Deducing technical requirements from legal regulations

19.07.2012

SecVote Dagstuhl

Remarks

- Based on research results from the VerKonWa and ModiWa projects
  - Projects funded by DFG
- Based on own experiences in earlier collaborations with legal scientists from the University of Kassel
- Focus: Germany, German law and German elections

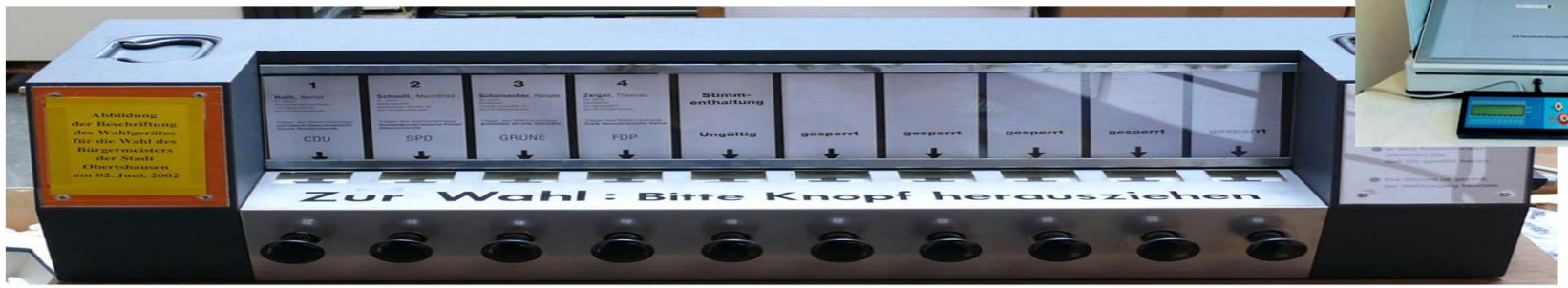
Overview

1. Situation in Germany including verdict from 2009
2. Methodologies to deduce technical requirements

Situation in Germany

Voting channels

- Main: voting in polling stations - the one the voter is assigned to
- About 30% postal voting (on request)
- In addition
  - Advanced voting at special locations: usually town hall
  - until 2009: 5% e-voting with voting machines



Voting systems

- Federal elections: 2 races / each one out of n
- Arbitrary complex local elections, about 500 candidates, 20 parties, 80 votes

Election laws

Human Rights Universal Declaration

International Convenant on Civil and Political Rights (ICCPR)

Grundgesetz

Bundeswahlgesetz

Landeswahlgesetz und Kommunalwahlgesetz

Bundespersonalvertretungs- und Betriebsverfassungsgesetz

Sozialgesetzbuch

Universitätsgesetz

Vereinsgesetz

.....

Grundgesetz (Basic Law)

universal

direct

secret

free

equal

public

Public nature of elections

Germany: Voters have the right to stay the whole day in the polling station - incl. to observe that the ballot box is empty and to observe the tallying

§ 31 Öffentlichkeit der Wahlhandlung (BWahlG)

Die Wahlhandlung ist öffentlich. Der Wahlvorstand kann Personen, die die Ordnung und Ruhe stören, aus dem Wahlraum verweisen.

… Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law (Grundgesetz–GG) which prescribes that all essential steps of an election (a) are subject to the possibility of public scrutiny unless other constitutional interests justify an exception and (b) can be examined reliably and without any specialist knowledge of the subject.

What are these essential steps?

- Voter can verify that ….
  - the ballot box is empty
  - the poll workers properly check the voter's right to vote
  - each voter receives only one ballot
  - voters are alone in the polling booth
  - voters cast their vote in a way that people in the polling station cannot see the content of the ballot
  - all votes including the own one are not altered
  - no additional votes are put into the ballot box
  - all votes including the own one are properly tallied
  - …

eligibility

secrecy

integrity

Note, but only in one polling station

Public nature of elections

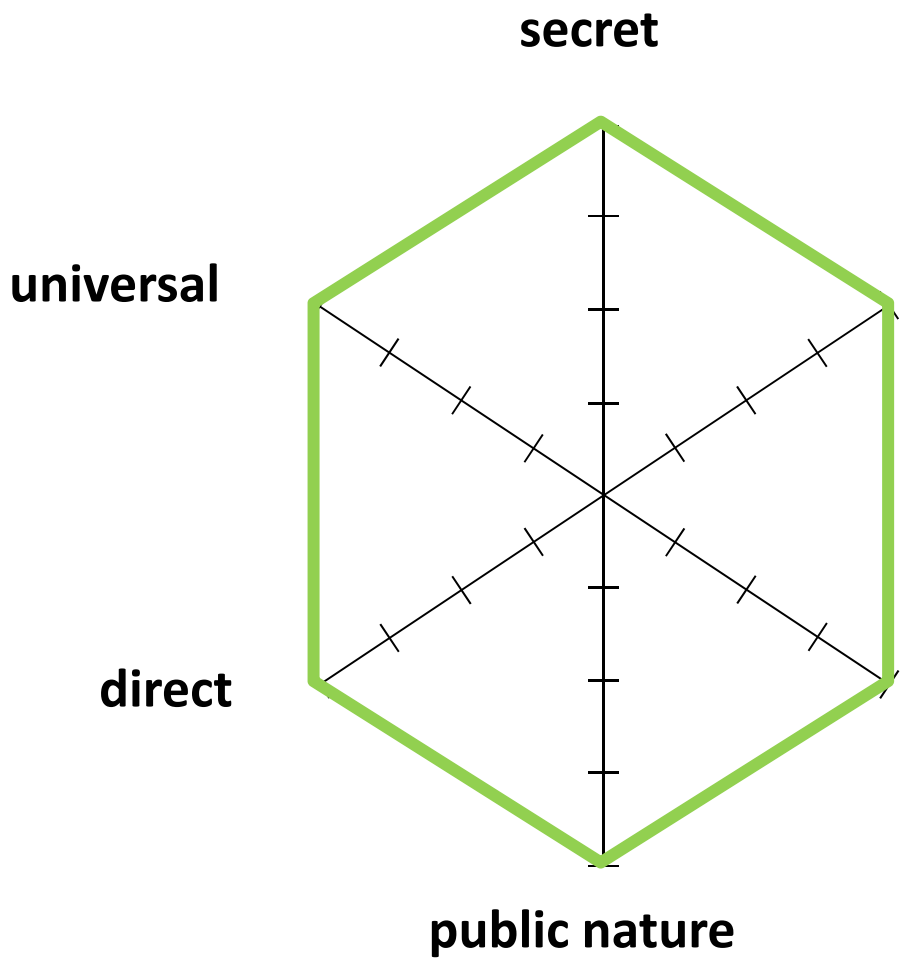
Germany: Voters have the right to stay the whole day in the polling station - incl. to observe that the ballot box is empty and to observe the tallying

§ 31 Öffentlichkeit der Wahlhandlung (BWahlG)

Die Wahlhandlung ist öffentlich. Der Wahlvorstand kann Personen, die die Ordnung und Ruhe stören, aus dem Wahlraum verweisen.

… Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law (Grundgesetz–GG) which prescribes that all essential steps of an election (a) are subject to the possibility of public scrutiny unless other constitutional interests justify an exception and (b) can be examined reliably and without any specialist knowledge of the subject.

What does it mean that other constitutional interests could justify an exception?



perfect democratic elections

Traditional elections in polling stations?

Postal voting?

What would be a reliable examination without any specialist knowledge?

- Understanding procedures / security mechanisms
  - On a high level?
  - Including the math behind?
- Can tools be used to support examination?

Remark: public nature of elections is not required in many other countries

Austria: Voters must leave the polling stations after having cast a vote

§ 84 (1) Wenn die für die Wahlhandlung festgesetzte Zeit abgelaufen ist und alle bis dahin im Wahllokal oder in dem von der Wahlbehörde bestimmten Warteraum erschienenen Wähler gestimmt haben, erklärt die Wahlbehörde die Stimmabgabe für geschlossen. Nach Abschluss der Stimmabgabe ist das Wahllokal, in welchem nur die Mitglieder der Wahlorgane, deren Hilfsorgane, die Vertrauenspersonen gemäß § 15 Abs. 4, die Wahlzeugen sowie die akkreditierten Personen gemäß § 20a Abs. 3 verbleiben dürfen, zu schließen.

NRWO

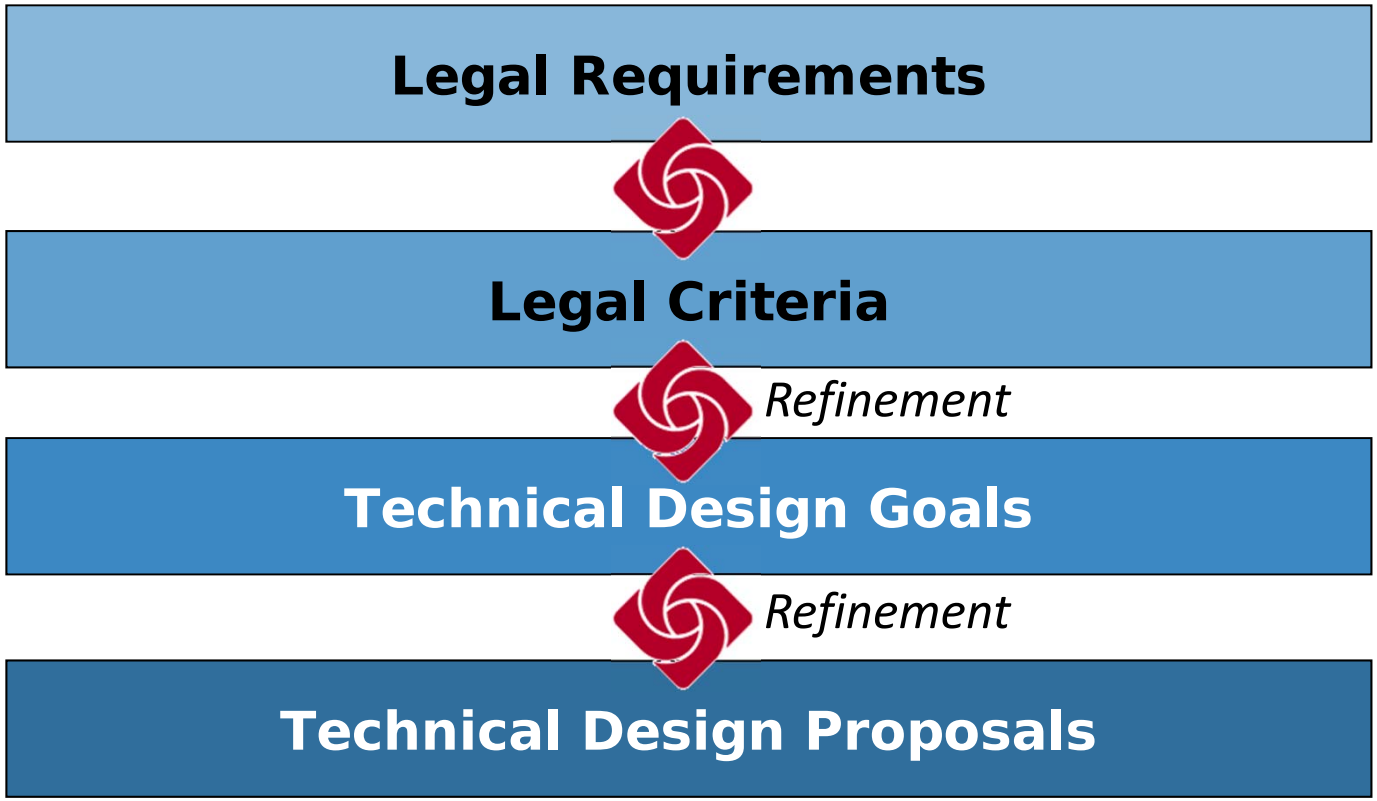
→ Very imporatnt to have in mind that different countries have different laws and different voting systems in place

Methodologies to deduce technical requirements

KoRA

- Refinement of abstract legal requirements into technical design proposals
  - Over 4 stages
  - Iterative process
  - In interdisciplinary projects
  - No automation

Four phases

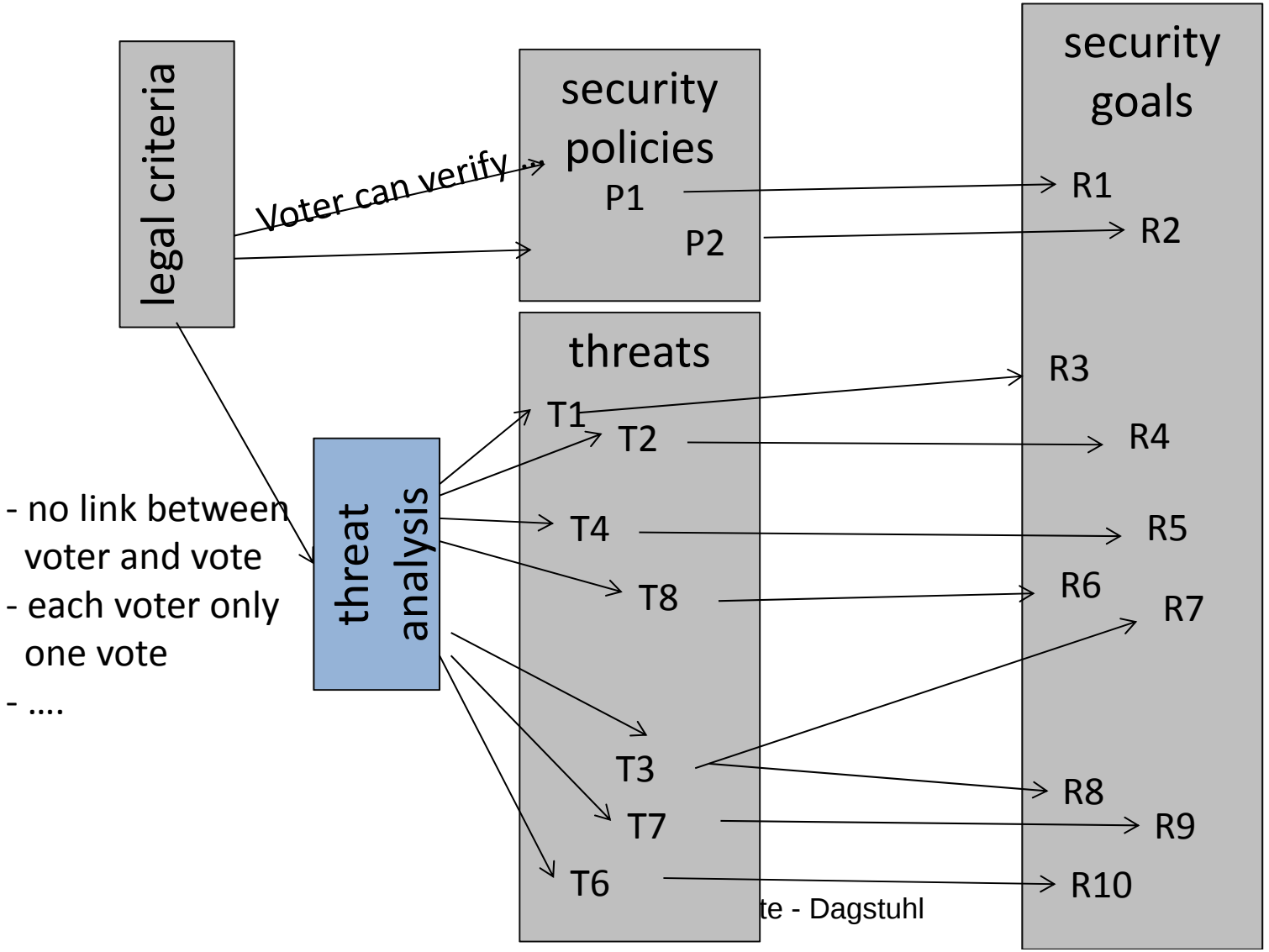


Basic law

Election laws and regulations + decisions

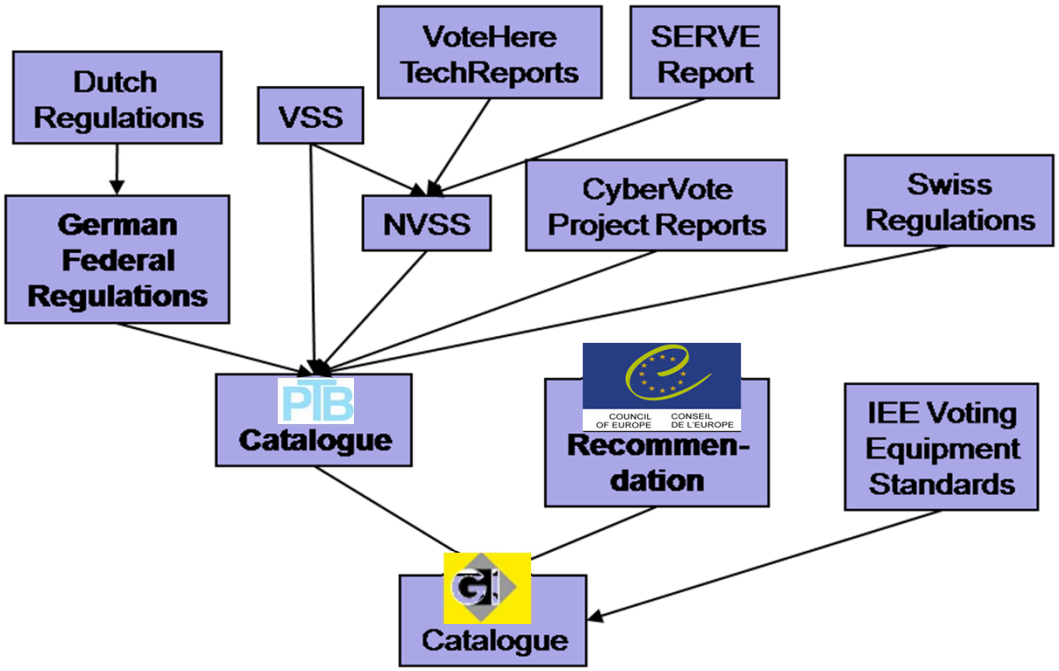
?

Technical Design Goals based on Common Criteria



Technical Design Goals based on literature review

Many e-voting requirement documents with long lists of security goals



Many (different) technical Interpretations / security goals in papers proposing voting schemes at different voting events (EVOTE, EVT/WOTE, Vote-ID, Re-Vote), crypto and formal methods conferences

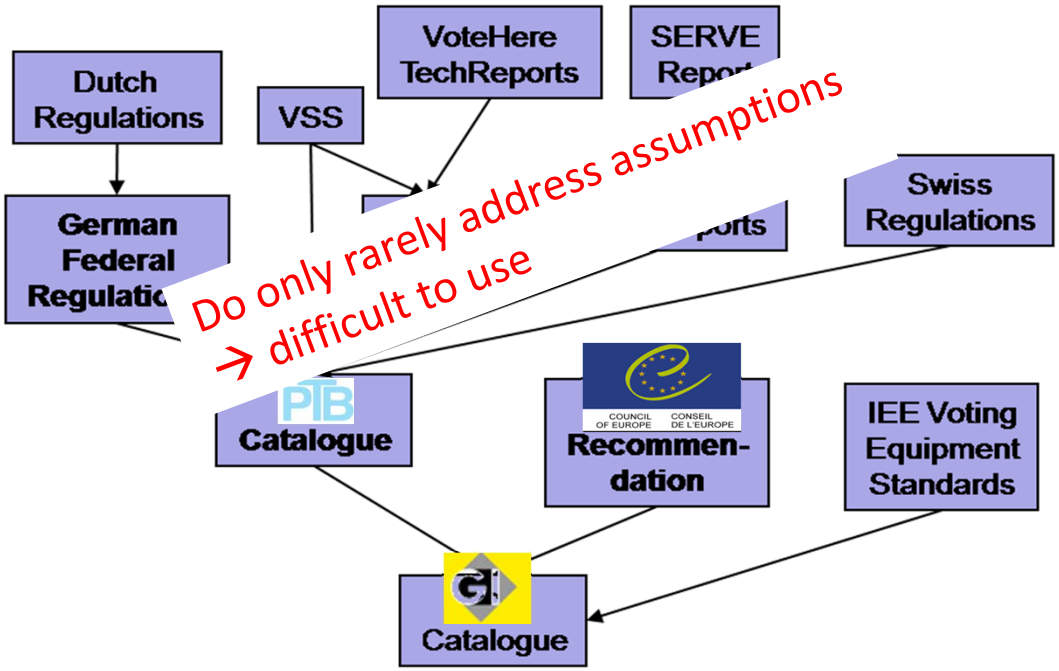
→ Map to legal criteria

Does it help?

- Neither any of the traditional systems nor any of the technical proposals for e-voting ensure these without making assumptions!

Technical Design Goals based on literature review

Many e-voting requirement documents with long lists of security goals

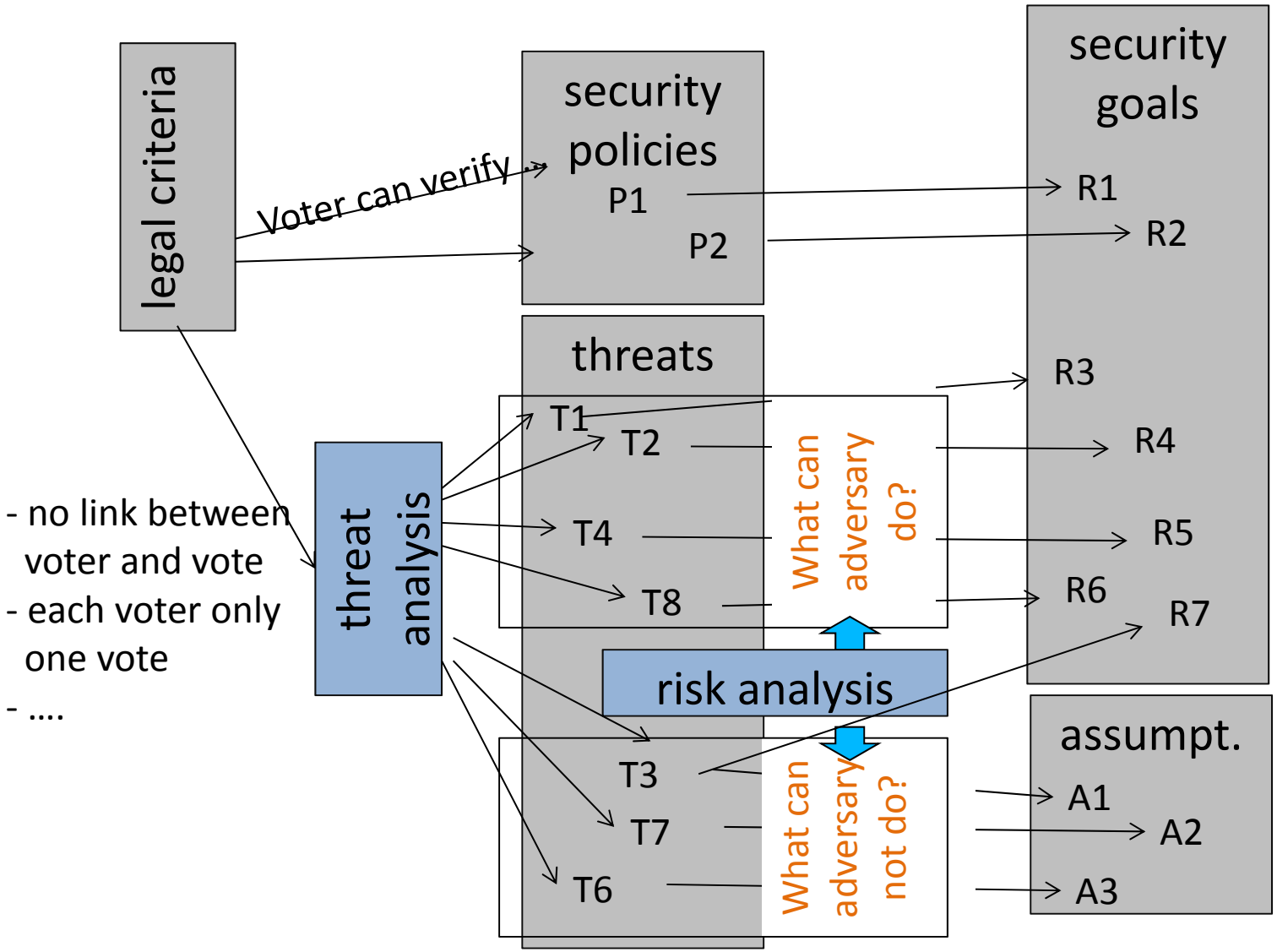


Many (different) technical Interpretations / security goals and different assumptions in papers proposing and analyzing voting schemes at different voting events (EVOTE, EVT/WOTE, Vote-ID, Re-Vote), crypto and formal methods conferences

→ Identify assumptions, i.e. non existence of specific threats / attacker capabilities

- Like secure voting environment
- Entities which do not collaborate
- Crypto is secure also in future
- Untappable channels
- Coercer cannot control voters during the registration phase

Technical Design Goals based on Common Criteria



Does it help?

- Neither any of the traditional systems nor any of the technical proposals for e-voting ensure these without making assumptions!

Assumptions

- In general not a legal concept → hard to discuss which are acceptable

- Instead concept of "Gestaltungsspielraum" (freedom of design)
  → other constitutional interests can justify an exception/weakening of others
  → comparison with traditional paper based election in place
  - Increase level of public nature as it is possible to verify correct tallying in all polling stations remotely and correct processing of own vote.

    Does this justify the assumption that crypto works also in future?
  - Increase level of universal principle by enabling blind people with DREs.

    Does this justify the assumption that emission might be measured with arbitrary expensive devices?

  - Risk analysis, how likely!
  - Not as justification: cheaper / faster results as such
  - Usually not that easy with one advantage and one disadvantage
  - In particular: decentralized versus centralized (whom to trust)

Recommendations

- Legal criteria as concrete as possible and map to technical goals
  - Have in mind what type of election and whether it is an additional channel or replaces one of the existing ones
- Analyze systems and be fair and realistic, and list all assumptions and reduce assumptions as much as possible
- Explain advantages and remaining assumptions and compare e-voting proposal with legal experts (ideally group of different technical and legal experts)
  - Have in mind what type of election and whether it is an additional channel or replaces one of the existing ones

Questions?