# A Report on the Finnish E-Voting Pilot

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

28 November 2009[1]
Edited by Antti Vähä-Sipilä

## Background

Finland piloted a direct recording electronic (DRE) type, polling station based (non-remote) e-voting system in its municipal elections in October 2008.

This report summarises the timeline of the e-voting pilot project. It comments the audit results of the Finnish system performed prior to the election, as well as a report produced after the pilot by Ministry of Justice, highlighting the issues and setting out potential requirements for future e-voting programmes.

In addition, this document compares the Finnish e-voting system with the Council of Europe recommendations for e-voting.

Information and claims on the Finnish e-voting system are based on information provided by the Ministry of Justice[2,3,4,5]. The Ministry of Justice has also released

[1] This is an update to the English language report, originally titled "Incompatibility of the Finnish e-voting system with the Council of Europe e-voting recommendations", first published in August 2008, before the Finnish e-voting pilot was actually used in an election. It has been updated and in all respects, it replaces all earlier versions of the report. This report (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, we would be more than happy to amend and correct the document, so 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

[3] 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

[4] 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

other documents pertaining to the system[6], but it has repeatedly refused to provide documents that would describe the exact operation and security aspects of the system.

It is important to note that the arguments made in this report either address the e-voting system as a whole, including the commissioning and operational phases, or the concept of fully electronic voting in general. It does not make claims about individual components (like the e-voting core) or specific supplier companies. The e-voting system is just as good as its weakest link; a single good component cannot offer assurances to the complete system.

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 1600 individual members.

## 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, one example of such system being the one that was 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 representatives of competing parties observe the voting process separately at each polling station, 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 the voter does not retain it. 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

[5] Sähköisen äänestyksen pilottihanke vuoden 2008 kunnallisvaaleissa ("The e-voting pilot in the 2008 municipal elections"). A memorandum from the Ministry of Justice, 30 September 2009. http://www.hare.vn.fi/upload/Asiakirjat/10514/30.9.2009, muistio sähköisestä äänestyksestä.doc

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

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.

# The Timeline

## *Before the elections*

The Finnish e-voting pilot[7] was based on a special temporary law[8] that was passed in 2006, which authorised electronic voting in the municipal elections of October 2008. Three municipalities (Karkkila, Kauniainen and Vihti) piloted this e-voting system. The law expired at the end of 2008. The use of e-voting in future elections would require new legislation.

Electronic Frontier Finland (Effi) was one of the first to raise public discussion on the e-voting pilot[9]. A member of Effi had requested e-voting related documents from the Ministry of Justice under the Finnish Act on the Openness of Government Activities[10] (which bears some resemblance to freedom of information laws in other countries). They declined to release all the requested documents with the following rationale[11]:

> *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).* (Unofficial translation)

and

> *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*

[7] Ministry of Justice project number OM024:00/2005, started 22 February 2005.

[8] Laki vaalilain muuttamisesta ("Law on changes to the election law"), 880/2006. The law was in effect from 1 January 2007 to 31 December 2008.

[9] Sähköisen äänestyksen pilottihanke vuoden 2008 kunnallisvaaleissa ("The e-voting pilot in the 2008 municipal elections"). A memorandum from the Ministry of Justice, 30 September 2009. http://www.hare.vn.fi/upload/Asiakirjat/10514/30.9.2009, muistio sähköisestä äänestyksestä.doc

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

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

> *documents containing other comparable private business information* [...] (Unofficial translation)

Electronic Frontier Finland felt that this response was inappropriate and unacceptable, as the voting system is one of the underpinnings of a democratic state. Of course, the physical security arrangements, such as storage of voting machines, naturally contain 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, in our opinion, software systems used in democratic elections 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[12] and is widely accepted in information security design.

These arguments raised the interest of the press, and brought the information security aspects of e-voting into the public discussion for the remainder of the project.

During the spring of 2008, University of Turku was commissioned to audit the e-voting system. Their audit report[13] was published by the Ministy of Justice.

Electronic Frontier Finland expressed its interest to take part in the audit. The association offered the help of seasoned professionals who would have worked pro bono. However, this cooperation never materialised, as TietoEnator, a Finnish company acting as a system integrator, required non-disclosure agreements that would have severely constrained the auditors' possibilities to publish their findings[14]. The Ministry of Justice tried to arbitrate a better non-disclosure agreement, but were unsuccessful.

Upon releasing the audit report, Ministry of Justice stated[15] 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 made no public statement of who would determine what is important, how those findings would be addressed, and whether the system would ever be audited again after making the changes or after any other updates have been applied.

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

[13] 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

[14] 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

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

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 University of Turku audit report. The audit report found that:

- According to the report, if the vote-counting software had been compromised, it could be theoretically 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. Also, the audit report found that individuals that could alter program code or have access to all decryption keys could compromise ballot secrecy, as 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, as the law requires this to be "not possible"[16].

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

- Further, the auditors found that there is no direct way to observe that a vote is recorded appropriately and that in this respect, the voter must just trust the software and voting officials (pages 3 and 4).

- The software, which is being used, is a trade secret and cannot be published (page 4).

- The auditors said that a group of insiders could in theory create a second ballot box and count the votes from that ballot box instead of the real one (page 6).

## *After the elections*

Several observers were present during the actual voting. The Council of Europe issued a report[17], which highlighted some of the same worries that had been raised by Electronic Frontier Finland, for example:

> *42. The information remains on the vote count computer until the next elections. The representatives of the IT contractor TietoEnator also acknowledged that a copy of all these elements would remain on their server until the elections had been certified. A theoretical possibility of decrypting the information does exist, including with the use of the four separately held e-keys that were required to make the decryption and vote count computer function.*

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

[17] Information report on the electronic voting in the Finnish municipal elections observed on 26 October 2008. Council of Europe.
https://wcd.coe.int/ViewDoc.jsp?id=1380337&Site=Congress

> *43. One may nevertheless pose the purely hypothetical question whether extraordinary events could lead to a situation where the responsible public officials, or indeed the involved computer experts, are forced to process and divulge the information on who voted how.*
>
> *48. In some instances, the source code has been published by the election authorities, at least after the elections. The Finnish authorities did not have any intention to do so. Information about the system audit that preceded the elections was published, but Your Rapporteur was told that more information clearly could have been provided to the public by the authorities.*
>
> *58. The measures to ensure transparency could also benefit from a review. A voter-verified paper trail could have helped avoiding the encountered problems, facilitated a possible recount and increased transparency. More general information about the experiment, in particular system certification, could also possibly have been made available by the organising authorities.*

During the main voting day, one person contacted one of the election boards, having got a feeling that the vote had not been registered. After further study, it turned out that 232 votes had been lost due to a usability issue[18]. It seems that the system required the voter to insert a smart card to identify the voter, type in their selected candidate number, then press "ok", check the candidate details on the screen, and then press "ok" again. Some voters did not press "ok" for the second time, but instead removed their smart card from the voting terminal prematurely, causing their ballots not to be cast.

This usability issue was exacerbated by Ministry of Justice instructions, which specifically said[19] that in order to cancel the voting process, the user should click on "cancel" and after that, remove the smart card. Thus, some voters did not realise that their vote had not been registered.

Voters from all three municipalities filed complaints under the election law. At first, the Helsinki Administrative Court ruled that the elections were lawful[20]. Later, the

[18] Sähköisen äänestyksen kokeilusta myönteistä palautetta – noin 200 äänestystä kuitenkin keskeytyi erehdyksessä ("E-voting pilot gets positive feedback - however, approximately 200 ballots were prematurely interrupted"). Ministry of Justice press release, 28 October 2008. http://www.om.fi/Etusivu/Ajankohtaista/Uutiset/1224166604122

[19] Ministry of Justice e-voting instructions (as of October 2008). http://www.vaalit.fi/sahkoinenaanestaminen/aanestyksen_kulku.html

[20] Helsingin hallinto-oikeuden päätös sähköäänestysasiassa ("Helsinki Administrative Court decision on the e-coting case"). Effi's blog entry, containing an unofficial copy of the ruling. 29 January 2009. http://www.effi.org/blog/hhao-2009-01-29.html

Supreme Administrative Court annulled the elections in these three municipalities[21]. New elections were held in September 2009.

Later in 2009, Ministry of Justice produced a report[22] on the e-voting pilot. This Ministry of Justice report contained a thorough timeline of the e-voting pilot and contains some interesting observations, such as

> *Both the closing* [probably meaning creation] *and opening of the* [electronic] *ballot box were extremely information technology heavy events. The success of the events practically relied on the IT supplier's staff acting appropriately. The others who were present and were not IT experts had hard time following and commenting the events.* (Unofficial translation)

Although there is no reason to suspect any foul play, Effi feels that reliance on IT staff on the correctness of the results is worrying.

In addition, the report states that

> *Due to the exceptional circumstances of the 2008 municipal elections, a copy of the electronic ballot box was also stored on TietoEnator* [the IT services provider] *servers* [in addition to being only stored in a physical safe, as was the original intention]. (Unofficial translation)

Although that copy was also encrypted, in our opinion, this greatly affected the chain of custody of the electronic ballot box.

The Ministry of Justice solicited comments for their report, after which the continuation of e-voting will be later discussed. The report also tentatively proposed potential future changes to e-voting, such as using open source software and voter-verified paper ballots.

At the time of writing, the commenting period for the report has closed and future actions are open.

[21] Supreme Administrative Court decision KHO:2009:39 (687/1/09), 9 April 2009. http://www.kho.fi/paatokset/46372.htm

[22] Sähköisen äänestyksen pilottihanke vuoden 2008 kunnallisvaaleissa ("The e-voting pilot in the 2008 municipal elections"). A memorandum from the Ministry of Justice, 30 September 2009. http://www.hare.vn.fi/upload/Asiakirjat/10514/30.9.2009, muistio sähköisestä äänestyksestä.doc

## Comparison with CoE recommendations

In this section, we compare the Finnish e-voting pilot system against the Council of Europe recommendation Rec(2004)11[23].

When we argue that something could affect the outcome of the election, these are theoretical or hypothetical cases. In the Finnish pilot, we have no reason to suspect any foul play or suboptimal quality or engineering practices from any vendor.

We have interpreted Council of Europe recommendations so that they would need to hold also on theoretical level, and also in the presence of hypothetical malicious intent.

It is important also to note that the arguments made in this report either address the e-voting system as a whole, including the commissioning and operational phases, or the concept of fully electronic voting in general. The e-voting system is just as good as its weakest link; a single good component cannot offer assurances to the complete system. We do not make claims about specific supplier companies or the compliance of individual components.

The text from the Council of Europe recommendation 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.*

Electronic Frontier Finland hopes that this type of risk assessment has actually been done on the complete system level. Results of such an 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[24] (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 before the election took place seemed to be a memorandum, which did acknowledge high

[23] 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

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

reliance on information technology and potential software issues, and the problem of not having physical ballots to recount[25].

It is therefore highly interesting whether a broad and detailed enough risk analysis, which takes specifically DRE related issues into account, had 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[26]. At the time of writing, the decision is still pending, however, as a part of the proceedings the Ministy of Justice referred[27] to two documents[28,29] 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, 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 many software vendors, and those should be conducted *before* the implementation takes place. As an example, Microsoft has even written a book[30] of its own secure software development lifecycle. It is most likely that individual components used in the e-voting system have been assessed by their vendors, but if the complete voting system had not been subjected to a proper system-level security threat and risk analysis, in our opinion, this is a major deviation from the recommendations.

> *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.

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

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

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

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

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

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

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. This was also echoed in the Ministry of Justice summary report. In addition, the documents released[31] 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. If this is indeed the case, it could 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 the Ministry of Justice is in conflict with the spirit of Council of Europe recommendations by electing to use an e-voting system that is protected under non-disclosure agreements and trade secrets.

> *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.*

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 directly "observed" in the traditional sense, as the counting itself takes place within the software of the e-voting system. Software

[31] 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.

activity cannot be observed by human senses. The only things that can be observed are those that software chooses to display. 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 preferably describe all their software development processes. This includes, for example, how source code changes are authorised and controlled.

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 will always yield the same result, as the inputs of 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[32] or a voter verified paper ballot, which is cast alongside with the electronic vote. Neither of these assurance methods was 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 hypothetical bribed or careless programmers), the risk of malicious or non-malicious programming errors being introduced increases.

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.

> *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 was not directly performed by the operators of the system but in fact by the software.

[32] One of the e-voting protocols specifically designed to guarantee confidentiality and anti-coercion through mathematical constructs that can be proven to do so. Essentially a protocol that would enable the voter to verify that the vote has been counted correctly, but without possibility to prove to others how the voter voted.

This means that the ballots were not directly counted by the Helsinki Voting District Committee[33] or the Ministry of Justice. Instead they only executed the computer program that actually counted the votes.

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

Electronic Frontier Finland would also like to point out that traditional paper ballots would be counted by the representatives from competing parties, separately at each polling station. Competing parties have a strong interest to monitor each other's 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.

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

A team from the University of Turku audited the e-voting system. The audit report[34] was released by the Ministry of Justice and was commented earlier in this report.

We also believe that the system is so complex that the costs of a full audit would be prohibitive. 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[35]. Because of this,

[33] 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.

[34] 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

[35] 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.

this risk has to be taken seriously. Luckily, it seems this aspect was 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[36].

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.*

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 directly observe what the software is doing. Even if the system would display the voter's selection on the screen and the voter would accept it, as for correctly storing the vote in the ballot box, all software components involved in this have to be trusted. This problem was also highlighted in the audit report.

These issues could have been mitigated to some extent by using technology from the e-voting engine supplier. The voting engine used in the Finnish pilot offers an electronic receipt that the voter could later have used 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"*[37]. Even though the receipt cannot be used to determine whom was voted, as this might lead to coercion and vote-buying[38],

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

[37] 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

it still could have been used to show that the vote was delivered and counted. This functionality was not used in the Finnish system.

Problems do not necessarily have to reside in software. For example, touchscreen calibration problems have been found in the United States[39]. 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 was 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[40]. Auditing them all would be very costly.

> *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.*

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[41], but perhaps the results could be checked by sampling the paper ballots only at some polling stations and applying statistical methods for the rest.

[38] 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 version of the Pnyx voting engine used in the Finnish pilot did not seem to offer this option.

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

[40] 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/

[41] 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.

In the United States, a voter verified paper ballot (also known as paper trail or paper record) is a requirement in 32 states[42]. The requirement has also been proposed in the Netherlands[43], although the requirement was deemed too problematic with the result of falling back to traditional voting altogether[44].

Electronic Frontier Finland does not see any reason why the Finnish e-voting system would be trustworthier 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.

## 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/.

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

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

[44] 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