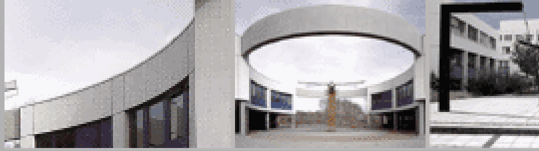
Deutsches Forschungszentrum für Künstliche Intelligenz



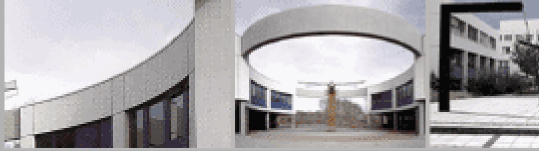
SiSo
Sichere Software

Requirements Engineering for eVoting

Roland Vogt and Melanie Volkamer

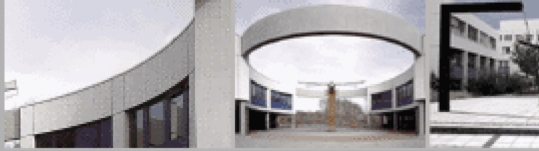
German Research Center for Artificial Intelligence (DFKI GmbH)
Saarbrücken, Germany

Overview



- Introduction
  - eVoting
  - Security requirements
- Why CC?
- Protection Profile for Online Voting
- Protection Profile for the Digital Election Pen
- Conclusion

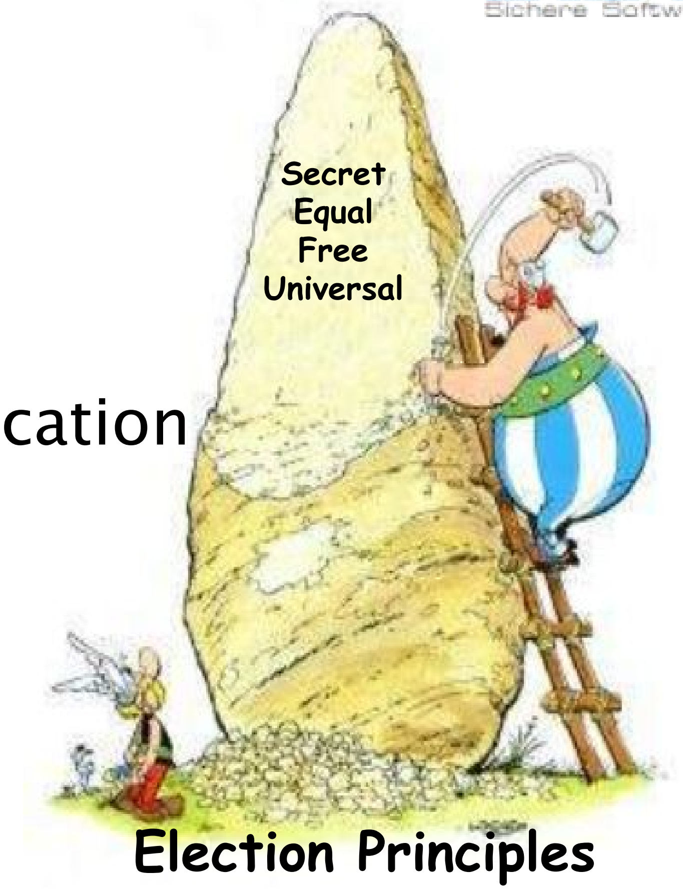
Introduction-eVoting



Environment Medium	Controlled	Uncontrolled	
Paper	Polling Place	Postal Voting	Counting Machines
Electronic	Stand-Alone Electronic Voting Machine	Remote Electronic Voting (PC, Cell Phone)	
	Stand-Alone Electronic Voting Machine		
	Networked Kiosk Electronic Voting		

Introduction-Security Requirements

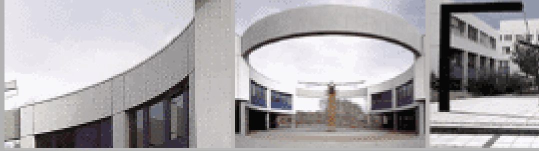
- Anonymity and unlikability
- Receipt freeness
- One-voter-one vote principle
  - Attention: system breakdowns
- Right to vote
  - Attention: system breakdowns
- Unique identification/authentication
- ….



Introduction–Existing Work

- Bundeswahlgeräteverordnung
- Recommendation of the Council of Europe
- Requirement Catalogue of the PTB / GI
- Cybervote Requirements Catalogue
- (Network) Voting System Standards
- Swiss Law
- IEEE Standard
- Safevote Voting System Requirements
- IN GENERAL: in each voting protocol paper
- …

Why a "new" Catalogue / CC?

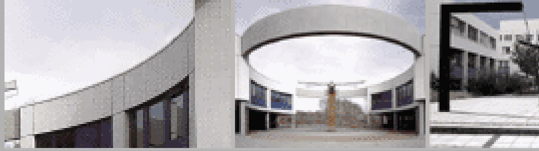


- Incomparable voting systems’ security
- Undetermined evaluation process
- Undetermined evaluation deepness
- Undetermined Evaluator and Certifying Institute
- Missing definition of the underlying Trust Model
  - Assumption to the environment
  - Intruder model
- International accepted certificate

Protection Profile for Online Voting

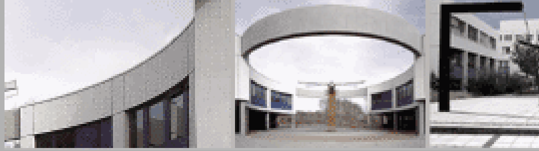
- For remote Online Voting
- Mainly for elections in associations (extendable)
- Sponsored by the Federal Office for Information Security
- Initiated by the Gesellschaft für Informatik e.V.
- Supported by a broad board (companies, universities, ministries,…)
- From December 2005 to September 2006
- Unfortunately currently in German

PP for Online Voting-Content



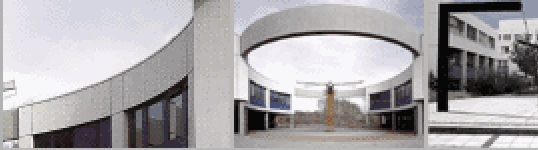
- Three phases: pre-/**main-**/post voting
- **Focus: systems which ensure unlinkability between voter and his (encrypted) vote at the end of the main voting phase**
- Open to any underlying voting scheme
- Open how many voting servers
- Basis requirements → “many” assumptions
  - Voter ensures the trustworthiness of his PC
  - Scrutineers ensure the trustworthiness of the voting server
  - …

PP for Online Voting-Discussions



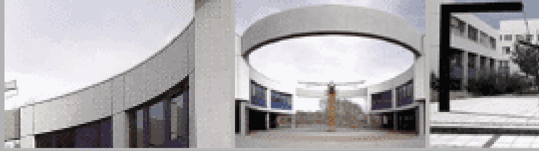
- Trustworthy client and voting server?
  - Handouts to the voter or special software
  - Administrator as part of the scrutineers
- EAL ? → security versus costs
- Additional verification necessary?
  - Code review e.g. of the counting procedure
  - ….

PP for the Digital Election Pen



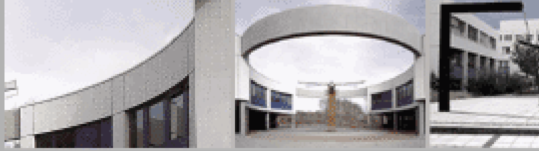
- For (local HH) parliamentary elections
- Sponsored by the Ministry of the Interior of HH
- Support complex election systems
- Simplification of complex counting mechanisms
- Provide a new form of election device
- Test election in 2005
- To integrate into the laws
- Bundeswahlgeräteverordnung does not fit
- Evaluation/certification in parallel
- End: August 2006

PP digital Election Pen –Discussions



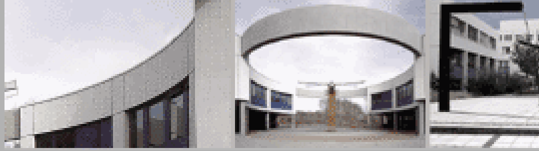
- ST/PP?
- Using standard devices like notebooks
- Ballot box part/outside the EVG
- Function tests ?
- Role of the administrator
- Number of docking stations
- As easy as possible for the scrutineers
- EAL 3
- …

Conclusion



- Two different PPs
  - Online Voting in associations
  - Digital Election Pen
- Some open problems BUT

  "E-Voting is an important field for Common Criteria"



Thank you for your Attention

Questions?

vogt@dfki.de