Incompatibility of the Finnish e-voting system with the Council of Europe e-voting recommendations

Electronic Frontier Finland – Effi
http://www.effi.org/

1st August, 2008
Edited and translated[1] by Antti Vähä-Sipilä

> *"Pnyx gives complete control over the election to the electoral authorities"*
>
> \- Pnyx.Core marketing material[2]

Executive Summary

Finland is piloting a direct recording electronic (DRE) type, polling station based (non-remote) e-voting system in its municipal elections in October 2008. In the proposed system, we argue that ensuring the correctness of the results is extremely difficult. The voting results may be affected by multiple components of the e-voting system, and observing the counting process of ballots is impossible in the traditional sense. The results may be affected by a small group of people, either involuntarily through programming errors, or with malicious intent. The inspections and audits of the system presently only apply to parts of the system, and even in these cases, citizens must trust specialists as major parts of the system software are considered to be trade secrets.

[1] This is an English translation of a report originally published in Finnish in June 2008. This version has been slightly updated to include comments on the University of Turku audit report and explanatory notes on Finnish elections. Subsequent versions of the Finnish document may or may not be available in English, and the different language versions may not be completely synchronised. As we cannot take responsibility of translation errors, this English version (as well as any translations of Ministry of Justice communications found in this document) should be considered as informational only. In the event that you find any mistakes or factual errors, please contact us (contact information can be found at our website).

[2] Pnyx Compliance with the Council of Europe's Security & Audit Standards on e-Voting. Scytl, December, 2004. http://www.scytl.com/docs/pub/science/Pnyx_Compliance_with_CoE_Standards.pdf

In addition, the audit of the system found that it may be possible to find out how an individual has voted, if an attacker would get access to the electronic ballot box and certain encryption keys, both of which are planned to be archived for several years.

This document compares the Finnish e-voting system with the Council of Europe recommendations for e-voting, and argues that the fully electronic voting system, which will be used in the Finnish e-voting pilot, does not meet these recommendations.

Electronic Frontier Finland (Effi) is a non-governmental and non-profit association registered under the Finnish law. It was founded to defend the digital rights of all citizens, such as the rights to uncencored communications, to fair licencing of digital content, and to freely develop and publish open source software. The association aims to elicit public discussion and works to affect Finnish and European legislation. At the time of writing, the association has more than one thousand individual members.

Background

The Finnish Ministry of Justice (Oikeusministeriö) has commissioned a solution for Finnish e-voting which is based on the Pnyx.Core e-voting product from a Spanish supplier, Scytl. TietoEnator acts as the systems integrator.

This work is based in a special law that was passed in 2006 which authorises electronic voting in the municipal elections of October 2008. Three municipalities (Karkkila, Kauniainen and Vihti) will pilot this e-voting system.

This document argues that the planned Finnish e-voting system is incompatible with Council of Europe recommendation Rec(2004)11[3]. Information on the Finnish e-voting system are based on information provided by the Ministry of Justice[4,5,6]. The Ministry of Justice has also released other documents pertaining to the system[7], but it

[3] Council of Europe Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Council of Europe, 30th September, 2004. https://wcd.coe.int/ViewDoc.jsp?id=778189

[4] Pnyx Compliance with the Council of Europe's Security & Audit Standards on e-Voting. Scytl, December, 2004. http://www.scytl.com/docs/pub/science/Pnyx_Compliance_with_CoE_Standards.pdf

[5] Sähköisen äänestyksen pilotti 2008: Tekninen toteutus ja tietoturvaratkaisut. ("E-Voting Pilot 2008: Technical implementation and information security solutions.") TietoEnator, 28th February, 2008. http://www.vaalit.fi/uploads/7aanqsm6czk.pdf

[6] Auditointiraportti kunnallisvaalien sähköisen äänestyksen pilotista. ("An audit report on the municipal elections e-voting pilot.") University of Turku, 13th June, 2008. http://www.vaalit.fi/uploads/6d8qgeom5g.pdf

[7] These include the use case documents available from http://www.vaalit.fi/42715.htm.

has repeatedly refused to provide documents that would describe the exact operation and security aspects of the system (see appendix 1).

Electronic Frontier Finland expressed its interest to take part in the audit of the system, which was conducted by University of Turku. The association offered the help of seasoned professionals who would have worked pro bono. However, this cooperation never materialised as TietoEnator and Scytl required non-disclosure agreements that would have severely constrained the auditors' possibilities to publish their findings[8]. The Ministry of Justice tried to arbitrate a better non-disclosure agreement, but were unsuccessful, and therefore this report is based on published sources only.

Definitions

In this document, unless otherwise specified,

"electronic voting" or "e-voting" refer to the direct recording electronic (DRE, without a voter-verified paper ballot) voting at a polling station as implemented for the Finnish e-voting pilot;

"traditional voting" refers to the current Finnish voting system using paper ballots, including ballots cast at polling stations on the voting day and absentee ballots cast at post offices during preceding weeks (Finland does not recognise remote voting). Votes are counted and the voting process is observed separately at each polling station by the representatives of competing parties, and votes are then re-counted separately at a central location;

a "voter-verified paper ballot" (also known as voter-verified paper record or paper trail) is a paper ballot that is filled in using an electronic system but will be cast in an ordinary ballot box after the voter has approved its contents. This is not a "receipt" as it is not retained by the voter. The Finnish e-voting system does not use voter-verified paper ballots;

a "receipt" is a paper or electronic receipt given to the voter after casting a vote. This is different from a voter-verified paper ballot as the receipt is retained by the voter and may give the voter means to verify that the vote has been received and/or counted properly. The Finnish e-voting system does not use receipts.

Comparison with CoE recommendations

The text from Council of Europe recommendations is printed in italics.

> *The design of an e-voting system shall be underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election or referendum. The e-voting system shall include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified.*

[8] Effi's blog entry on 20th March, 2008 contains the details on the proposed NDA: http://www.effi.org/blog/2008-03-20-Tapani-Tarvainen.html

Electronic Frontier Finland hopes that this type of risk assessment has actually been done. Results of such assessment have been repeatedly requested from the Ministry of Justice, but access to risk assessment results has been denied.

The e-voting pilot required a special law to be passed by the parliament of Finland. The government bill[9] (law proposal) did not make any reference to the specific risks of DRE systems that were already widely known and documented at the time, for example, in the United States. The most comprehensive published risk analysis seems currently to be a memorandum which does acknowledge high reliance on information technology and potential software issues, and the problem of not having physical ballots to recount[10].

It is therefore highly interesting whether a broad and detailed enough risk analysis, which takes specifically DRE related issues into account, has ever been conducted.

Ministry of Justice's refusal to release risk analysis results was brought to the supreme administrative court of Finland by an individual[11]. At the time of writing, the decision is still pending, however, as a part of the proceedings the Ministy of Justice referred[12] to two documents[13,14] that allegedly contain risk analysis information. Only one of them seems to have been written at the beginning of the project. The date of the other document suggests that it has, like the University of Turku audit report, to have been written after the system has apparently been already (almost) completed.

Effi would like to point out that a security threat analysis and risk assessment are today a standard practice for any self-respecting software vendor, and those should be conducted *before* the implementation takes place. As an example, Microsoft has even written a book[15] of its own secure software development lifecycle. If the voting system has not been subjected to a proper security threat and risk analysis, this is a major deviation from the recommendations.

[9] Government Bill (Hallituksen esitys) HE 14/2006: http://www.finlex.fi/fi/esitykset/he/2006/20060014

[10] Ministry of Justice memorandum 12th January, 2004. http://www.vaalit.fi/uploads/wtethk6kup41.pdf

[11] Supreme administrative court, case number 1683/1/08.

[12] Ministry of Justice statement 20/51/2008, 18th June, 2008.

[13] Ehdotukset pilotin tuotannonaikaisista toimenpiteistä. ("Proposals on production-time activities of the pilot.") 3rd October, 2006. Not published.

[14] Auditoijan opas. ("Auditor's guide.") 25th February, 2008. Not published.

[15] M. Howard ja S. Lipner. SDL: The Security Development Lifecycle. Microsoft Press, 2006.

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

The recommendation states earlier that "[*e*]-*voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means*". The reliability of the traditional voting system is highly dependent on the voters and election officers understanding of the correct procedures and mechanics of the voting process. E-voting systems should be understood at an equal level.

However, arriving at an equal level is currently impossible. First, the Ministry of Justice has refused to release exact information of the e-voting system (this also counters the spirit, if not the text, of the recommendation 21, "[*i*]*nformation on the functioning of an e-voting system shall be made publicly available.*").

Second, understanding the traditional voting system is possible for anyone as it operates in the physical world of paper, envelopes, wooden boxes and physical security (doors, locks, etc.), for which people have significant practical experience and can have realistic assumptions of security. A similar level of understanding in e-voting would require significant information technology and information security expertise. In addition, the documents released[16] by the Ministry of Justice are so general and high-level in nature, that even an information technology expert cannot arrive at an equal level of understanding. Full understanding would require fully transparent access to the system source code and its development processes.

Because of this, the vast majority of voters need to trust a third party who has audited the e-voting system and written an audit report. Compared with the traditional system, the trust is concentrated in a much smaller group and we argue that even the auditors' specialist understanding is on a lower level than in traditional voting.

In addition, we believe that the auditors are likely to be under a non-disclosure agreement (see "Background" on page 2). If this is indeed the case, it may restrict their possibilities of reporting on their findings.

With regard to NDAs, Electronic Frontier Finland understands that trade secrets must be honoured in a competitive business environment. However, we believe that applying non-disclosure agreements and trade secrets to a voting system of a democratic country is in direct conflict with the spirit of Council of Europe recommendations.

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

[16] Ministry of Justice has done a significant amount of awareness raising activity, partially through their elections portal http://www.vaalit.fi/. However, the awareness material does not help with determining the trustworthiness and reliability of the system, as the material that has been published is too general in nature.

as well as

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

The e-voting counting process cannot be "observed" in the traditional sense, as the counting itself takes place within the software of the e-voting system. Software activity cannot be observed by human senses. The only things that can be observed are those that are chosen to be displayed by the software. The fact that an observer can see something, for example, on a workstation screen or on a printer, are not direct evidence of how the counting process is executing, but instead an indirect indication that is controlled by the software. In contrast, in a traditional vote counting, the actual counting can be observed as the ballots are physical items and the numbers written on them can be seen with a naked eye.

Essentially this means that the observers must have faith in the system developers and auditors. This is not to say that observers would not be necessary – they are needed to observe the persons who operate the vote counting software – but the observers cannot directly observe the vote counting process itself.

> *225. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.*

Software is developed by writing source code. Source code is a human-readable form of software, which is later transformed into a program that is actually run by the computer.

The source code of a complex system is a very large amount of text. During development, it is usually stored in a centralised place called a version control system, where all programmers will introduce their changes.

In order to really track the changes, the independent body should also be able to monitor the development of the software and not only the finished product. Finding problems in the finished product is like finding the needle in a haystack.

The "necessary security measures" defined by the recommendation are also related to whether the software is written by following the principles of a secure software development lifecycle. Because of this, the software vendors and systems integrators should describe all their software development processes. This includes, for example, how source code changes are authorised and controlled.

Unless the software development practices can also be audited, the independent body will not be able to give full assurances of the software integrity and security. In addition, following the proper software development practices needs to be assured in all situations, and this might prove to be extremely difficult in times of internal or external political pressure.

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

Recounts aim at detecting transient errors, such as humans losing count, by comparing the results of separate counts. In the proposed e-voting system, a recount by the same vote counting software cannot detect a systemic counting error. Software is deterministic, that is, given the same inputs, software will always produce the same output. Because of this, recounts made using the same system that was used for the first count are meaningless as the inputs an the software will stay the same.

In addition, the vote-counting software can only produce a result that is as good as the original correctness of ballot information. If the ballots have been incorrectly cast and stored by the voting system in the voting booth, no number of recounts – even by independent systems – is going to remedy this situation.

The only way to conduct a trustworthy recount in an electronic voting system is to introduce a completely independent way of casting the vote and counting the ballots. This might be a mathematical construct[17] (a protocol that can provide the voter with a receipt) or a voter verified paper ballot, which is cast alongside with the electronic vote. Neither of these assurance methods are used in the Finnish e-voting pilot.

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

The most critical "technical activity" is the actual development of the system, meaning its design and implementation.

If there is even one critical part of the system that might be affected by a small team of people (such as bribed or careless programmers), the risk of malicious or non-malicious programming errors being introduced is very real.

The two-person and team composition change recommendations are the minimum requirements, but this should also be extended to software development time and be clearly documented.

We currently have no information whether these recommendations have been followed at the system development time.

[17] It should be noted that the Finnish e-voting system does use cryptography internally. However, this is not the type of cryptography we mean here. What we would like to see would be one of the e-voting protocols specifically designed to guarantee confidentiality and anti-coercion through mathematical constructs that can be proven to do so.

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

As previously discussed in this document (with regard to recommendations 23 and 56), the counting of ballots in e-voting will not be performed by the operators of the system but in fact by the software.

This means that the ballots are not counted by the Helsinki Voting District Committee[18] or the Ministry of Justice. Instead they will only be executing the computer program that actually counts the votes.

This computer program does what its programmer has instructed it to do. Therefore, if one wants to identify the actual persons who are involved in the vote counting process, those persons are in fact the persons who have implemented the e-voting system. It is probable that there are several of these persons and they may well be foreign citizens. These people will take part in the counting process in a very direct and concrete fashion.

Electronic Frontier Finland would also like to point out that traditional paper ballots will be counted by the representatives from competing parties, separately at each polling station. Competing parties have a strong interest to monitor each others' behaviour at the polling stations. In addition, the traditional counting process is extremely distributed. Conducting a large scale fraud in the traditional election would require a large number of polling stations to be compromised.

In contrast, counting the votes in the electronic ballot box has been centralised into a single computer system with a single supplier. The fact that the encryption keys required for accessing the contents of the electronic ballot box are split between different keyholders is in itself mostly irrelevant. Being authorised to start the counting process does not guarantee the correctness of the result.

As a potential analogy, counting the votes in the proposed e-voting system might be compared to a set-up where counting the traditional ballots would be contracted to a single company without oversight on the counting activity itself.

> *59. The e-voting system shall be auditable.*

The e-voting system was audited by a team from the University of Turku. The audit report[19] was released by the Ministry of Justice and warrants a longer discussion, which can be found in its own section later in this document.

[18] Helsinki Voting District Committee (Helsingin vaalipiirilautakunta) is made up of representatives of different parties. They have a role in overseeing the count of electronic ballots, namely unlocking the electronic ballot box.

We also believe that the system is too complex to be fully auditable. Discussion of this can be found below, as it relates to recommendations 75 and 92.

> *75. Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from any person. During the election or referendum period a physical disaster recovery plan shall be in place. Furthermore, any data retained after the election or referendum period shall be stored securely.*

Storing the e-voting equipment is a risk that has been realised in the United States. Voting machines have been found unattended at polling stations[20]. Because of this, this risk has to be taken seriously. Luckily, we have no reason to believe that this aspect wouldn't be handled appropriately.

However, it is highly questionable whether others than computer hardware specialists can spot if any unauthorised modifications have been done to the e-voting machines. According to the Ministry of Justice, the e-voting system utilises off-the-shelf PC hardware. This kind of hardware has a significant number of interfaces such as USB interfaces, all of which may not necessarily be seen from outside but may be present on the motherboard. Even if the hardware would be booted from a dedicated boot medium, the machine may still first execute programs that have been injected through one of these interfaces. This risk has also been identified in the United States[21].

Changes made to the hardware may be invisible to the naked eye as they may be located within the firmware inside the components themselves (such as hard disk firmware, which could alter the data which is being written to disk, or in the display adapter, which could alter the data being shown on the screen). The changes may have been done a long time before the hardware has been delivered to the election officials. Electronic Frontier Finland would like to draw attention to the complete sourcing chain and chain of custody of the e-voting equipment as well as their firmware.

> *92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.*

[19] Auditointiraportti kunnallisvaalien sähköisen äänestyksen pilotista. ("An audit report on the municipal elections e-voting pilot.") University of Turku, 13th June, 2008. http://www.vaalit.fi/uploads/6d8qgeom5g.pdf

[20] Ed Felten is an information security professional who has witnessed this already three times: http://www.freedom-to-tinker.com/?p=1297, http://www.freedom-to-tinker.com/?p=1253 and http://www.freedom-to-tinker.com/?p=1084.

[21] See "Boot loader reflashing" in Diebold TSx Evaluation document by Harri Hursti, 11th May 2006. http://www.blackboxvoting.org/BBVtsxstudy.pdf

The e-voting booth at the polling station is fully responsible for correctly storing the ballot and therefore it is the most critical part of the system.

As has been previously stated many times, the end user cannot actually know what the software is doing. Even if the software would display the voter's selection on the screen and the voter would accept it, it does not guarantee that the vote will actually be stored correctly in the electronic ballot box. This problem was also highlighted in the audit report.

The Spanish voting engine provider Scytl offers an electronic receipt that the voter could later use to determine whether the vote has been counted: *"Pnyx generates a voting receipt that allows each individual voter to verify the correct treatment of his/her vote"*[22]. The receipt cannot be used to determine whom was voted, as this might lead to coercion and vote-buying[23]. The function of the receipt in Scytl's system is only to show that the ballot has been delivered and counted. This functionality does not seem to be used in the system which is to be used in Finland.

Problems do not necessarily have to reside in software. For example, touchscreen calibration problems have been found in the United States[24]. This could lead to a situation where the user chooses a candidate on the screen, but a different candidate is registered on the electronic ballot.

In the Finnish e-voting pilot, touchscreen calibration is probably not a big issue as the voter has to check the candidate information before the voting process is complete. However, this is a good example of the fact that problems may crop up in any part of the system. There are a very large number of these components – both software and hardware – and they have been implemented in various parts of the world[25]. Auditing them all is practically impossible.

> *107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.*

[22] Pnyx Compliance with the Council of Europe’s Security & Audit Standards on e-Voting. Scytl, December, 2004. http://www.scytl.com/docs/pub/science/Pnyx_Compliance_with_CoE_Standards.pdf

[23] It is possible to build a voting protocol that uses suitable mathematical constructs to check that the vote has also been counted correctly. However, based on what we have understood from Scytl material, the receipt provided by the Pnyx voting engine does not seem to offer this option.

[24] Again Ed Felten's blog, http://www.freedom-to-tinker.com/index.php?p=707.

[25] Security and usability expert Ka-Ping Yee has drawn a picture of the components of a typical e-voting system. Any of these components might affect the results. http://usablesecurity.com/2006/02/23/the-election-software-supply-chain/

If the audit system is built as a part of the e-voting system, it comes from the same supplier, and is in itself audited by the same team that audits the e-voting system, it cannot protect from issues that are intrinsic to the system.

Therefore any audit system would need to be decoupled from the e-voting system.

Electronic Frontier Finland believes that until mathematically sound e-voting systems that have formal proofs are commercially available, e-voting should use a voter verified paper ballot. In this case, the voter would vote with the e-voting system but in addition to the vote being stored electronically, the system would produce a paper ballot. This would be dropped to a traditional ballot box after being inspected by the voter. Recounts could then be facilitated by these physical hard copies of the ballots.

Of course, a voter verified paper ballot would nullify most of the benefits that an e-voting system allegedly brings to a Finnish election[26], but perhaps the results could be checked by sampling the paper ballots only at some polling stations and applying statistical methods for the rest.

In the United States, a voter verified paper ballot (also known as paper trail or paper record) is a requirement in 31 states[27]. The requirement has also been proposed in the Netherlands[28], although the requirement was deemed too problematic with the result of falling back to traditional voting altogether[29].

Electronic Frontier Finland does not see any reason why the Finnish e-voting system would be more trustworthy in some magical way than the ones used in the United States or the Netherlands. Because of this, voter verified paper ballots should be mandated in our e-voting pilot as well.

[26] Finnish elections are quite simple: only one candidate is voted for, identified by a number. There are no write-in candidates. Elections are single-purpose only: there are separate elections for the president, for the town council, for the parliament and for the European Union parliament. Vote counts are ready in a matter of hours as the counting is highly distributed. What benefits e-voting would bring is not very clear.

[27] http://www.verifiedvoting.org/

[28] Stemmen met vertrouwen. Adviescommissie inrichten verkiezingsproces. 27th September 2007. http://www.minbzk.nl/108589/stemmen-met

[29] A letter from the Ministry of Interior of the Netherlands to the speaker of the lower house, 16th May 2008. http://www.wijvertrouwenstemcomputersniet.nl/images/7/7b/Briefaantweedekamerov erinrichtingverkiezingsproces.pdf

Comments on the audit report

University of Turku was commissioned to audit the e-voting system. Their audit report[30] was published by the Ministy of Justice. This section highlights some of their most critical findings.

Upon releasing the audit report, Ministry of Justice stated[31] that the audit findings show that the e-voting system is on a "solid and secure foundation".

The Ministry of Justice also stated that the findings would be addressed "as required", but at the time of writing they have made no public statement of who will determine what is important, how those findings will be addressed, and whether the system will ever be audited again after making the changes or after any other updates have been applied.

Among the audit findings, the following are of great interest in the context of Council of Europe recommendations. The page numbers refer to the pages of the audit report.

- It is possible to find out how an individual voter voted, as votes are processed in an unencrypted form during the counting process, with voter-identifying information attached to each vote. It seems that ballot secrecy could be compromised by system programmers or a group of insiders having access to all decryption keys, as according to the audit report, both the electronic ballot box and the keys would be archived for several years (page 6). Electronic Frontier Finland argued that this finding actually makes the system incompatible with Finnish law[32]. Today, cryptographic protocols exist where this type of threat does not exist, and Electronic Frontier Finland is concerned why the Finnish system does not seem to be based on such protocols.

- Only the critical parts of the source code have been audited (audit report, page 3). Supporting software (for example, the operating system and drivers) have not been audited (page 8). The operating system boot disk version that was used in the audit was not the final one (page 9).

- Voters have no way of being assured that their votes were correctly delivered and counted (pages 3 and 4). This is related to the lack of a receipt or any mathematically sound voting protocol that would ensure this.

[30] Auditointiraportti kunnallisvaalien sähköisen äänestyksen pilotista. ("An audit report on the municipal elections e-voting pilot.") University of Turku, 13th June, 2008. http://www.vaalit.fi/uploads/6d8qgeom5g.pdf

[31] Ministry of Justice press release on 19th June, 2008. http://www.om.fi/Etusivu/Ajankohtaista/Uutiset/Uutisarkisto/Uutiset2008/1213368440031

[32] Effi press release on 24th June, 2008. http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2008-06-24.html

- The software which is being used is a trade secret and cannot be published (page 4).
- A group of insiders could in theory create a bogus ballot box and count the votes from that ballot box (page 6), as the votes are not cryptographically signed by the polling station or voter, independently of the counting authority.

Further information

Electronic Frontier Finland maintains a frequently asked questions list on e-voting issues in Finnish language. The FAQ clarifies, for example, why a comparison between Internet banking and e-voting is flawed. Our FAQ can be read at http://www.effi.org/sahkoaanestys-faq.html (at the time of writing, no English language version is available).

The most recent version of this document can be acquired from the Electronic Frontier Finland web site, http://www.effi.org/.

This document has been released into public domain. Attribution to Electronic Frontier Finland (Effi) is kindly requested.

Appendix 1

E-voting documents were requested from the Ministry of Justice under the Finnish Act on the Openness of Government Activities[33] (which bears some resemblance to FOI laws in other countries). They declined to release all the requested documents with the following rationale[34]:

> *According to the Act on the Openness of Government Activities (621/1999, JulkL) section 24.1 clause 7, documents relating to or affecting the implementation of the security arrangements of information and communications systems should be kept secret, unless it is clear that the target of the security arrangements would not be compromised by their release. Detailed technical documentation is typically secret and cannot therefore be released (see the Government Bill on the Act on the Openness of Government Activities and related acts, HE 30 1998 vp, p. 91).*

Electronic Frontier Finland would like to point out that physical security arrangements, such as storage of voting machines, naturally contains aspects that should be kept secret. Similarly, it is understandable that for example banks do not divulge details of their information systems to those who have no need to know. However, we are now talking about software that is to be used in a democratic election. These systems must be engineered to be secure even if their internal workings (for example, source code) would be made completely public. This principle is known as the Kerckhoffs' principle[35] and is widely accepted in information security design. Even though the system uses public and known cryptographic algorithms, this is not enough: the main point is that actually how these algorithms are used, and whether they and their surrounding software has been implemented correctly.

Moreover,

> *According to the Act on the Openness of Government Activities section 24.1 clause 20, official documents that should be kept secret include documents containing information on a private trade or professional secrets, as well as documents containing other comparable private business information* [...]

Basically this means that according to the Ministry of Justice response, some documents may be considered trade secrets of the system vendors and cannot therefore be released.

[33] Act on the Openness of Government Activities. An unofficial English translation available at http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf

[34] A response (by e-mail) from the Ministry of Justice to a document request, 29th February, 2008. Translated into English.

[35] http://en.wikipedia.org/wiki/Kerckhoffs%27_principle

Electronic Frontier Finland would like to comment that the integrity and correctness of democratic elections cannot be a trade secret. The votes are counted by the software, not by the software operator. Electronic Frontier Finland believes that holding the details of the counting process a trade secret is plainly unacceptable.