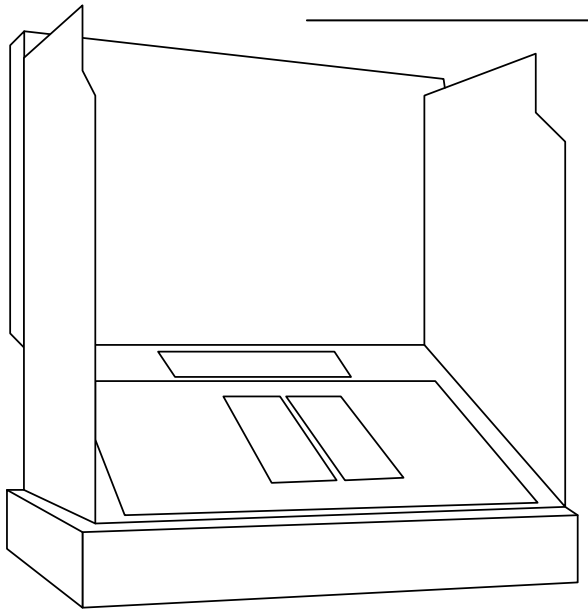
e-Voting

Hacking the Electoral Law



23nd Chaos Communication Congress

Berlin, 27/12/2006

Ulrich Wiesner

Claim

- In Germany (and other countries), the administration turns fundamental election principals into their opposite, without parliamentary authorisation.
- They have, effectively, hacked the Electoral Law
- The “Hacking Tool” they use are voting computers.

Agenda

- Overview
  - Terminology, Status quo
- Fundamental Principles of Democratic Elections
  - Copenhagen Declaration of OSCE member states
  - Implementation example: German constitution, electoral law and electoral regulations
- Hacking the Electoral Law: Violation of Democratic Principles
  - Germany: Nedap
  - Hamburg: Digital Pen
  - e-Counting: Hessen, Bayern, Baden-Würtemberg
- Where are we?
  - Legal action
  - Upcoming elections

Terminology

- e-Voting
  - Electronic Voting
  - offline or online
  - In election office or remotely
  - using public or private equipment

- e-Counting
  - Computer assisted counting of paper ballots
  - Barcode, PC based capture of ballots…

Flavours

- Voting Computers
  - DRE (Direct Recording Electronics)
    - With or without paper trail
  - Optical Scanners

- Remote e-Voting = Internet voting
  - Vote casting from private PCs over a public network
  - Just picking up
    - Estonia: Launched for regional elections 2005
    - Pilots in Switzerland since 2004

Situation

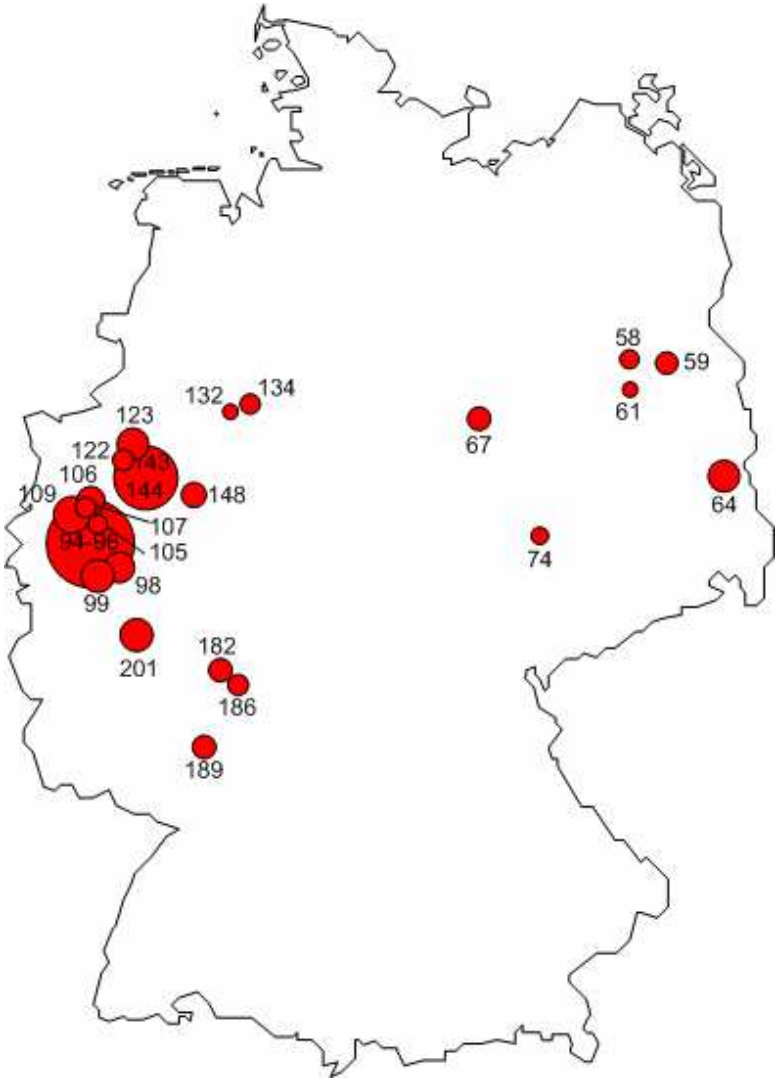
- More and more Countries switching to e-Voting
  - Early adaptors: The Netherlands, India, Brazil, Belgium
  - High penetration: Venezuela, USA, Ireland
  - Picking up: France, Germany, Kazakhstan
  - Getting ready: Namibia, Poland,…
- Internet Voting
  - Launched in Estonia in local elections
  - Switzerland run several pilots
  - Getting ready: Lithuania

Germany

- National elections
  - 5% of votes are cast with DRE
  - Nedap currently only certified vendor
  - Rumours that ES&S is preparing for market entry
- State or local elections
  - Nedaps allowed in some federal states
    - Nordrhein-Westfalen, Hessen, Rheinland-Pfalz, Brandenburg, Niedersachsen
  - Hamburg about to launch “digital pen”
    - Based on Anoto technology – scan while you write
- E-Counting entering through the backdoor in some areas
  - Hessen, Bayern, Baden-Württemberg

Bundestagswahl 2005

- ~2000 Nedaps used
  - ~1000 voters per device
- Major Cities using Nedaps:
  - Cologne
  - Dortmund
  - Neuss
  - Cottbus
  - Koblenz



Fundamental Principles of Democratic Elections

1990 OSCE Copenhagen Declaration

- **Free** elections at reasonable intervals.
- All seat in at least one chamber of national legislature are freely contested in popular vote
- **Universal** and **equal** suffrage for adult citizens
- Votes are cast by **secret** ballot or equivalent free voting procedure
- Votes are **counted and reported honestly** with results made public
- Respect the right of individuals and groups to establish, in full **freedom**, their own political parties
- Permit political campaigning to be conducted in a **fair** and **free** atmosphere
- unimpeded access to the media on a non-discriminatory basis for all political groupings and individuals
- Elected candidates are duly installed in office and permitted to remain in office until their term expires
- **Observers**, both foreign and domestic, are permitted and invited

Implementation Example - Germany

- **Constitution, Article 38 (1)** Members of the German Bundestag shall be elected in **general**, direct, **free**, **equal**, and **secret** elections. They shall be representatives of the whole people, not bound by orders or instructions, and responsible only to their conscience.

- **Grundgesetz Art. 38 (1)** Die Abgeordneten des Deutschen Bundestages werden in **allgemeiner**, unmittelbarer, **freier**, **gleicher** und **geheimer** Wahl gewählt. Sie sind Vertreter des ganzen Volkes, an Aufträge und Weisungen nicht gebunden und nur ihrem Gewissen unterworfen.

Implementation Example - Germany

- **Constitution, Article 41**
- (1) Scrutiny of elections shall be the responsibility of the Bundestag. It shall also decide whether a Member has lost his seat.
- (2) Complaints against such decisions of the Bundestag may be lodged with the Federal Constitutional Court.

- **Grundgesetz Art. 41**
- (1) Die Wahlprüfung ist Sache des Bundestages. Er entscheidet auch, ob ein Abgeordneter des Bundestages die Mitgliedschaft verloren hat.
- (2) Gegen die Entscheidung des Bundestages ist die Beschwerde an das Bundesverfassungsgericht zulässig.

Implies: Election results need to be **verifiable** and **auditable**

Implementation Example - Germany

- **Constitution, Article 20 (1)**
- The Federal Republic of Germany is a **democratic** and social federal state.

- **Grundgesetz Art. 20 (1)**
- Die Bundesrepublik Deutschland ist ein **demokratischer** und sozialer Bundesstaat.

***Democratic* implies**: Parliament is elected, works and decides in transparent manner and in public.

Manifests in §§ 10 and 31 of Federal Electoral Act: Elections are transparent and in public

References: e.g.

•Wolfgang Schreiber: Handbuch des Wahlrechts zum Deutschen Bundestag, §10 RN 1

•Hans D. Jarass, Bodo Pieroth, Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Art. 20, RN 11

Implementation Example - Germany

- **Federal Electoral Act**
- **§10 (1)** The electoral committees negotiate, consult and decide in public meetings. […]
- **§31** The ballot is conducted in public. […]

- **Bundeswahlgesetz**
- **§10 (1)** Die Wahlausschüsse und Wahlvorstände verhandeln, beraten und entscheiden in öffentlicher Sitzung. […]
- **§31** Die Wahlhandlung ist öffentlich. […]

Implements transparency:

Everybody can observe if the election is conducted in a fair manner and honestly counted

OSCE vs. German Implementation

OSCE – Copenhagen

- Universal
- Free
- Equal
- Secret
- Honest counting and reporting
- Observable and in public

German Constitution

- General
- Free
- Direct
- Equal
- Secret
- Auditable and verifiable
- Transparent and in public

Election Principles

Conceptual

- General
- Free
- Direct
- Equal

- Define characteristics of democracy

Procedural

- Secret
- Honest counting and reporting
- Observable and transparent

- Implement and ensure adherence to conceptual principles

A closer look: Secrecy

- Enables voter to make free decision
- Prevents physical or social pressure
- Prevents vote selling/buying
- Secrecy is not voluntary
  - Voter must not be able to prove his vote
  - Voting must be receipt free

A closer look: Transparency

- Everyone can observe election process and verify that
  - The secrecy of the election is ensured
  - Only voters can cast ballot papers, and that only one vote is cast per voter
  - Nobody has access to the content of the ballot box until the end of the election
  - The votes in the ballot box (and only these) are counted
  - The votes are counted correctly and honestly

- Implies:
  - Votes are counted immediately after the election and at the polling place

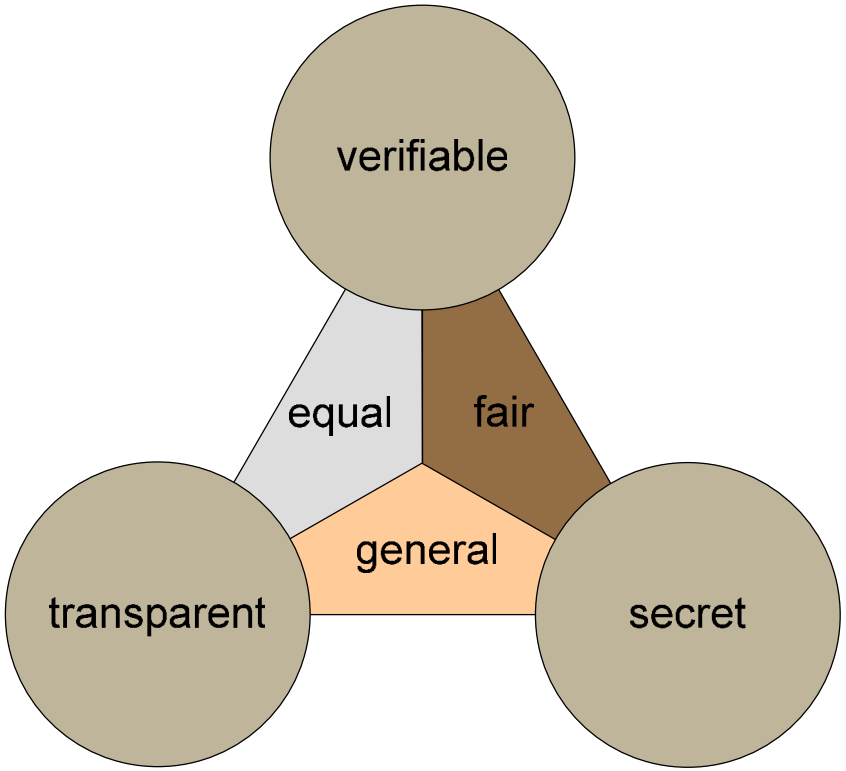
- **Ensures**
  - **The integrity of the election can be verified without trust into election officials**

A closer look: Verifiability

- Election results can be verified
- Votes can be re-counted
- There is evidence that the votes originate from the voters

Election Triangle

- **Verifiability**, **transparency** and **secrecy** ensure that elections are **free**, **fair** and **general**

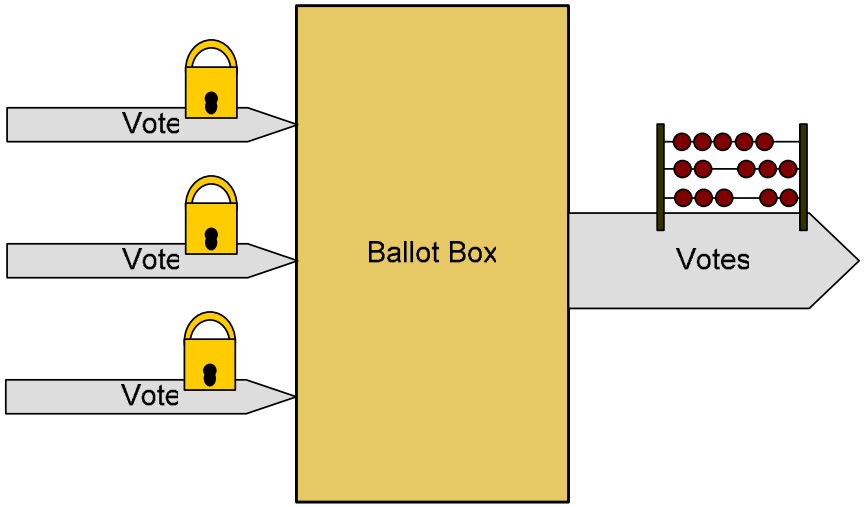


Hacking the Electoral Law

How e-Voting violates democratic principles

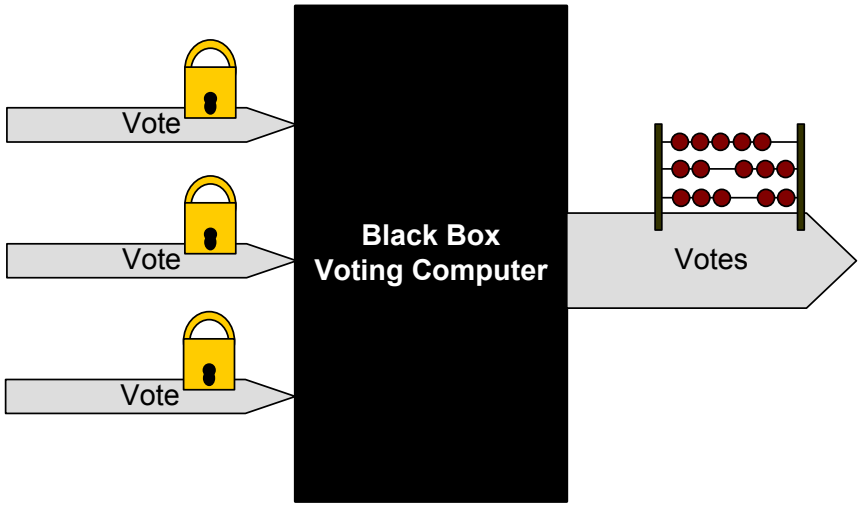
Black box voting – where is the issue?

- Paper based election



- Ballot Box is passive device
- Output is input
- Tampering needs to be done in public

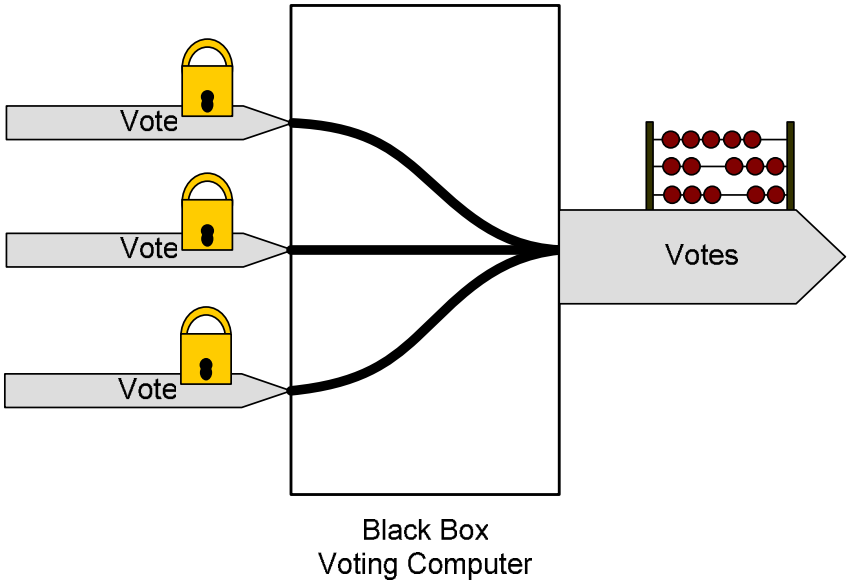
- Black box voting



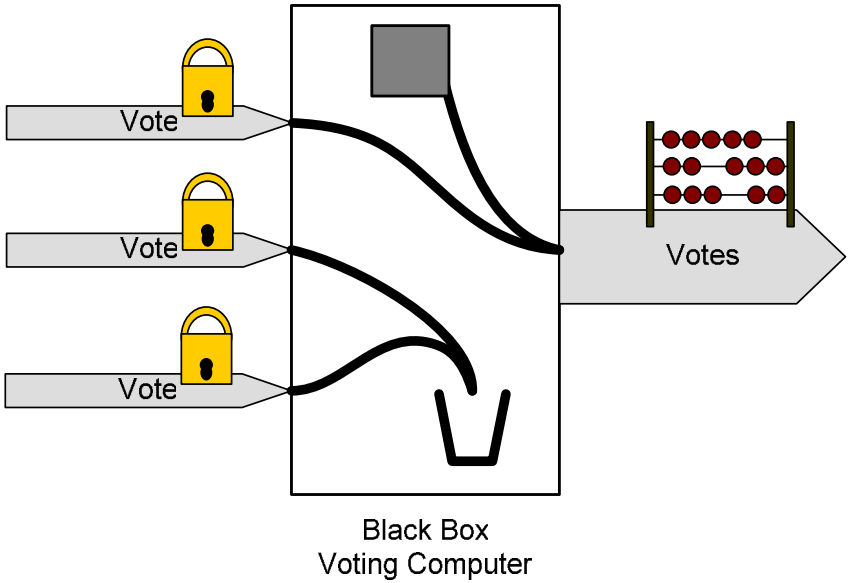
- Voting Computer is active device
- Output might be Input
- Processing not observable

Can you tell the difference?

- PowerVote



- PowerFraud

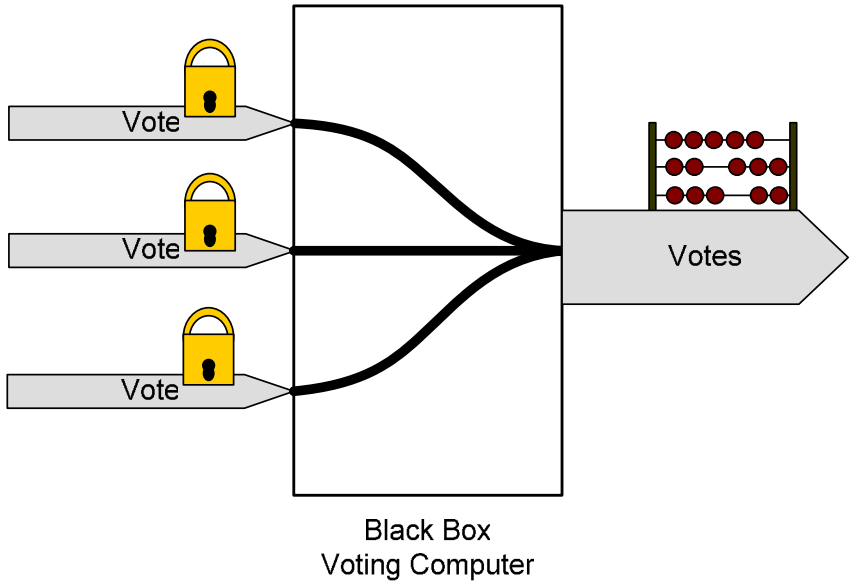


- Black Box voting computers might count correctly or might not
- Voters and observers are not able to decide if the election result is correct
- Trust in voting machine vendors and operators is required

Who can we trust?

Hypothesis:

- Every electronic voting system violates at least one of the three procedural election principles: Secrecy, Transparency, Verifiability



- Every electronic voting system requires trust into vendor and operators
- Trust is inappropriate measure to ensure election integrity

Have elections been tampered?

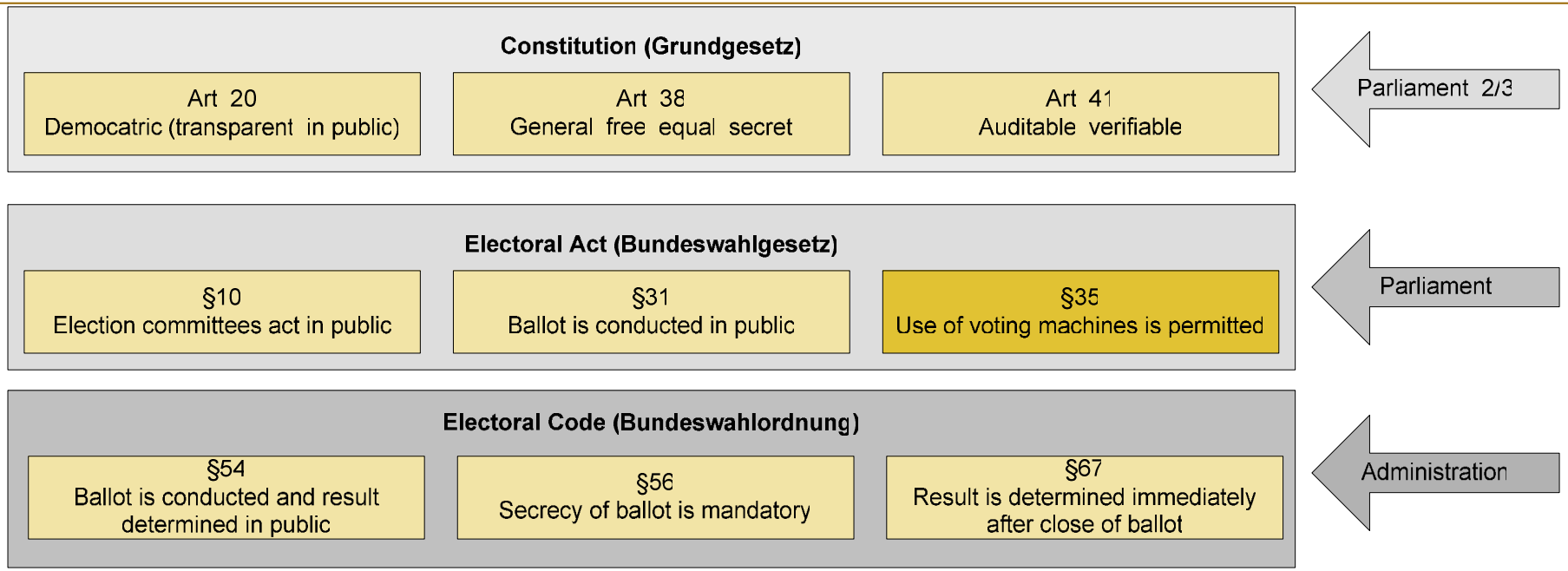
- Paper based elections can be tampered as well
  - But tampering of paper based elections requires decentralised actions and large number of participators
  - As election process is transparent, tampering needs to occur in public
  - Unlikely to remain secret
- There is no evidence that e-Voting (in Europe) has been tampered
  - But (other than for paper based elections) there is also no evidence that no tampering occurred
- E-Voting allows centralised, automated and large-scale tampering of elections
  - Even if voting computers are not linked, they could all run the same, fraudulent software
  - Only very few people need to be involved in a manipulation
  - Manipulative action can be de-coupled from the election itself

Hacking the Electoral Law

Hacking

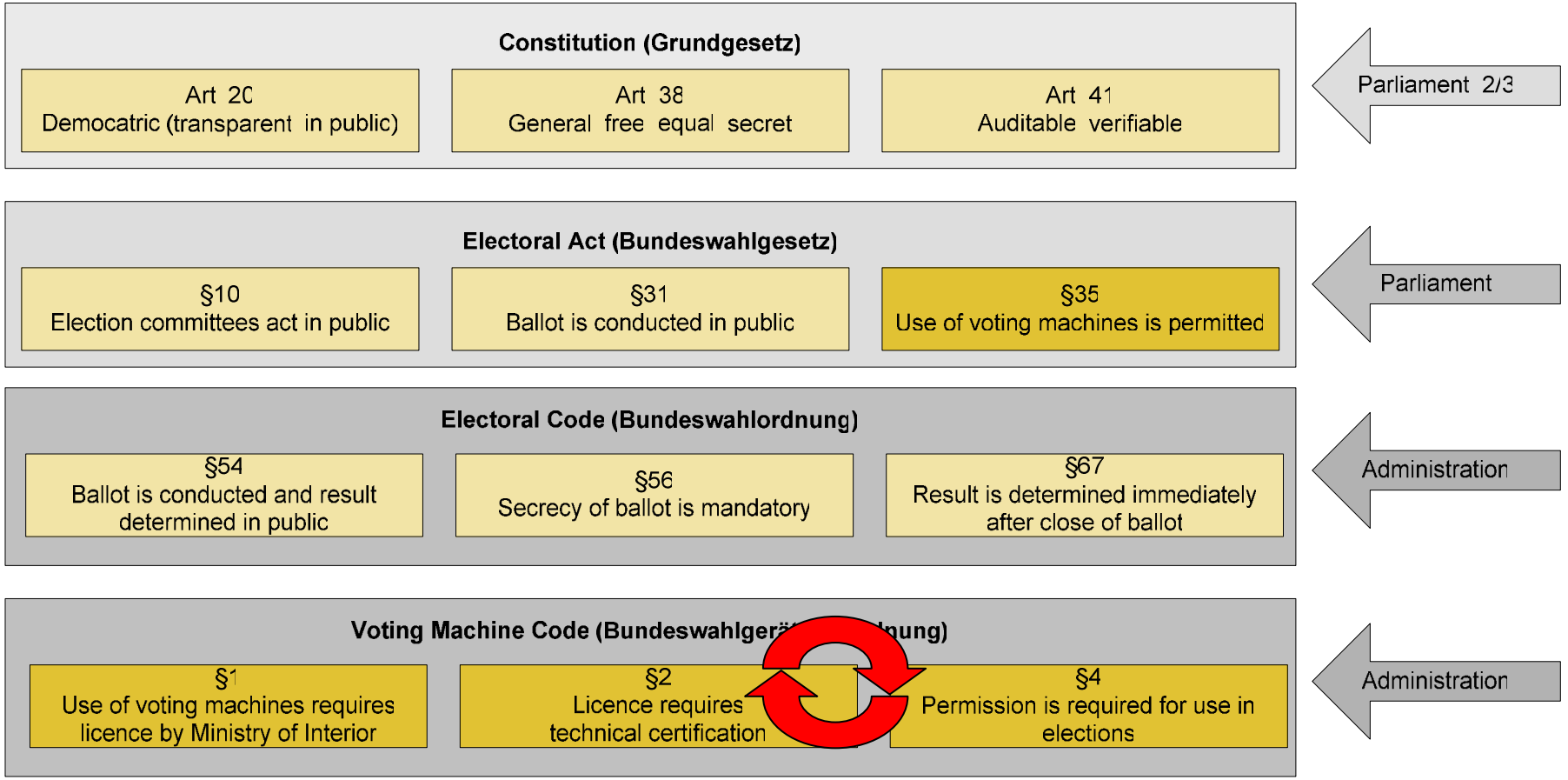
- Use of black box voting computers is not compliant with fundamental election principles: Transparency and Verifiability
  - Paper based elections
    - Allow everybody to verify election integrity
    - Very robust against tampering
  - Black box voting
    - Prevents everybody from verifying election integrity
    - Allow large scale manipulations by insiders
- How can this be legal?

Elections and transparency



- Law is explicit on election and determination of result being conducted in public

E-Voting and transparency



- But e-Voting regulations do not repeat transparency

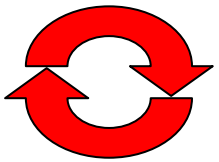
2005 Election Scrutiny

- Bundestag election, September 19th, 2005
- Four e-Voting related complaints filed with scrutiny committee of the parliament
- Federal Ministry of the Interior replied in May 2006
  - Input from Federal Physical Technical Agency and Federal Election Officer
- Bundestag rejected complaints on December 14th, 2006
  - Mainly follows arguments of Ministry of the Interior
  - No evidence of tampering, threads are hypothetical

- But
  - We know the official arguments now
  - We can escalate the complaint to the constitutional court

Arguments are self-referential

- The Nedap voting machines used in the 2005 election fulfil the legal requirements.
- §35 of the electoral act permits the use of voting computers
- The approval process for voting machines has been followed.



It is legal because it is legal?

- BT-Drucksache 16/3600

So entsprechen die bei der Bundestagswahl 2005 eingesetzten Wahlgeräte der Firma NEDAP den gesetzlichen Vorgaben. § 35 BWG regelt i. V. m. der BWahlGV, die das Bundesministerium des Innern im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie auf der Grundlage von § 35 Abs. 3 BWG erlassen hat (VO vom 3. September 1975, BGBl. I S. 2459 mit späteren Änderungen, vgl. dazu Schreiber, a. a. O., S. 824), die Voraussetzungen und das Verfahren der Stimmabgabe mit Wahlgeräten. Somit können anstelle von Stimmzetteln und Urnen bei einer Wahl auch mechanisch oder elektrisch betriebene einschließlich rechnergesteuerter Geräte eingesetzt werden (§ 1 BWahlGV).

Das in § 35 BWG vorgeschriebene Verfahren und die Zuständigkeiten beim Einsatz von Wahlgeräten der Firma NEDAP sind bei der Wahl zum 16. Deutschen Bundestag eingehalten worden. Die gemäß § 35 Abs. 2 Satz 2 BWG erforderliche Bauartzulassung wurde erteilt und im Bundesanzeiger bekannt gegeben. Die Verwendungsgenehmigung gemäß Absatz 2 Satz 4 und 5 liegt ebenfalls vor.

Bundestag: Transparency

- The voting computers are used in public:
  - Public access to the polling place is ensured
  - There are no legal restrictions to transparency
- After the election, the print out of the results is observable
- As the number of cast votes in the election register needs to match the sum of valid and invalid votes of the election result, it can be validated if the voting machine captured and added all votes correctly.

It is transparent because you can be present?

§ 5 BWahlGV verweist auf die Anwendbarkeit der BWO. Somit gilt auch bei der Wahl mit Wahlgeräten, dass die Verhandlungen, Beratungen, Abstimmungen und Entscheidungen der Wahlausschüsse und -vorstände für Jedermann zugänglich sind. Damit findet der gesamte Willensbildungs- und Entscheidungsprozess, der zu der Feststellung des Ergebnisses für den Wahlbezirk führt, im Lichte der Öffentlichkeit statt. Auch der öffentliche Zugang zum Wahlraum ist bei der Wahl mit Wahlgeräten gewährleistet. Schließlich finden, unter Beachtung des Grundsatzes der Geheimheit der Wahl, auch die Wahlhandlung (§ 54 BWO) sowie die Stimmauszählung (§ 67 ff. BWO) beim Einsatz von Wahlgeräten öffentlich statt. Es existiert daher keine rechtliche Beschränkung der Öffentlichkeit bei der Wahl mit Wahlgeräten.

Die Öffentlichkeit kann auch den Ausdruck des vom Wahlgerät errechneten Ergebnisses des Wahlbezirks nach Beendigung der Wahlhandlung sowie die Übernahme des Ergebnisses in die Wahlniederschrift und damit die Auszählung insgesamt kontrollieren. Durch den von § 14 BWahlGV vorgeschriebenen Abgleich der Stimmabgabevermerke im Wählerverzeichnis mit den vom Gerät registrierten gültigen und ungültigen Erst- und Zweitstimmen kann auch kontrolliert werden, ob das Wahlgerät alle Stimmabgaben erfasst und korrekt addiert hat. Zudem können alle gespeicherten Stimmen als Stimmzettel mit den entsprechenden Kreuzen ausgedruckt und von Hand nachgezählt werden.

Bundestag: Transparency

- Votes are cast in context of competing principles of ballot secrecy and election transparency
- It is acceptable that not each step of the vote registration is transparent to everybody
- It is a feature of today's increased use of technology that the correctness of systems can be assumed if they have been tested in a specific procedure

  But this is not appropriate in elections

In der Rechtswirklichkeit steht die konkrete Wahlhandlung der Stimmabgabe beim Einsatz von Wahlgeräten somit im Spannungsfeld des Prinzips der geheimen Wahl und des Öffentlichkeitsgrundsatzes. Vor diesem Hintergrund ist es hinnehmbar, dass beim Einsatz rechnergesteuerter Wahlgeräte nicht jeder Teilakt des Stimmenregistrierungsverfahrens für Jedermann transparent ist. Es gehört zu den Besonderheiten der fortschreitenden Technisierung, dass von der Funktionsfähigkeit der eingesetzten Systeme ausgegangen wird, wenn sie vor ihrem Einsatz in einem speziellen Verfahren geprüft worden ist. Dies gilt umso mehr, als in allen anderen Verfahrensschritten die erforderliche Kontrolle stattfindet und dadurch die erlangten Ergebnisse auf ihre Plausibilität überprüft werden können.

Bundestag: Device Security

- Exchange of software can not impact election result:
  - Before the device is configured for the election, it is unknown which party / candidate is on which button
  - After configuration, the device is sealed
  - Access to the source code of the software is required for manipulation
- *Post Nedap Hack argument!*
- *Even wrong from non-technical view: sequence of parties is regulated by electoral act*

Das BMI hat festgestellt, dass Manipulationen zwar theoretisch möglich, in der Praxis aber kaum vorstellbar sind. Solange sie sich allein auf die Eproms beschränken, wäre eine gezielte Beeinflussung des Wahlaktes nicht möglich, da bis einige Wochen vor der Wahl aufgrund der sich von Wahl zu Wahl ändernden Tastenbelegung nicht bekannt ist, welcher Kandidat mit welcher Taste gewählt wird. In diesem Fall ist also nur eine Sabotage des Wahlaktes möglich, nicht dagegen eine gezielte Manipulation zugunsten eines bestimmten Kandidaten. Eine Manipulation der Software setzt voraus, dass der Täter auf den Quellcode des Softwareprogramms oder auf die gefüllten Speichermodule Zugriff hätte. Da der Quellcode ebenso wie Speichermodule nach ihrer Komplettierung und Versiegelung gesichert aufbewahrt werden, ist die Manipulation in dem gleichen Maße möglich oder unmöglich wie bei den von der Gemeindebehörde aufbewahrten Stimmzetteln bei der Urnenwahl. Jedenfalls aber würde ein unbefugter Zugriff aufgrund der erbrochenen Siegel und der nach der Inbetriebnahme des Gerätes erscheinenden Fehlermeldung nicht unbemerkt bleiben.

Bundestag: Election integrity

- Manipulations by the vendor are possible in theory but
- Contractual and written agreements prevent vendor from doing so.

So why not outsource the entire election to someone who agrees not to tamper?

Theoretisch sind zwar auch Manipulationen möglich, die direkt beim Hersteller vorgenommen werden. Neben den vertraglichen Vereinbarungen und der entsprechenden schriftlichen Versicherung der Firma NEDAP bietet aber auch das eingeführte Audit eine hohe Gewähr für einen Schutz vor internen Eingriffen.

Bundestag: Risk Assessment

- Replacement of Software is only theoretical thread
  - Extremely unlikely even if only 2 minutes are required
  - During election, voting machines is placed in public and next to election officials
  - During election, nobody can spend 2 minutes with a screwdriver at the back of the voting machine

Ein dazu erforderlicher Austausch der Software während der Wahl erscheint, auch wenn er „innerhalb von zwei Minuten“ vorzunehmen sein sollte, extrem unwahrscheinlich, da der Wahlvorstand sich in geringer Entfernung zu den Wahlgeräten befindet und das Gerät in einem öffentlich zugänglichen und von Wählerinnen und Wählern besuchten Raum steht. Zudem befindet sich die Software, wie der Einspruchsführer selbst mitteilt, hinter einer durch Schrauben gesicherten und mit zwei Siegeln versehenen Abdeckung. Manipulationen, so sie denn theoretisch vorkommen können, würde der Wahlvorstand mit an Sicherheit grenzender Wahrscheinlichkeit bemerken. Es ist also davon auszugehen, dass niemand mit einem Schraubendreher zwei Minuten an der Rückseite eines Wahlgerätes unbemerkt manipulieren könnte.

- Scenario comparable and similar unrealistic as ballot box stuffing by voters
- Thread is manipulation by insiders
- Transparency is countermeasure, but is disabled


Hamburg's Digital Pen

Digital Pen

- Introduction driven by new complex local electoral system
- Traditional paper ballots are marked with a digital pen
- Paper is marked with dot pattern
  - Allows pen to recognise coordinates where paper is marked
- Paper ballot is put in to ballot box
- Digital ballot is unloaded at docking station
- At end of election day, digital ballots are counted
  - Ambiguous votes are presented to election officials for manual classification
- Paper ballots are not counted, but provide physical audit trail and can be counted in doubt

Solution to all challenges?

- Digital vote will be binding
- No counting of paper ballots
  - 1.5% sample in first election only
- No right to request recount for voters
  - Argument will be: no evidence that tampering occurred
- Digital Pen is black box voting system
  - Just the user interface is different
  - It provides a paper trail
- Just another optical scanning system
  - But scanning can not be repeated
  - No automatic recount with other device
  - Threads of optical scanning systems are discussed in detail in the US

Digital Pen CC Protection Profile

- City of Hamburg prepared Common Criteria Protection Profile for Digital Pen
- Explicitly documents assumptions for safety concept

- It is assumed that the election committee is reliable and does not tamper with the digital pen. It is assumed that attempts to tamper can only occur in the polling booth.

- Es wird angenommen, dass der Wahlvorstand vertrauenswürdig ist und den EVG nicht absichtlich manipuliert. Generell wird angenommen, dass nur in der Wahlkabine ein Manipulationsversuch am EVG stattfinden kann, da hier die Wähler unbeobachtet sind.

Digital Pen CC Protection Profile

Assumptions

- **Personnel.** Administrator and election committee do not act careless or hostile. They follow instructions of the documentation for users and system administrators.

- **Malicious Software.** The system administrator ensures that the IT-environment is free of malicious software (viruses, etc.) He checks the IT-environment before installation of the digital pen with appropriate tools (e.g. anti-virus software)

Digital Pen is secure by assumption

Annahmen

- **A.Personal** Adminstrator und Wahlvorstand handeln nicht sorglos, nachlässig oder feindselig. Sie beachten und befolgen die von der Benutzer- und Systemverwalterdoku-mentation zur Verfügung gestellten Anweisungen.

- **A.Schadsoftware** Der Administrator sorgt dafür, dass die IT-Umgebung keine Schadsoftware (Viren etc.) enthält, die den EVG beeinflusst. Hierzu überprüft er die IT-Umgebung vor der Installation des EVG mit geeigneten Werkzeugen (Antivirensoftware etc.).


E-Counting

E-Counting

- Traditional voting with paper ballots
- Votes are manually entered into PC or captured with bar code scanner
- Capturing of votes is observable, but counting is not
- Italian E-Counting experiments got significant international attention in early December 2006
  - Evidence for tampering in 2006 parliamentary elections
  - Demonstrates risks
  - Italy committed to stay away from e-Counting in future
- In Germany, driven by more and more complex election systems for regional elections
  - Hessen: One vote for each seat in the corresponding institution
    - More than 70 votes to spend (and count) per voter in Frankfurt
    - Up to 3 votes per candidate, votes across multiple parties

Example: Hessen

Hessian Regional Electoral Act

- After the election, the election committee determine the result by count the votes in public

- Typical interpretation of similar paragraph on federal state level:
  - After the election, the election committee determine the result of the polling station without interruption

Hessisches Kommunalwahlgesetz

§20 (1) Nach Beendigung der Wahlhandlung ermitteln die Wahlvorstände öffentlich das Wahlergebnis im Wahlbezirk durch Zählen der Stimmen.

Landtagswahlordnung §58

Im Anschluß an die Wahlhandlung ermittelt der Wahlvorstand ohne Unterbrechung das Wahlergebnis im Wahlbezirk

Example: Hessen

Hessian Regional Electoral Act

- The election committee can decide to postpone counting
- The votes can be counted in an automated procedure, if the security and reliability of the determination of the election result is ensured.

Count when, where and how you want

Hessische Kommunalwahlordnung

- (7) Der Wahlvorstand kann beschließen, dass die Stimmermittlung vertagt wird;
- (8) Die Stimmermittlung kann auch mit automatisierten Verfahren erfolgen, wenn dabei Sicherheit und Zuverlässigkeit bei der Ermittlung und Feststellung des Wahlergebnisses gewährleistet sind


Where are we?

…and what's next?

Legal Action - Germany

- Contested National Elections
  - Bundestag rejected case on 14/12/2006 based on recommendation of Scrutiny Committee
    - “obviously unsubstantiated “ (offensichtlich unbegründet)

- Next step is Constitutional Court
  - To be filed by 14/02/2007
  - Three of four contestants want to go to the next round
  - **Minimum of 100 signatures required for formal acceptance**
  - More signatures would provide evidence for public interest

  - You need to be German and have the right to vote
  - **Please sign today**
    or look for additional details at ulrichwiesner.de

Procurement - Germany

- Nedap
  - Evidence that purchasing municipalities have never heard of legal and technical challenges
  - Local elections with complicated election systems drive acquisition
    - 300 machines used in Hessen 2006 regional election compared to 100 in national election 2005
  - Recent discussions:
    - Cottbus – Previously used rented machines, now revisiting decision to purchase
    - Hemer, Westfalen – waiting election schedule, will only buy if local and European elections take place on same day
    - Bad Oeynhausen - borrowing machines for local election in 2007
- Digital Pen
  - No permission for national elections (yet)
  - Bremen about to change electoral act for local elections
  - Digital pen might follow

Upcoming Elections

- Germany
  - No major computer based elections in 2007
  - Spring 2008 – Hessen and Nordrhein-Westfalen (Nedap)
  - Spring 2008 – Hamburg (Digital Pen)
  - Autum 2009 – Bundestag (Nedap)
- Europe
  - Spring 2007 – Ireland (100% Nedap, suspended)
  - June 2007 – Belgium (40%)
  - June 2007 – France (5%)
- European Parliament
  - Spring 2009 – Irish Government committed to use Nedap

To does

- Penetration is still relatively low
  - But municipalities busy buying and US vendors at the doorstep
- Raise awareness
  - Many Politicians and Journalists still unaware of e-Voting and related issues
  - Vendors still gets away with aim to provide the modern approach to elections
  - Discussion needs to leave the IT corner
- Procurement is local process
  - Make sure your municipality understands the issues
- Tell your Member of Parliament that you insist in election transparency
- Do we need a campaign? Should it be European? National?
  Can existing organisations pick up?
- Regional electoral systems require review
  - Systems need to be efficient enough to enable choice at reasonable counting effort

Who can we trust?

- Public control – not trust – implements the integrity of the election
- Trust in election officials (or vendors) is desirable, but not an appropriate approach to ensure democratic elections.
- Trust in election officials might be appropriate in most cases
- Trust as main measure to ensure election integrity is not appropriate.


Questions and Answers

http://ulrichwiesner.de