own computers.

The software application that calculates the election results does not provide a proof of their correctness. Therefore, it must be possible to ensure that the results are calculated using the correct software application. Security can be enhanced by using two groups of people to calculate the results.

A group of system insiders is in principle able to generate an entirely new yet genuine-looking electronic ballot box and change the election result calculated from it to their liking. Therefore, it must be possible to ensure that the result is calculated from the correct ballot box. On the basis of the documents available to us, it is difficult to estimate how large a group of fraudulent individuals would be required to accomplish this. For this reason, it is important that a sufficiently large number of specialists are present when the ballot box is being handled. (The problem could also have been avoided if it was impossible to fill in a counterfeit ballot box with genuine-looking ballots. This could have been accomplished by preventing anyone else but the voter to access the voter's electronic voting IDs.)

3.3 Preserving the secrecy of the ballot

- Observation class: 3

- Corrective measure: Internal instructions on the generation and storage of the electronic ballot box and its secret key. A sufficient number of specialists representing different interest groups should be present when generating the key and the electronic ballot box.

It is possible to trace the ballot of an individual voter by obtaining a copy of the electronic ballot box and the key required for decrypting the encryption of the ballots. The ballot box is accessible by all of the specialists maintaining the system. The key for opening the ballot box will be stored in a safe after it has been generated. The possession of the key can be obtained by those who have access to the said safe and who are able to bypass the seals. This can also be done by individuals who have succeeded in changing the program code used for handling the key or managed to install their own code on the computer processing the key.

The software application performing the mixing of ballots is able to 'see' which vote was cast by which voter. Here, again, the only option is to trust that the software being employed is the correct one.

It should also be borne in mind that the voters' ballots remain identifiable until all copies of the electronic ballot box or keys to the ballot box have been destroyed. The electronic ballot boxes and ballot box keys used in the elections are intended to be archived for several years.

3.3.1 Mixing of ballots

- Observation class: 4
- Corrective measure: A larger number of ballots may need to be selected for mixing in a single batch.

Prior to counting, the ballots are mixed in a batch of one thousand ballots. The secrecy of the ballot is not necessarily preserved if only a few votes cast in the same polling station end up in the same batch or if the batch contains 1 advance vote and 999 votes cast on the polling day. Even in this unlikely situation the secrecy of the ballot is secured if all parties involved operate in compliance with the instructions given.

3.3.2 Storage of the secret ballot box key during the elections

- Observation class: 5
- Corrective measure: Simplification of the procedure.

According to the description of the system being audited, the secret ballot box key is divided into parts and these parts are stored on smart cards. The smart cards and the PIN codes required for opening them are all stored in the same safe. Dividing the key into parts is of no use if all parts are kept in the same place. The PIN codes are similarly useless if they are kept in the same place with the cards.

3.4 Summary

The reliability of the audited system is largely based on the assumption that election officials are able to detect any fraud attempted by voters and other officials both at the polling and vote-counting stations. There is, of course, no reason to suspect that the entire personnel arranging the elections did not act honestly and with due diligence. There is, however, reason to suspect *if it is possible to recruit a sufficiently large number of people mastering basic IT skills* so as to make it possible to detect any attempted fraud.

In general it can be estimated that the probability for the occurrence of any fraud attempts is relatively small in Finland. Yet on the other hand, if successful, the ramifications of a committed fraud would be radical, at least if the fraud attempt was to take place during the counting of votes. It is also possible to assume that in certain countries, the use of the system in question would arouse strong suspicions on the trustworthiness of the results. By placing a few ‘suitable’ persons in key places of the system the results of the elections could be modified precisely as desired without a risk of ever getting caught.

The Ministry of Justice should be the correct instance to assess whether the probability of the risks is small enough compared with the damage arising from the possible realisation of the risks.

4 Implementation

4.1 General observations concerning the core

The actual code relating to the auditing of the pilot version of the election system divides into two larger wholes:

- The code constituting the core of the voting system proper, such as the code related to the vote-casting events in the centrally located server system and the electronic ballot box;

- The code relating to the application of the software referred to above, such as the code required for the voting and officials' terminals and for connecting them with the server software.

The configuration of the entire election system also comprises a lot of other code, the major part of it being contained in off-the-shelf software applications that are not included within the scope of this audit as far as their code is concerned. The code constituting the core of the actual voting system was reviewed for those sections that were considered to be critical. Furthermore, the source code of critical encryption components of the applications in the voting system terminals, as well as those used on the server level, was also reviewed.

The reviewed source code was in certain regards fragmentary and, in part, insufficiently documented, which impaired its readability for audit purposes in particular. The code as such is functional, even though some minor programming-related remarks are in order.

4.2 Pnyx.core

The code for the electronic ballot box of the actual voting system, as well as that of the mainframe server used in the voting system, contains several sections that are not relevant in terms of this audit: all of the features and solutions implemented in the software supplied as the system core will not be used in the pilot. Generally speaking, software applications supplied as off-the-self components often involve technical problems related to their usability and adaptability. However, this does not result in any major problems in respect of code behaviour thanks to the structure of the server-level software of the voting system. It would, of course, be preferable that a system intended for this critical a use did not contain any additional code.

4.3 TietoEnator

As with the actual voting system, the supplied code relating to the use of the voting system core contains unused testing-related code that is not intended to be released in the final compiled version. As to the operating system of the voting and officials' terminals, the potential opportunities for abuse allowed by the operating system were assessed. Modifications and restrictions to prevent abuse have been made in the Knoppix operating system, but the absence of the final version presents a problem.

Let it also be noted that troubleshooting issues have been quite well addressed. However, more informative troubleshooting practices would be in order in cases such as those related to network traffic problems for which a local computer support person might be able to provide assistance.

4.3.1 Management of software versions

- Observation class: 3
- Corrective measure: A sufficient number of competent people must be present when installing the software.

It is important that only the correct and reviewed version of each and every software application is used. The only viable option for meeting this requirement is to carry out the compilation of the software by a sufficiently large number of people. When assembling the boot disks for voting and officials' terminals, it is similarly important that the disks contain the correct versions of the correct software applications.

4.4 Knoppix CD

- Observation class: 2
- Corrective measure: Final version of the operating system disks.

The development work on the operating system disks is yet in progress. The operating system plays a crucial role in system security.

5 Data communications arrangements

5.1 Connections between polling stations and the supplier's network

Public networks are employed in the connections from polling stations to the supplier's network (existing Internet connection in the polling station), through which the information is transported in packet form using an IP protocol (IPv4).

5.1.1 Data security and operational reliability of the implementation

- Observation class: 4
- Principal threat: Interruption of service as a result of which a standby system (conventional secret ballot) is switched to. The secrecy of the ballot is not compromised as a result of the interruption.
- Corrective measure: Request for clarification from the operator of the connection link if deemed necessary.

As the information transported over the network is heavily encrypted both in the application layer and in the transmission layer, the secrecy of the ballot can be deemed as secured in this regard.

As to the operational reliability of the connections and the data security of the network layer (legibility of IP addresses and TCP ports), the operators providing the data communications connections play a central role. Both of the above depend on the operator and the service package purchased from the operator. For example, the operator may offer centralised data security solutions, but no assumptions can be made in this regard.

The operability of connections provided by Finnish Internet service providers is, in general, reliable. Brief occasional interruptions of service can, nevertheless, occur in normal operation. Should an interruption of service occur, a standby system (conventional secret ballot) needs to be switched to. A potential interruption of service will not compromise the secrecy of the ballot in respect of the electronic votes already cast.

When considering the general operational reliability of commercial connections during the past few years, it can be assumed that the probability of an extensive and long interruption of service during the pilot elections is very small. However, a data security attack, e.g. a denial-of-service attack, targeted against the key equipment of a specific operator is always possible. An attack targeted against the web servers maintained by the connection link operator could also affect the operating reliability of the data communications connections used in the elections.

A clarification of the level of data security arrangements and, for example, of the physical protection of the equipment that is critical for the operation of the network can be requested from the operators of the connection link.

5.1.2 Prevention of system intrusions and tampering with its operation

- Observation class: 4

- Principal threat: Denial-of-service attack resulting in an interruption in data communications as a result of which a standby system (conventional secret ballot) is switched to. The secrecy of the ballot is not compromised as a result of the interruption.

- Corrective measure: A tunnelled, IPSec-based VPN connection between the polling station and the voting system if deemed necessary.

See the preceding section. As regards the connection link consisting of the subnets of different operators, the prevention of intrusions to and tampering with the operation of key equipment falls under the responsibility of the respective operator. If successful, the potential intruder would probably attempt to either obstruct the traffic (i.e. disconnect the data communication connection between the polling station and the voting system) or eavesdrop it without modifying it. In the latter case, the intruder could, at most, be able

to trace the IP addresses of the communicating devices and the TCP ports of local the applications, since the transported information is encrypted in respect of the payload of both the application (OSI layer 7) and transport layers (OSI layer 4). A tunnelled, IPSec-based VPN connection between the polling station and the voting system would prevent the tracing of the IP addresses and local TCP ports if deemed necessary. In this case, the potential eavesdropper would only be able to trace the IP addresses of the end points of the tunnel, not those of the actual communicating stations.

5.1.3 Instructions to the election organisation to prepare against emergencies

- Observation class: 5

- Corrective measure: More specific instruction as regards interruptions in data communications connections.

Problems arising as a result of data communications errors are not discussed at all in *Ongelmatilanteet* ('Problems') section of the document entitled *Äänestyspaikan tekninen opas* ('Polling Station Technical Guide'). Section 3 of the said guide does, however, provide instructions for testing the connections.

5.2 Design documents concerning the supplier's internal network

As regards data communications arrangements, the technology of the supplier's internal network is described in the document entitled *Sähköisen äänestyksen tuotantoympäristön kuvaus*. ('Description of the production environment of electronic voting') The supplier's internal network employs private network IP addresses, commercial (certified) firewall and IDP solutions, and, as regards the transportation of electronic votes, encrypted connections.

5.2.1 Data security and operational reliability of the implementation

- Observation class: 4

- Principal threat: Security attack from a public network resulting in an interruption in data communications as a result of which a standby system (conventional secret ballot) is switched to. The secrecy of the ballot is not compromised as a result of the interruption. More unlikely threats mainly relate to the physical data security of the premises.

- Corrective measure: The arrangements are sufficient for the piloting of electronic elections. From the point of view of potential security attacks, the production system is adequately protected and can be disconnected from the public network if required, and a standby system (conventional secret ballot) can be switched to at the polling stations. As regard physical data security, the access control of the premises during the elections and the verification of the legal use of the configuration and calculation equipment are of paramount importance.

After the voting has ended, the electronic ballot box is transferred, using either a portable electronic (USB memory, etc.) or portable optical (CD-ROM, DVD-ROM) medium, to a device outside of any information network for the purpose of calculating of the election result. The devices between which the transfer is carried out are located in the same access-controlled premises. Physical data security arrangements can thus be considered sufficient in this regard.

The physical data security of the location of the election system (access control, guarding, etc.) is not described in any greater detail. A separate definition of the physical data security of the location during the elections is required to ensure the success of the pilot.

The production environment has in place a system with duplicated servers (one of them being 'cold' with the estimated deployment time ranging between 0.5 and 2 hours if the situation so requires). The selected firewall system is certified to be used as the external limit of the domain. The firewall contains an IDS feature, but it is not used in the production system for the elections; instead, a separate IDP system had been selected as its replacement. A set of allowed IP address ranges is defined for the polling stations in the firewall rules, and the IDP system is defined to only allow traffic from specific applications (voting applications). The arrangements can be considered sufficient in this regard.

For the purpose of enhancing data security and preventing potential attacks, the IP addresses of the voting servers will not be disclosed. However, this solution does not preclude the possibility of tracing the IP addresses on the basis of a traffic analysis.

5.2.2 Prevention of system intrusions and tampering with its operation

As regards physical data security, firewall and the IDP system, see the preceding section.

Encryption is used in some forms of data communication between the voting system and the election information system, but not all. However, this trafficking takes place within the supplier's internal network protected by firewall and the IDP system. Although encryption is for this reason not necessary, its use should be considered for the sake of consistency.

5.3 Instructions for and implementation of the internal network of the polling station

In these regards, the assessment is based on the documents entitled *Arkkitehtuuri* ('Architecture') and *Äänestyspaikan tekninen opas* ('Polling Station Technical Guide').

5.3.1 Data security and operational reliability of the implementation

- Observation class: 4

- Principal threat: Interruption in data communications as a result of which a standby system (conventional secret ballot) is switched to. The secrecy of the ballot is not compromised as a result of the interruption.

- Corrective measure: A tunnelled, IPSec-based VPN connection between the polling station and the voting system if deemed necessary. Measures to ensure physical data security.

The reliability and security of the internal data communications arrangements of the polling station are highly dependent on the infrastructure of the communications network constructed at the polling station. The location may be furnished with cabled or wireless network connectivity, surface-mounted electrical and data communications cables installed on cable trays, or centralised cable shafts and cable penetrations piped inside the walls. A cabled network with surface-mounted cables running in cable trays, for example, is more vulnerable to physical sabotage (e.g. cutting of cables).

A person with access to the network of a polling station could, for example, attempt to overload the network by a massive data transfer volume or eavesdrop the network traffic for the purpose of traffic analysis. Traffic analysis could potentially be used for tracing the IP addresses and TCP ports of communicating devices. However, the transported voting data cannot as such be disclosed due to the encryption systems used. The traffic analysis could be made more difficult to perform by using a VPN tunnel between the polling station and the voting system.

Generally speaking, in electronic voting the arrangements at the polling station involve more opportunities for impairing the reliability and security of the voting process without provoking any major attention compared with conventional voting.

5.3.2 Prevention of system intrusions and tampering with its operation

- Observation class: 4

- Principal threat: Interruption in data communications as a result of which a standby system (conventional secret ballot) is switched to. The secrecy of the ballot is not compromised as a result of the interruption.

- Corrective measure: Instruction for checking the physical data security arrangements on the polling day prior to opening the terminals and during the course of the elections.

As to preventing that the operation of the system is not tampered with, it is essential that the physical data security of the data communications connections is checked and the locking of all IT premises other than those used for voting is ensured on the

polling day both prior to opening the voting terminals and several times during the polling day. In this way it can be ensured that no one has had the opportunity to make their own connections or, for example, gained access to any of the IT premises to disturb or eavesdrop the communications traffic. This is essential in terms of ensuring the success of the pilot. Similarly, it should be ensured several times during the polling day that the connection cabinets are locked, the connections have not been altered, and the IT premises are vacant and locked.

6 Instructions to the officials

The voting event, together with all of the inspections and errors potentially involved with it, is highly complex and requires that the officials have at least average computer skills, in addition to which they must be provided with thorough training. All computer-related issues must not be left to taken care of by a single point of computer support. All activities should be overseen by at least two officials at all times, both of whom having a proper understanding of what is taking place. The careful handling of passwords and other material should also be emphasised.

Overall, the instructions provided to the officials were highly incomplete (e.g. closing of an officials' terminal), and the content of the training provided for them was not known by the auditors.

Annex A

The following documents were available in the protocol audit:

- Pnyx.core functional description v.1.7.1b
- Arkkitehtuuri v.1.4H (17 January 2008)
- Auditoijan opas v.0.94K (31 January 2008)
- Tekninen toteutus ja tietoturvaratkaisut v.1.0E (12 June 2007)
- Äänestyspaikan tekninen opas v.1.31E (23 May 2008)
- Vaalien perustaminen, sähköisen uurnan avaus ja tulosten laskenta v.1.0E (7 April 2008)
- Arkistointikäytännöt v.1.1H (17 April 2008)
- Testaussuunnitelma v.2.0H (6 March 2008)
- Sähköisen äänestyksen tuotantoympäristön kuvaus v.1.0E (19 February 2008)
- Sähköinen äänestämisen testaus, ppt presentation (Ministry of Justice, 12–28 March 2008)

In addition, certain items had to be verified from the source code and by testing the software.

Annex B

Scale for the criticality of the observations:

1. Highly critical. The piloting cannot be performed in municipal elections without taking corrective measures. The data security measures planned for the piloting will not resolve the detected risk scenario.

2. Critical. The piloting should not be performed in municipal elections without taking corrective measures. However, the other data security measures planned for the piloting will significantly reduce the probability of the risk scenario.

3. Important. Corrective measures should be taken prior to the elections. The detected risk is minor and/or the other planned data security measures will in practice prevent the realisation of the risk scenario.

4. Limited. Corrective measures need not be taken as regards the municipal elections of 2008. Other data security measures will prevent the realisation of the risk scenario and/or the realisation of the risk scenario is highly unlikely.

5. General observation. The observation does not have a direct effect on the correctness or data security of electronic voting. The observation relates to items such as the quality of information systems or operating instructions or product features that are not used in the piloting.

Annex C

Audit working group:

- Prof. Juhani Karhumäki, Accountable Project Leader
- Tommi Meskanen, Ph.D., coordination and general assessment, as well as the analysis of cryptographic protocols, 2 months
- Seppo Virtanen, D.Sc. (Tech.), data communications arrangements, 0.5 months
- Arto Lepistö, Ph.D., analysis and general assessment of the source code, 2 months
- Petri Salmela, Lic.Phil., Knoppix operating system,1 month
- Ari Renvall, Ph.D., analysis of cryptographic protocols, 0.5 months
- Sami Mäkelä, M.A., review of the source code, 2 months

- Tommi Penttinen, undergraduate student, review of the source code, analysis of the data security of applications and actions during elections, 2 months

- Hannu Nurmi, Academy Professor, election specialist

The audit group consists of people from the University of Turku. The group leader Juhani Karhumäki is currently Professor of Discrete Mathematics in the Department of Mathematics. Academy Professor Hannu Nurmi is one of the leading election specialists in Finland. Research scientists Ari Renvall and Tommi Meskanen, who were responsible for the analysis of cryptographic protocols, both hold a Ph.D. in cryptography from the University of Turku. The subject matter of Renvall's thesis was expressly concerned with electronic elections. The auditing of data communications solutions was performed by D.Sc. (Tech.) Seppo Virtanen. Arto Lepistö, Ph.D., assumed the main responsibility for the review of the source code and the operating system. He was assisted by Petri Salmela and Sami Mäkelä, both soon to defend their thesis, as well as Tommi Penttinen, who is currently a master's student.

Annex D

Implementation of the audit:

The audit was performed at the Department of Mathematics in the University of Turku. The composition and areas of responsibility of the working group are described in Annex C. The completion of the work required a total of 10 man-months. The work was carried out in a room specifically reserved for the purpose, where only the members of the audit group had access. The source code was analysed using computers that were specifically purchased for the purpose and not connected to any network.

The principal areas covered by the audit are briefly described below. The project reviewed the cryptographic protocols employed, along with their suitability to electronic voting. At the same time, the pilot was assessed in comparison with manual voting and other electronic voting systems.

As regards data communications connections, the audited items included the design documents concerning the inter-network communications connections of the polling station and e-voting supplier, design documents concerning the internal communications network of the e-voting supplier, and the instructions for and implementation of the internal communications network of the polling station.

The documents submitted to the auditors concerning the set-up and supervision of the elections and the calculation of votes were assessed and the instructions related to them were reviewed.

The source code supplied by TietoEnator, as well as the source code of critical security components included in the Scytl pnyx.core product, were reviewed and assessed in terms of data encapsulation and integrity and in view of the sufficiency and necessity of the operation of the software applications. In other words, the object of the audit was to determine whether the software applications do what they are supposed to do, and only that.

During the course of the project, the data security of election officials' and voting terminals was assessed by determining, among other things, the sufficient and necessary conditions for using them from another machine. Conversely, the opportunities for modifying the information, e.g. voter data, were assessed at different stages of the protocol.

The control of the activities that take place during the elections, such as the interaction between officials, has a major impact on the success of the voting process. To this end, the project also examined the physical framework of the elections and its impact on the data security of the voting event.

On behalf of the project,
Turku, 13 June 2008

Juhani Karhumäki
Accountable Project Leader

Tommi Meskanen
Senior Assistant