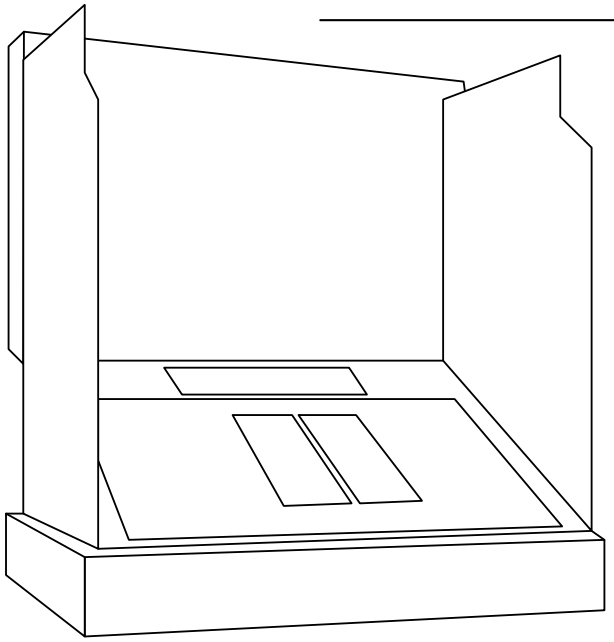
e-Voting

Silent decline of public control



22nd Chaos Communication Congress

Berlin, 29/12/2005

Ulrich Wiesner

Agenda

- Nedap Voting Computers
  - High level functional and technical overview
- Voting Machines in Germany
  - History, relevance, recent elections
- Prerequisites for Democratic Elections
  - Conceptual requirements
  - Constitutional, legal and regulatory requirements
- The Irish Report
  - Background, Findings, Concerns, Security Issues
- Conclusions

Terminology

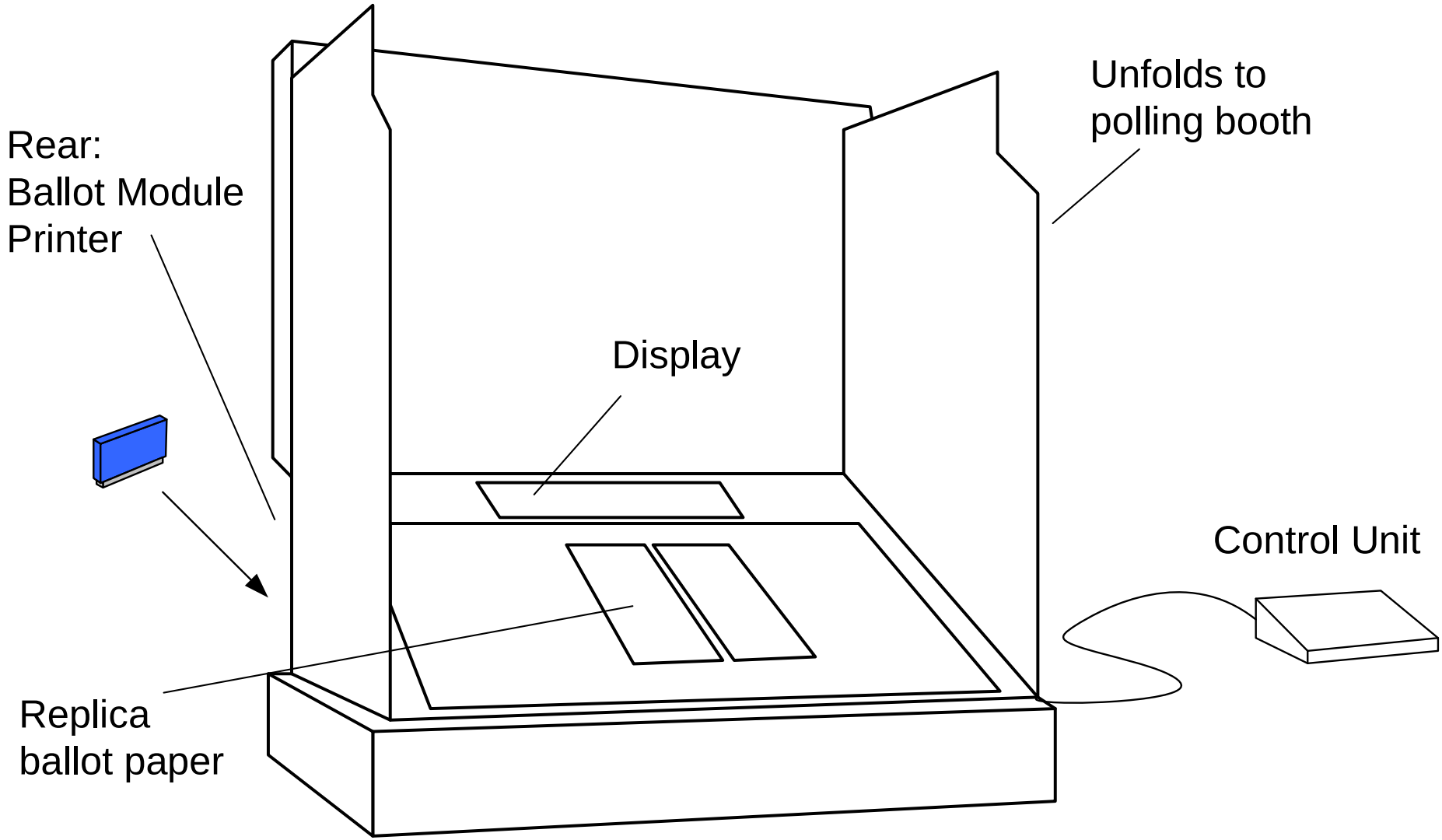
- e-Voting
  - Electronic Voting
  - Offline, in election office
  - using public equipment only

- i-Voting
  - Internet Voting
  - Online, in election office or elsewhere
  - Using public or private equipment on user side
  - (Not subject of this talk)

Nedap Voting Computers

High level technical and functional overview

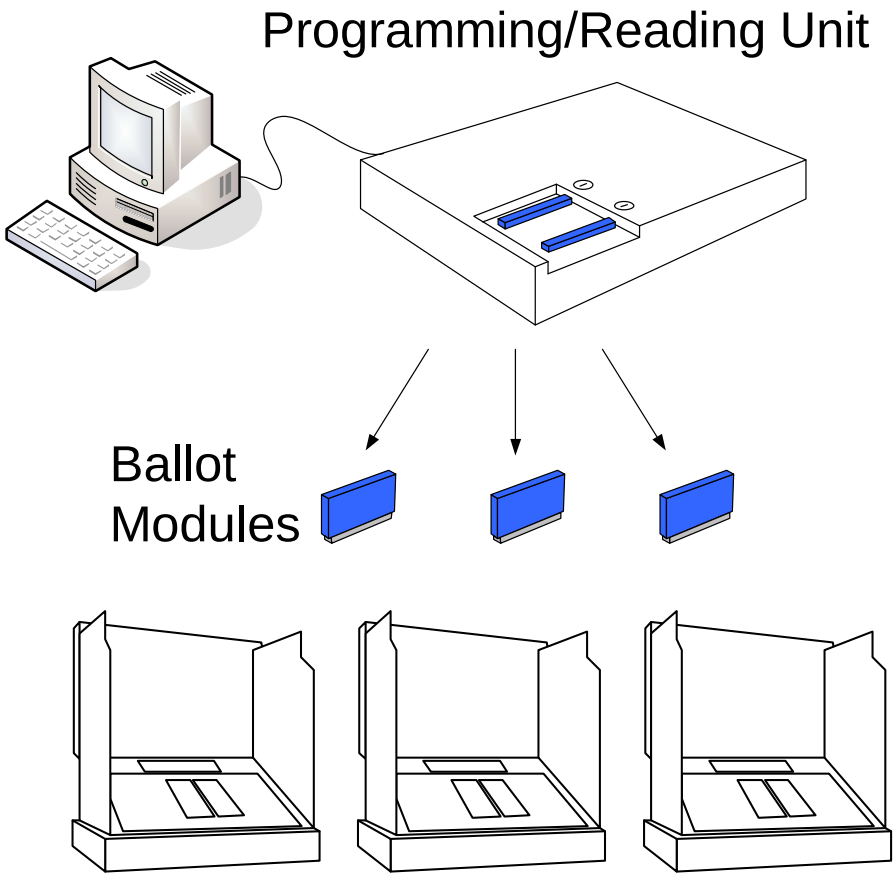
Nedap Voting Machines



Pre Election: Set-up

At central election offices:

- Define Election details using Integrated Election Software on PC connected to Programming/Reading Unit
- Copy election details on each Ballot Module using Programming/ Reading Unit
- Insert configured Ballot Modules into voting machine
- Print replica ballot paper (Stimmzettel) and place on front pannel of voting machine



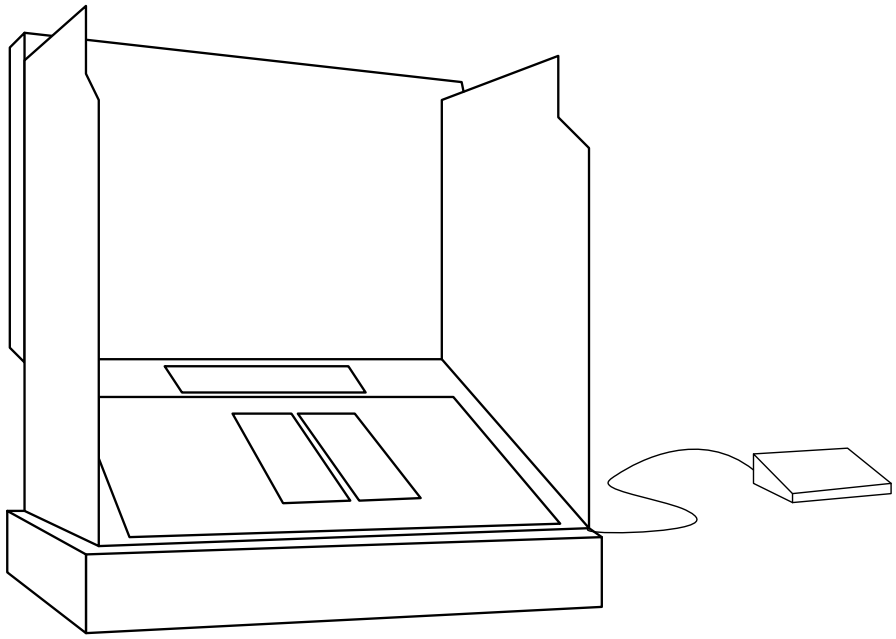
Election

At polling station:

- A polling clerk activates the voting machine for each voter via control unit
- Voter cast their votes, which are automatically recorded on ballot module

At end of polling:

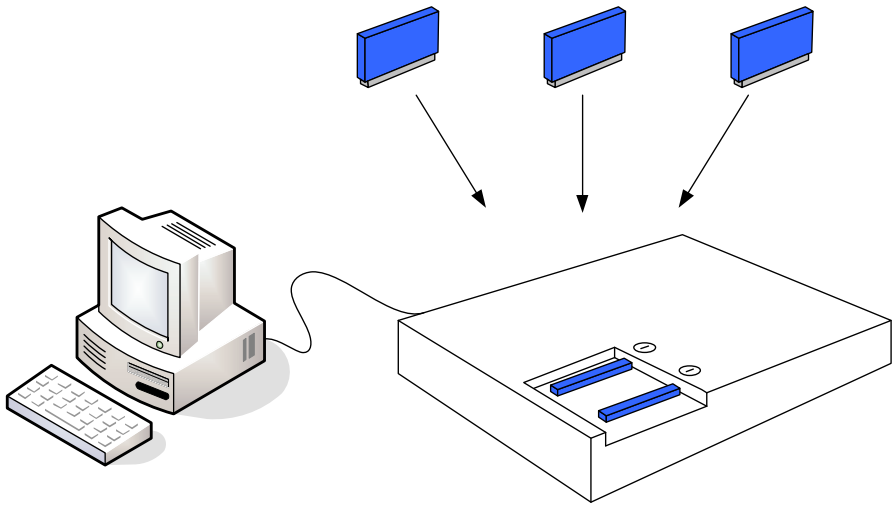
- backup copy of ballot module is made
- Election results are printed and documented
- Ballot module is removed, sealed & sent to voting centre



Post election: vote counting

At central election offices:

- Ballot Modules are inserted into Programming/Reading Unit
- Votes are loaded into attached PC using Integrated Election Software
- Votes are counted and results are printed/published by Integrated Election Software



Technology

- Voting Machine and Programming/Reading Unit
  - Motorola M68000 processor
  - Software on two EPROM 27C512 (socketed)
  - Controlling Software is written in C
- Ballot Module
  - Two Flash-EEPROM 28F512
  - Proprietary connector
  - Votes stored unencrypted, but redundant (2x on each EEPROM)
- Integrated Election Software
  - Running on hardened Windows PC, MS-Access database

Voting Machines in Germany

History, relevance, recent elections

Voting Machines in Germany

- 1960's
  - Counting machines allowed by law
  - Very rarely used
- 1975
  - Regulations now talk of voting machines.
  - Physikalisch-Technische Bundesanstalt (PTB) responsible for certification
- 1999
  - New Regulation on voting machines explicitly refers to microprocessor controlled devices
  - Nedap Computers tested by PTB and appointed by BMI
  - Nedap Computers used by City of Cologne in European elections
- 2002 Election of Bundestag
  - Nedap Computers used by several cities and 1+ Million voters
- 2005 Election of Bundestag
  - 2+ Million voters use Nedap machines

Certification and procurement

- Vendors apply for a certification of their machines
- Physikalisch-Technische Bundesanstalt (PTB) checks one specimen and certifies on vendor's costs. Results and technical details remain confidential.
- Minister of the Interior approves certification
- Purchase decision (if and what) is with municipalities
- Minister of the Interior approves usage individually for each election
- Vendor guarantees that delivered machines are equivalent to tested specimen

Motivation to use machines

- Typical reason to switch from ballots to machines:
  - Difficult to find sufficient number of volunteers for elections
  - Significant reduction of staff in election office
  - Vendors claim cost benefits
  - Vendors claim high reliability and user acceptance
  - Fewer invalid votes by avoiding ambiguous selections

- Drivers are local not federal elections
  - Complex voting systems (vote splitting, vote cumulation)
  - high counting effort – high costs

Where is the issue?

- I frequently use cash machines – why should I distrust a certified voting machine?

- When using a cash machine
  - you can instantly verify the amount you receive
  - You can “audit” the amount debited in your account statement

- A voting machine
  - Does not necessarily allow you to verify the vote is counted
  - Does not necessarily allow the results to be audited

How do you vote?

- Vote generation
  - Traditional: Marking your vote with a pencil
  - e-Vote: Selecting the vote on a user interface
- Vote casting
  - Traditional: Putting the vote into the ballot
  - e-Vote: Submit your selection / relinquish control over vote
- Vote recording
  - Traditional: Storing the vote within the ballot
  - e-Vote: Recording the vote in a storage device
- Vote counting
  - Traditional: Counting votes manually
  - e-Vote: Return counted values

Prerequisites for Democratic Elections

Conceptual and legal requirements

Principals of Democratic Elections

- General — No groups are excluded from right to vote
- Free — Ability to cast a vote without pressure
- Secret — Implements free vote
- Equal — All votes count in the same way
- Democratic — The votes are honestly counted as cast

Implemented through / enforced by

- Public control of the election process
- Feasibility of election audits (Wahlprüfung)

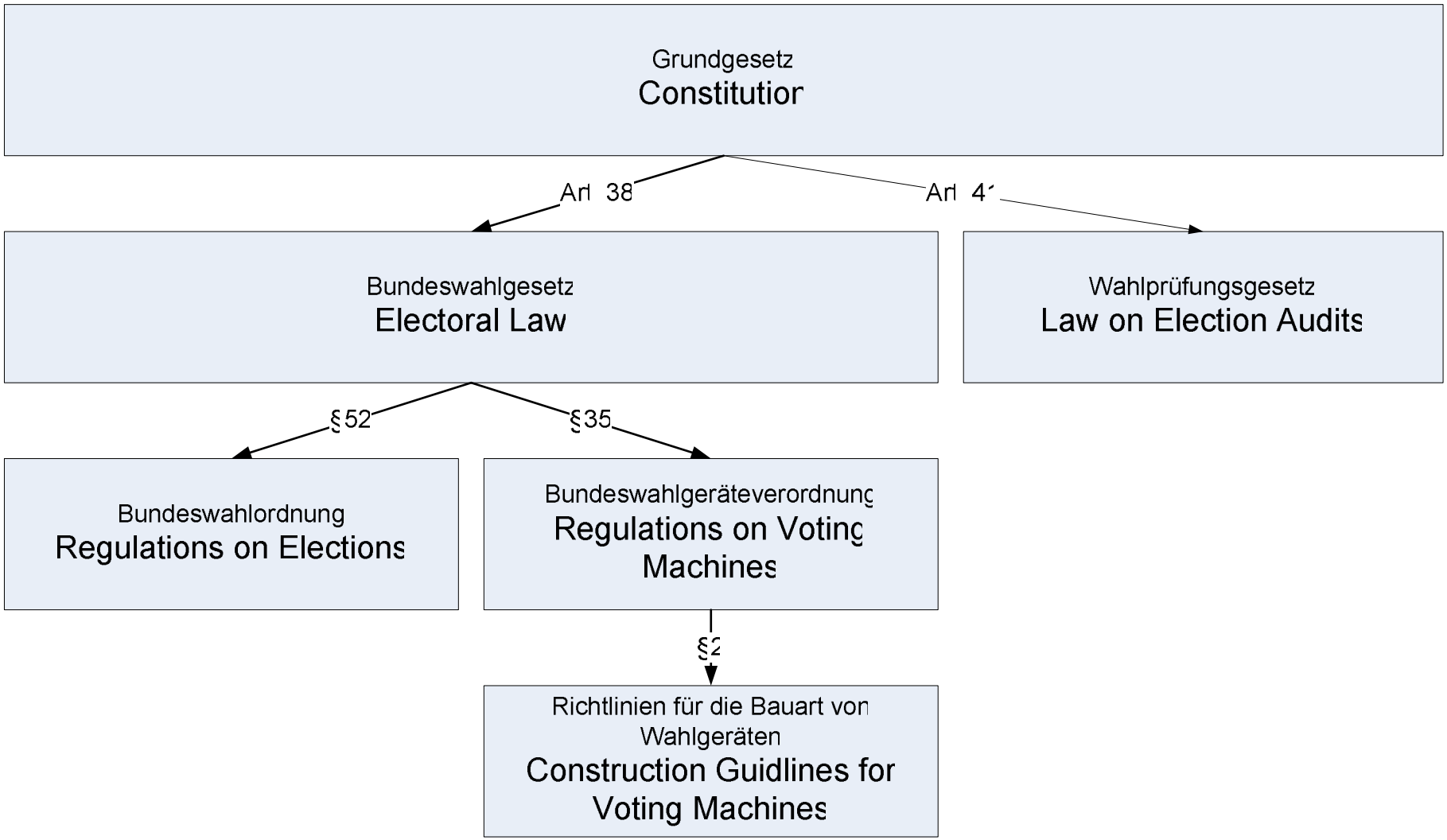
OSCE Requirements

- Copenhagen, 1990 (election-specific commitments)
  - ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public;
  - presence of observers, both foreign and domestic, is invited.

OSCE Office for Democratic Institutions and Human Rights (Ed.):

Election Observation Handbook, 5.Ed., Warsaw (2005)

German Legal Framework



German Legal Framework

- Constitution
  - Art. 20 Democratic federal republic
    The public is highest sovereign
    implicitly: public control of election process
  - Art. 38 Elections of the Parliament
    general, direct, free, equal, confidential
  - Art. 41 Election Audits
    Responsibility of Parliament, then Constitutional Court

- Electoral Law (Bundeswahlgesetz)
  - §10 Public status of all voting committee's work
  - §31 Public status of the voting process
  - §35 Vote casting with voting machines

German Legal Framework

- Regulations on Voting Machines
  - §§1-3 Voting Machines are subject to certification process and technical audit by PTB

- Construction Guidelines for Voting Machines
  - Sect. A Definitions
  - Sect. B Requirements
    - §1 Unambiguous identification of hardware and software version Source code subject to PTB audit
    - §2.1 State of the art technology, appropriate for critical application, prevention of undetected h/w & s/w manipulations
    - §2.2ff Physical and technical stability
    - §3 Functional requirements

The Irish Report

Background, Findings, Issues

Background

- Republic of Ireland has chosen Powervote/Nedap as vendor for voting machines in 2003 (?)
- Public debate resulted in government establishing a commission on the "*Secrecy, Accuracy and Testing of the Chosen Electronic Voting System"* in 03/2004
- Final Report published 12/2004

- As PTB reports are unpublished, Irish report is primary source of information

Commission's Conclusion

- *"not in a position to recommend with the requisite degree of confidence the use of the chosen system"*

- *"not based on any finding that the system will not work,*
- *but on the finding that it has not been proven that it will work."*

First Report of the Commission on Electronic Voting, p. 12

Feasibility of Audit

- *“The NEDAP system does not provide a full audit trail; […]*
- *There is no post facto method of validating that the votes stored in the data cartridge are the same as those entered at the keyboard by the voters”*

First Report of the Commission on Electronic Voting, p. 363

Audit trail is feasible

Several concepts have been suggested / implemented, e.g.

- Paper trail
  - Allows voter to verify his vote
  - Paper trail allows re-count
- Printer/Scanner
  - Voter generates machine readable ballot paper
  - Voter puts ballot paper into ballot box
  - Votes are counted by second device / scanner
  - Ballot papers are available for re-count
- Card Writer/Reader
  - First device (Writer) stores vote on chip card
  - Second device (Reader) allows voter to verify selection
  - Chip cards are stored for physical evidence and recount

Software authentication

- At startup, machine displays/prints Software version and checksums for both EPROM
- Does not ensure integrity of installed software

- *“Someone with access to Nedap’s source code could alter the program while also ensuring that it returned the expected checksum at start-up.”*
- *“An exchange of the ROM chips including fraudulent presentation of the correct checksums cannot be avoided by software but by means of sealing only.”*

First Report of the Commission on Electronic Voting, p. 96

Software manipulation

- *“In practice it took a technician about 40 seconds to open the machine from the back. We observed that the controlling program chips are actually socketed for ease of access. Therefore there is little to prevent removal and substitution of the program […]. We estimate that 2 minutes of unauthorised access would be sufficient to switch programs.”*

  First Report of the Commission on Electronic Voting, p. 139

- *“The seals on the voting machine peeled back equally easily. Four Philips head screws had to be removed.”*

  First Report of the Commission on Electronic Voting, p. 189

Ballot Modules

- Votes stored unencrypted
- Standard components are used (EEPROM 28F512), specs available on Internet
- Main protection against tempering are proprietary connectors of ballot modules

Integrated Election System

- IES controls Programming/Reading Unit for set-up and vote counting
- Not subject to the certification process in Germany
- In Ireland, IES is running on “hardened” PCs

- Multiple versions of IES can be installed on same PC, older versions can be installed over newer ones
- Usage of hardened PC is not enforced

  First Report of the Commission on Electronic Voting, p. 56

- Irish report provides step by step guide to bypass protection measures (p. 151)

Security - Conclusions

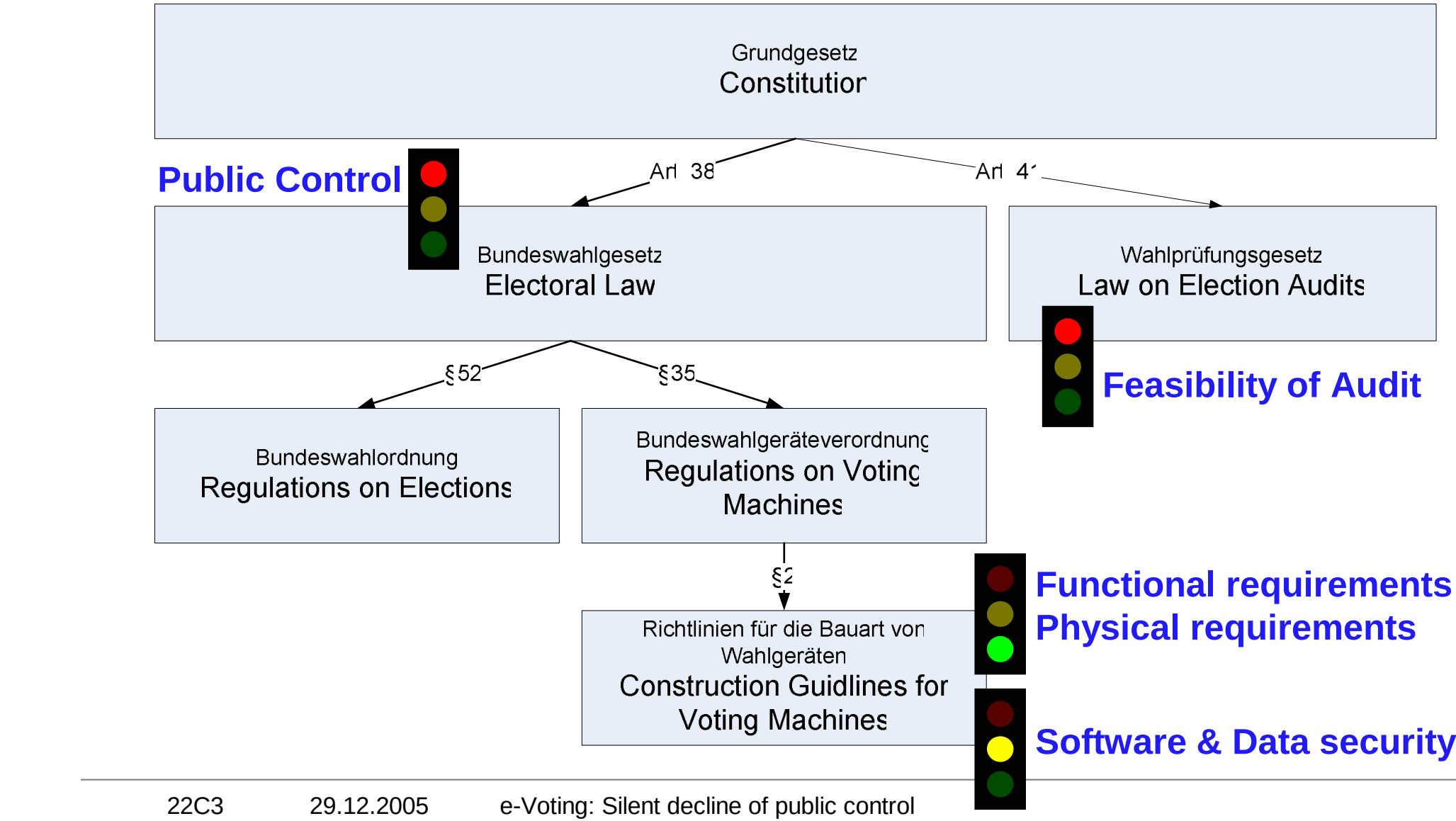
- *“The voting system is 1980’s technology. In the 1980’s the threats to this kind of technology were not as well understood as they are today; furthermore many effective defensive counter-measures have been perfected in the meantime (such as the use of cryptography) which are not deployed here. “*
- *“Security, such as it is, relies largely on the long discredited concept of ‘Security Through Obscurity’. It is a well-established principle in the world of electronic and computer security, that this is inadequate.”*

First Report of the Commission on Electronic Voting, p. 129

Checklist

Requirements met / not met by Nedap

German Legal Framework



Conclusions

- Voter’s control over his personal vote
  - Impossible to determine if vote is recorded correctly
- Public Control
  - Impossible to determine if installed software is certified one
  - Impossible to know if software counts correctly
  - Impossible to determine if votes have been stored as cast by the voters and have not been manipulated afterwards
- Feasibility of Audit:
  - Impossible to verify if election result is based on cast votes
- Technical requirements unlikely to be met
  - Security measures unlikely to be state of the art
  - Impossible to detect software manipulations

What is needed?

- Public control over voting process and feasibility of audit need to be ensured for voting machines
- Certification process for voting machines and test results needs to be transparent and results need to be published
- Installed software needs to be authenticated on every machine immediately before elections

- Absence of audit trail and intransparent certification process/results are unacceptable in a democracy

Next steps

…and how you can help

I need your support

- I have filed a complaint to the Bundestag, challenging the results of the recent elections where Nedap machines have been used
- If the parliament rejects the complaint, 100 supporting signatures are required to file a case at the constitutional court
- You need to be a voter in Germany (wahlberechtigt)
- If you consider to support me, please send an e-mail to

  wahlgeraete@yahoo.de

- Thank you!

References

Links and Literature

References

- *First Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System, Dublin, 15 December, 2004;*
  - *www.cev.ie/htm/report/first_report.htm*
- *California Institute of Technology and The Massachusetts Institute of Technology* (Ed.): Report of the Caltech/MIT Voting Technology Project: Voting - What Is, What Could Be (2001)
  - www.vote.caltech.edu/reports/2001report
- Legal Framework:
  - www.bundeswahlleiter.de/ bundestagswahl2005/informationen/rechtsgrundlagen.html
- *Martin Leder*: Der Einsatz von Wahlgeräten und seine Auswirkungen auf die Amtlichkeit und Öffentlichkeit der Wahl, Die Öffentliche Verwaltung, August 2002, S. 648-654
- *Wolfgang Schreiber*: Handbuch des Wahlrechts zum Deutschen Bundestag. Kommentar zum Bundeswahlgesetz, 7. Auflage, Köln (2002)
- *Ulrich Karpen:* Elektronische Wahlen? Einige Verfassungsrechtliche Fragen. Baden-Baden (2005)