zda Zentrum für Demokratie Aarau

THE SWISS POST / SCYTL TRANSPARENCY EXERCISE

AND POSSIBLE IMPACT ON I-VOTING REGULATION

Ardita DRIZA MAURER
Legal researcher and independent consultant

E-Vote-ID 2019, Bregenz, Austria

Outline

- i-v transparency regulation
- PIT and source code publication
- Questions on:
  - Source code transparency
  - Verifiability
  - Certification
  - State of the art and good practice
  - Accountability
  - Costs
- What is our understanding of verifiability?

i-v transparency

i-v Regulation v. 1

2002/2003

1. Report 2002: test i-v feasibility

- Detailed regulation
- Peer control, authorities control, external audits
- Transparency is a cantonal matter

2. Report 2006: extend electorate

i-v Regulation v. 2

2013/2014

3. Report 2013: from «black box» to E2E verifiable systems

- Regulation reflecting state of the art
- Controls by independent and competent bodies
- Verifiability +plausibility
- Open source (July 2018)

i-v Regulation v. 3

2020/2021?

2017 Gvt. decides to put i-voting in regular operation

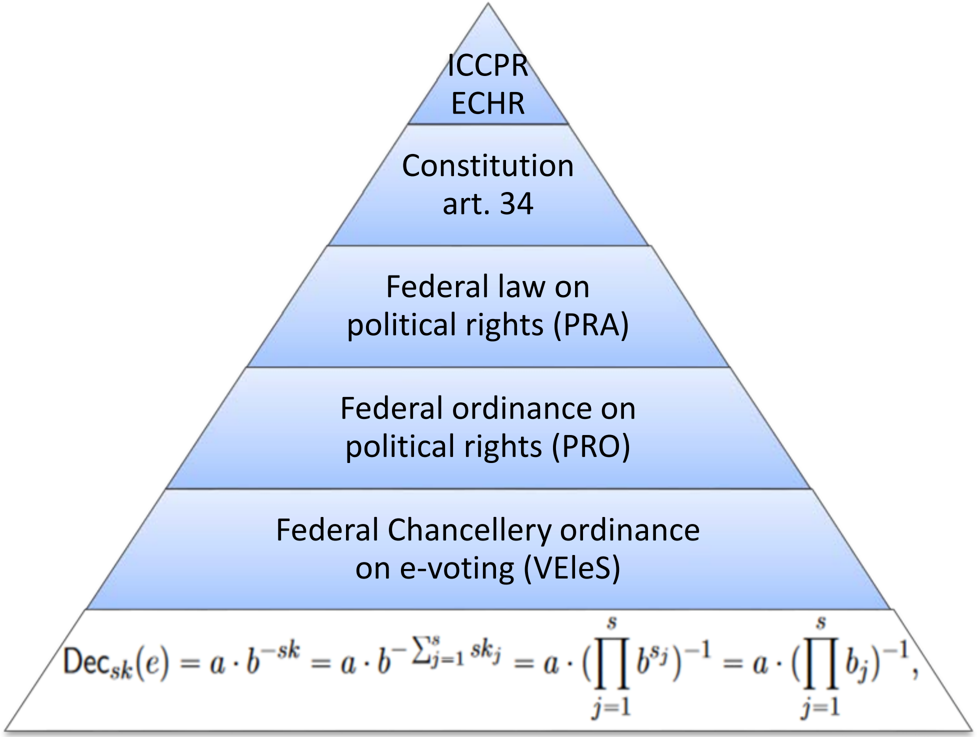
Revision of PRA (law)

- Consultation (Jan-Apr.'19)
- Conclusion: regular operation is premature

June 2019: Gvt. decides to prov. forgo regular operation + redesign trials

POPULAR INITIATIVE : MORATORIUM ON E-VOTING

i-v regulation’s structure



ICCPR
ECHR

Constitution
art. 34

Federal law on
political rights (PRA)

Federal ordinance on
political rights (PRO)

Federal Chancellery ordinance
on e-voting (VEleS)

$$\mathsf{Dec}_{sk}(e) = a \cdot b^{-sk} = a \cdot b^{-\sum_{j=1}^{s} sk_j} = a \cdot \Big(\prod_{j=1}^{s} b^{s_j}\Big)^{-1} = a \cdot \Big(\prod_{j=1}^{s} b_j\Big)^{-1},$$

CHVote System Specification
R. Haenni *et al.*, 2017

PIT and source code publication

- Decision to organize a PIT
  Fall 2018
- PIT duration
  25 Feb. – 24 Mar. 2019
- Bug bounty
- Some 3200 participants from +130 countries
- Accompanied and monitored by management committee
- 16 responses classified as breaches of best practice

- Requirement to publish the source code:
  July 2018
- Source code publication GitLab : 7 Feb. 2019
- Significant flaws affecting universal and individual verfiablity discovered and communicated by Lewis, Pereira, Teague.
- Other researchers discovered same issues
- Flaws apparent in the system specification document (BFH)
- Fed. Chancellery and Swiss Post took note and communicated after each published finding

Source code transparency

- Code published and made available upon registration + acceptance of terms of use including a 45 days silence period
- Findings were communicated on twitter in breach of the 45 day silence
- Small percentage of documents examined; not a full and systematic control of system’s security
- No bug bounty
- What is the justification of the 45 days silence period? Is it acceptable and in line with good practice? If not, what is a good practice?
- How to handle “leaks” if publication done in line with good practice?
- Source code publication with bug bounty?

Verifiability

- Universal verifiability flaw: built-in trapdoor allowing system operator or person with access to the system to modify any number of votes undetected
- Individual verifiability flaw: invalidate votes (without being detected)
- Control of E2E V and requirements thereof ?
- Discussion about trust assumptions (BFH)?

Certification

- Publication of the source code only after certification and other controls
- Critical vulnerabilities apparent in the system specification documentation. PIT and publication of source code played a secondary role (BFH)
- Fed. Chancellery to review certification and accreditation procedures
- Role of other controls ?

State of the art and good practice

- Requirements, systems, implementation should be state of the art
- Extremely complex structure of code and documents
- Who defines state of the art?
- Who checks?
- Is certification the right place for defining state of the art?
- What if partial implementation of state of the art?
- Legality vs state of the art

Accountability

- No e-voting on 19 May; no e-voting on federal elections of 20 Oct.
- May cantons sue the provider Post for not fulfilling its contractual obligation ?
- What are the responsibilities of the certification body and other controllers?
- What responsibilities for the State?

Costs

- Geneva system : end Nov. 2018 GE Gvt. said it would cease operating its system beginning 2020
- 19 June 2019: GE Gvt. and cantons working with GE decided to stop with immediate effect
- Friction between requirements for i-voting (federal level) and their implementation and financing (cantonal level)

What is our understanding of verifiability?

OPTIMUM SECURITY =

state of the art security measures

+ controls of compliance, certification

+ verifiability

+ source code transparency

If the control of the end-to-end verifiability solution and its implementation presents difficulties similar to those related to controlling the system itself, is end-to-end verifiability a good solution?