



Public verifiability challenges CC paradigm in the context of e-voting and beyond

Roland Vogt

DFKI GmbH
IT Security Evaluation Facility

Democracy, republic and rule of law

- Principle of sovereignty of the people:
People are the source of all political power.
- Political philosophy is based on essays of
Jean-Jacques Rousseau, 1762
- The election of representative bodies is
the main way of applying this principle.

Sovereignty of the people

“Alle Staatsgewalt geht vom Volke aus.
Sie wird vom Volke in Wahlen ... ausgeübt.“

German basic constitutional law, art. 20, par. 2

Public nature of elections

<http://www.bverfg.de/en/press/bvg09-019en.html>

German Federal Constitutional Court

Judgment of 3 March 2009:

- The German Federal Voting Machines Ordinance is unconstitutional because it does not ensure that ...
- ... only such voting machines are permitted and used which meet the constitutional requirements of the principle of the public nature of elections.

Public nature of elections

All essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception.

Public nature of elections (cont.)

<http://www.bverfg.de/en/press/bvg09-019en.html>

- The computer-controlled voting machines used in the election of the 16th German Bundestag did not meet the requirements which the constitution places on the use of electronic voting machines.
- The use of electronic voting machines requires that the essential steps of the voting and of the determination of the result can be examined by the citizen reliably and without any specialist knowledge of the subject.
- The voters themselves must be able to understand without detailed knowledge of computer technology whether their votes cast are recorded in an unadulterated manner as the basis of vote counting.

Public verifiability ...

- ... is implied by the basic constitutional principle of sovereignty of the people;
- ... is one of the fundamental principles of voting;
- ... ensures the democratic legitimacy of an election;
and
- ... directly counters technical errors and fraudulent manipulations

Public verifiability

- Every voter shall be able to reliably verify every essential election step in the vote casting and counting process.
- Every voter shall be able to perform the verification without detailed knowledge of computer technology

Naïve approach

Provide a receipt to every voter upon successful casting of the vote. Generate audit records containing the receipts of all votes.

Public verifiability

- Every voter shall be able to reliably verify every essential election step in the vote casting and counting process.
- Every voter shall be able to perform the verification without detailed knowledge of computer technology.

Naïve approach

Provide a receipt to every voter upon successful casting of the vote. Generate audit records containing the receipts of all votes.

NOT APPROPRIATE

Public verifiability

- Every voter shall be able to reliably verify every essential election step in the vote casting and counting process.
→ What are the essential election steps?
- Every voter shall be able to perform the verification without detailed knowledge of computer technology.
→ How

Ongoing scientific/technological movement
 Current hot spot:
 End-to-End (E2E) auditable voting systems

End-to-end (E2E) auditable voting systems

- Individual verifiability
Any voter can verify that his or her ballot is included unmodified in a collection of ballots;
- Universal verifiability
Any voter (and typically any independent party additionally) can verify, with high probability, that the collection of ballots produces the correct final tally;
- Election secrecy
No voter can demonstrate how he or she voted to any third party.

End-to-end (E2E) auditable voting systems

- Individual verifiability
Any voter can verify that his or her ballot is included unmodified in a collection of ballots;
- Universal verifiability
Any voter (and anyone else) can verify that the collection of ballots is correct and tallied;
- Election verifiability
No voter can demonstrate how he or she voted to any third party.

Bulletin board (communication model first presented by Benaloh et al., 1985):
A public channel where data can be published by authorized participants only and, once published, cannot be erased or overwritten by anyone.

Individual verifiability

Classification by Langer, Schmidt, Volkamer, Buchmann (2009):

- **Weak individual verifiability before / after tallying**
The voter can verify that his ballot has been cast / counted, i.e. is published on the bulletin board before / after tallying. There is no verifiability or proof provided regarding the question whether the ballot has been cast / counted as intended.
- **Average individual verifiability before / after tallying**
The voter can verify that his ballot has been cast / counted, i.e. is published on the bulletin board before / after tallying. Additionally, he is furnished with a proof that the ballot has been cast / counted as intended. The voter cannot verify the correct content of the ballot in terms of reconstructing the vote from the information he is provided with.
- **Strong individual verifiability before / after tallying**
The voter can verify that his ballot has been cast / counted, i.e. is published on the bulletin board before / after tallying. Additionally, he can verify that the ballot has been cast / counted as intended by reconstructing the vote from the information he is provided with.



Universal verifiability

Classification by Langer, Schmidt, Volkamer, Buchmann (2009):

- **Weak universal verifiability.**
Any interested party can verify that the tally is correctly computed from votes that were counted. Only the last step of the election procedure can be verified, i.e. the correct tallying of the votes contained in the ballot box immediately before the tallying phase.
- **Average universal verifiability.**
Any interested party can verify that the tally is correctly computed from votes that were cast.
- **Strong universal verifiability.**
Any interested party can verify that the tally is correctly computed from votes that were cast by legitimate voters.

Public Verifiability

- Every voter shall be able to reliably verify every essential election step in the vote casting and counting process.
→ What are the essential election steps?
- Every voter shall be able to perform the verification without detailed knowledge of computer technology.
→ How

Public verifiability challenges CC paradigm:
verification by the public
vs.
investigation by security experts

Public verifiability and CC paradigm

- Assurance gained from independent investigations by security experts does not immediately provide sufficient grounds for achieving confidence.
- Scaling up the level of effort in terms of scope, depth and rigour cannot properly satisfy the demand for public verifiability.
- Public verifiability requirements are, essentially, some kind of security requirements that should be reflected in appropriate CC SFR components.



Public verifiability and CC paradigm

Standard approach

- One may expect that the task of choosing appropriate SFRs covering public verifiability can be performed as a routine requirements engineering process.
- However, the result of such an approach will just add some further requirements to the security target of an e-voting product.
- It remains unclear to which extent the public verifiability of some set of requirements can be established by adding new requirements.



Public verifiability and CC paradigm

Refined approach (new proposal)

- In addition to management and audit actions the description of security functional families may be enriched by a section on verifiability actions.
- Such actions are intended to provide a new notion of dependency between SFR components.
- This kind of dependency is sufficient to demonstrate completeness w.r.t. individual or public verifiability demands.



Public verifiability and CC paradigm

- Experimental illustration of the refined approach using a specific set of SFRs:
 “Basic set of security requirements for Online Voting Products” (BSI-CC-PP-0037, April 2008)
- This Protection Profile does not contain any SFRs concerning public verifiability.
- Key question:
 Which SFRs demand for public verifiability?
- Decisive criterion:
 Identification of essential election steps



Basic set of security requirements for Online Voting Products (BSI-CC-

FDP_IFC.1A.1

The TSF shall enforce the SFP for polling processes on the following subjects, information, and controlled operations:

- Subjects: voter
- Information: ...
- Controlled operations:
 - identification / authentication
 - initiation of vote casting
 - revocation of initiated vote casting
 - final vote casting

Public verifiability and CC paradigm

- Typically, the operations of access/information flow control policies cover essential election steps.
- The following actions could be considered for the management functions in FMT w.r.t the controlled operations:
 - a) weak/average/strong individual verifiability [as defined previously]
 - b) weak/average/strong universal verifiability [as defined previously]



Public verifiability and CC paradigm

Abstraction for achieving a general refined approach.

Weak individual verifiability before / after tallying

The **voter** can verify that his ballot has been cast / counted, i.e. is published on the bulletin board before / after tallying. There is no verifiability or proof provided regarding the question whether the ballot has been cast / counted as intended.

voter → user (who is bound to the subject)

Public verifiability and CC paradigm

Abstraction for achieving a general refined approach.

Weak individual verifiability before / after tallying

The voter can verify that his **ballot has been cast / counted**, i.e. is published on the bulletin board before / after tallying. There is no verifiability or proof provided regarding the question whether the **ballot has been cast / counted** as intended.

ballot has been cast/counted → operation has been completed

Public verifiability and CC paradigm

Abstraction for achieving a general refined approach.

Weak individual verifiability

The user can verify that his operation has been completed, [i.e. is published on the bulletin board]. There is no verifiability or proof provided regarding the question whether the operation has been completed as intended.

Public verifiability and CC paradigm

- Public verifiability activities are not restricted to access/information control policies.
- FDP_UCT / FDP_UIT:
public verification of successful transfer w.r.t. confidentiality/integrity user data
- FIA:
public verification of successful identification/
authentication attempts

Public verifiability and CC paradigm

CC roadmap:

- Elaboration of the refined requirements engineering approach for all SFR families of CC Part 2
- Application of the refined approach to the enforcement of privacy policies in e-government, e-health, and e-business scenarios.