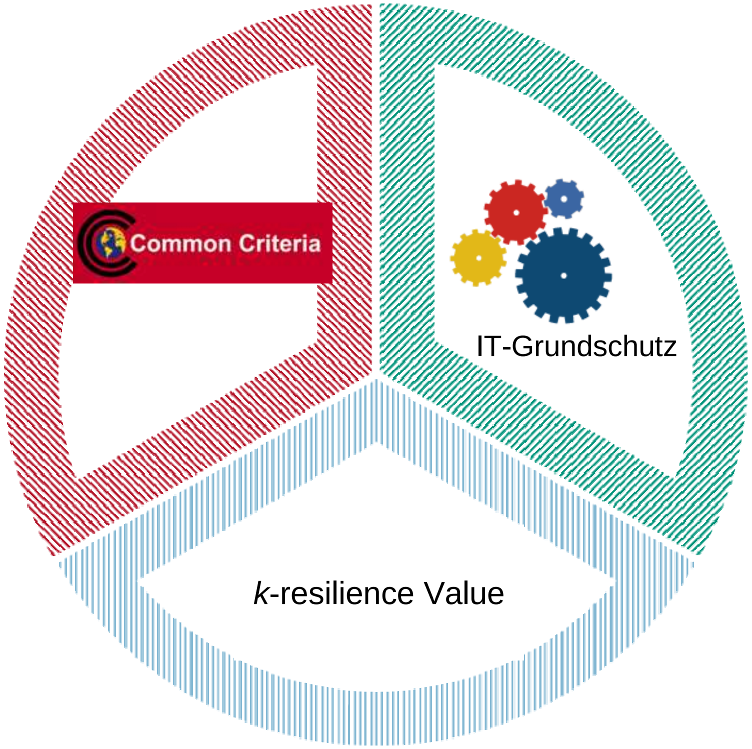
Evaluation & Certification of (Internet) Voting Systems regarding Security Requirements

Melanie Volkamer

Evaluation and Certification Approach



Common Criteria for voting software

IT Grundschutz (includes ISO 27001) for operational environment

→ Outside threats

Existing international standards

k-resilience value → insider threats

Resarch

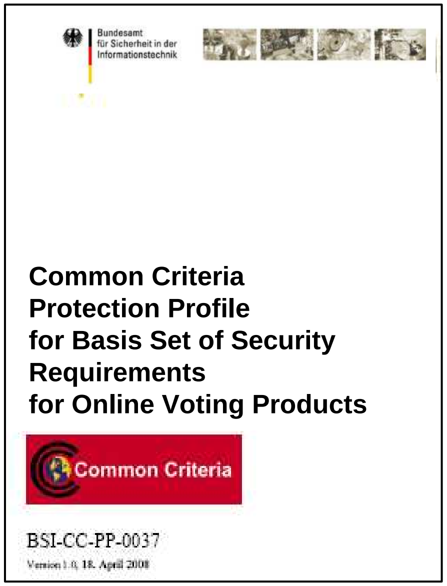
Common Criteria - Overview

The Common Criteria for Information Technology Security Evaluation (CC) is an international standard (ISO15408) for the evaluation and certification of security critical software.

- users *specify* security *functional* and *assurance* requirements plus the *trust model*
- vendors *implement* and/or make claims about the security of their products, and
- testing laboratories *evaluate* products to determine if they actually meet the claims.
- certification authorities observe the evaluation process & certify products after successful evaluation

Common Criteria – Protection Profile

- ... is a document, typically created by users/community, which identifies security functional requirements and evaluation assurance requirements plus the trust model for a class of security critical products



Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria
Protection Profile
for Basis Set of Security
Requirements
for Online Voting Products

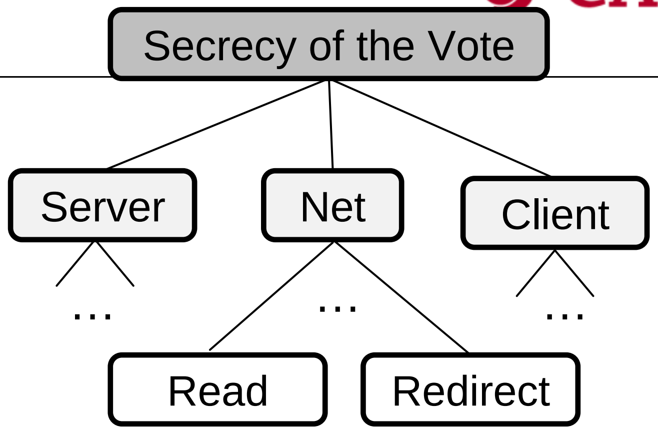
Common Criteria

BSI-CC-PP-0037
Version 1.0, 18. April 2008

http://www.bsi.de/zertifiz/zert/reporte/pp0037a.pdf

Common Criteria - SFRs

- Threat Analyses


Secrecy of the Vote

Server

Net

Client

…

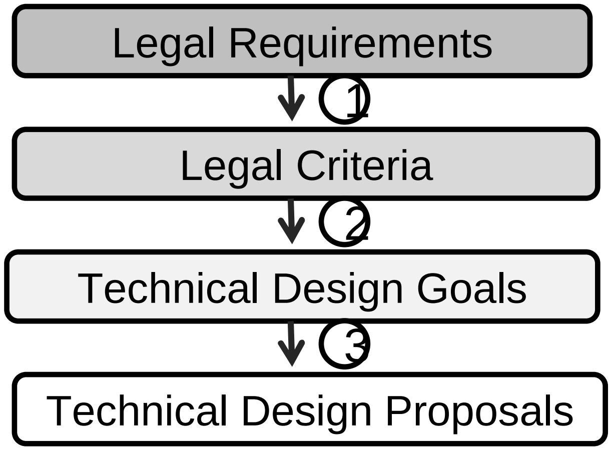
…

…

Read

Redirect

- KORA-Approach
  - Konkretisierung rechtlicher Anforderungen


Legal Requirements

1

Legal Criteria

2

Technical Design Goals

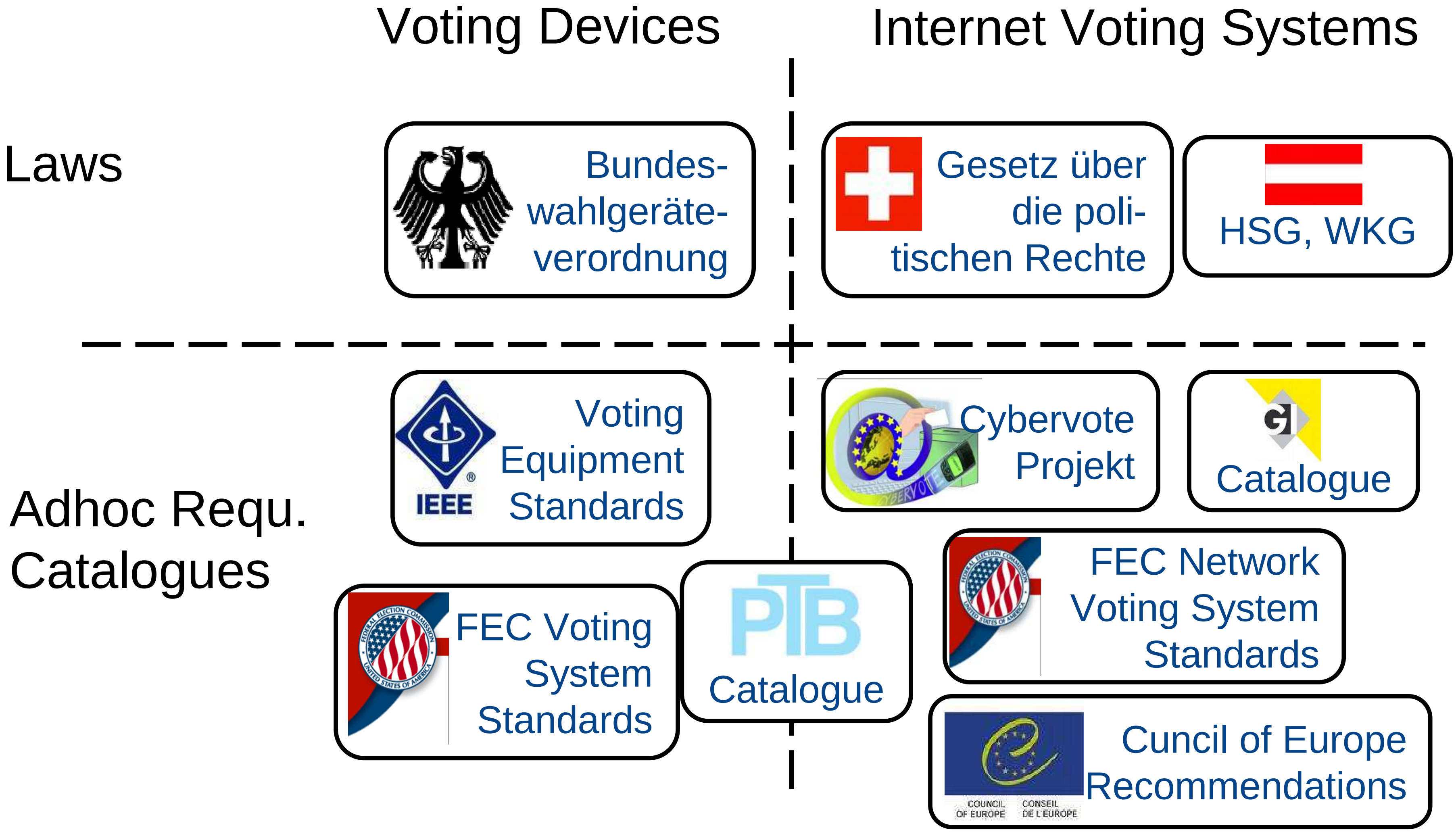
3

Technical Design Proposals

- Literature Research

Common Criteria - SFRs

CASED



Voting Devices

Internet Voting Systems

Laws

Bundeswahlgeräteverordnung

Gesetz über die politischen Rechte

HSG, WKG

Adhoc Requ. Catalogues

IEEE

Voting Equipment Standards

Cybervote Projekt

GI Catalogue

FEC Voting System Standards

PTB Catalogue

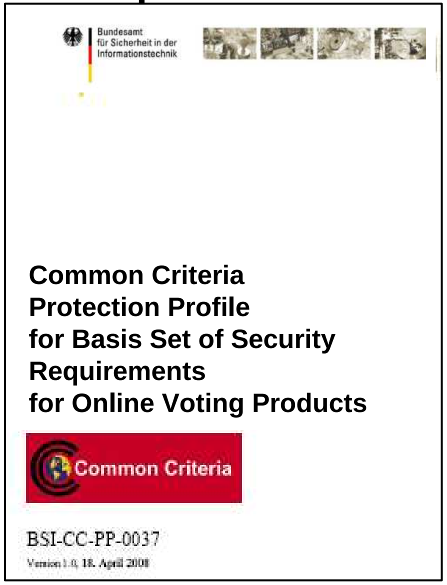
FEC Network Voting System Standards

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Cuncil of Europe Recommendations

Common Criteria – Protection Profile

- ... is a document, typically created by users/community, which identifies security functional requirements and evaluation assurance requirements plus the trust model for a class of security critical product



Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria
Protection Profile
for Basis Set of Security
Requirements
for Online Voting Products

Common Criteria

BSI-CC-PP-0037

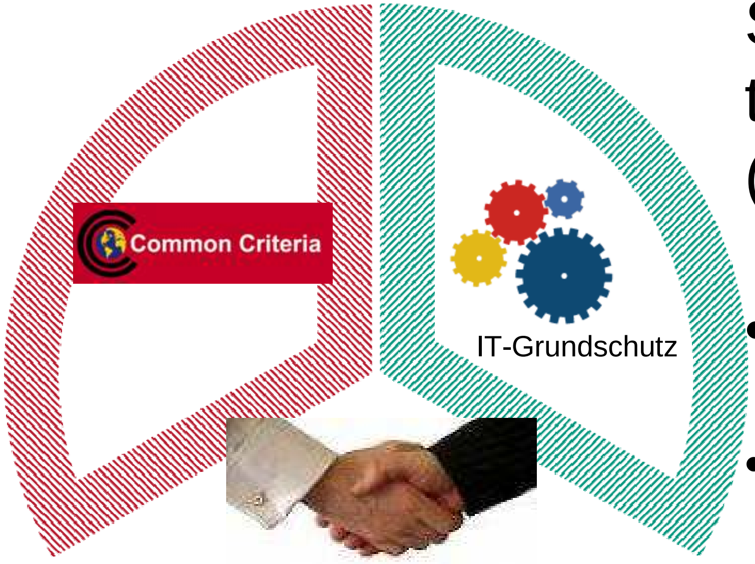
Version 1.0, 18. April 2008

https://www.bsi.bund.de/cae/servlet/contentblob/480286/publicationFile/29305/pp0037b_engl_pdf.pdf

Common Criteria – SAR & Trust Model

- Evaluation Assurance Requirements
  - EAL 2+ (EAL1-7)
    - Formal methods for EAL6/7
      - e.g. PI-Calculus for voting protocols (→Mark Ryan)
- Trust Model
  - Intruder‘s Capability
    - Basic (basic, enhanced-basic, moderate, high)
  - Set of Assumptions to the Organisation Environment
    - A.ElectionServer, A.Availability, A.ServerRoom, …

IT-Grundschutz - Overview



Standard safeguards to evaluate typical organizational Environment (incl. IT infrastructure)

- Includes ISO 27001
- Methodology (simplified):
  - Description of IT structure
  - Mapping to ITGS modules
  - Showing how assigned safeguards are met
  - Evaluation
  - Certification

IT-Grundschutz – „Template“

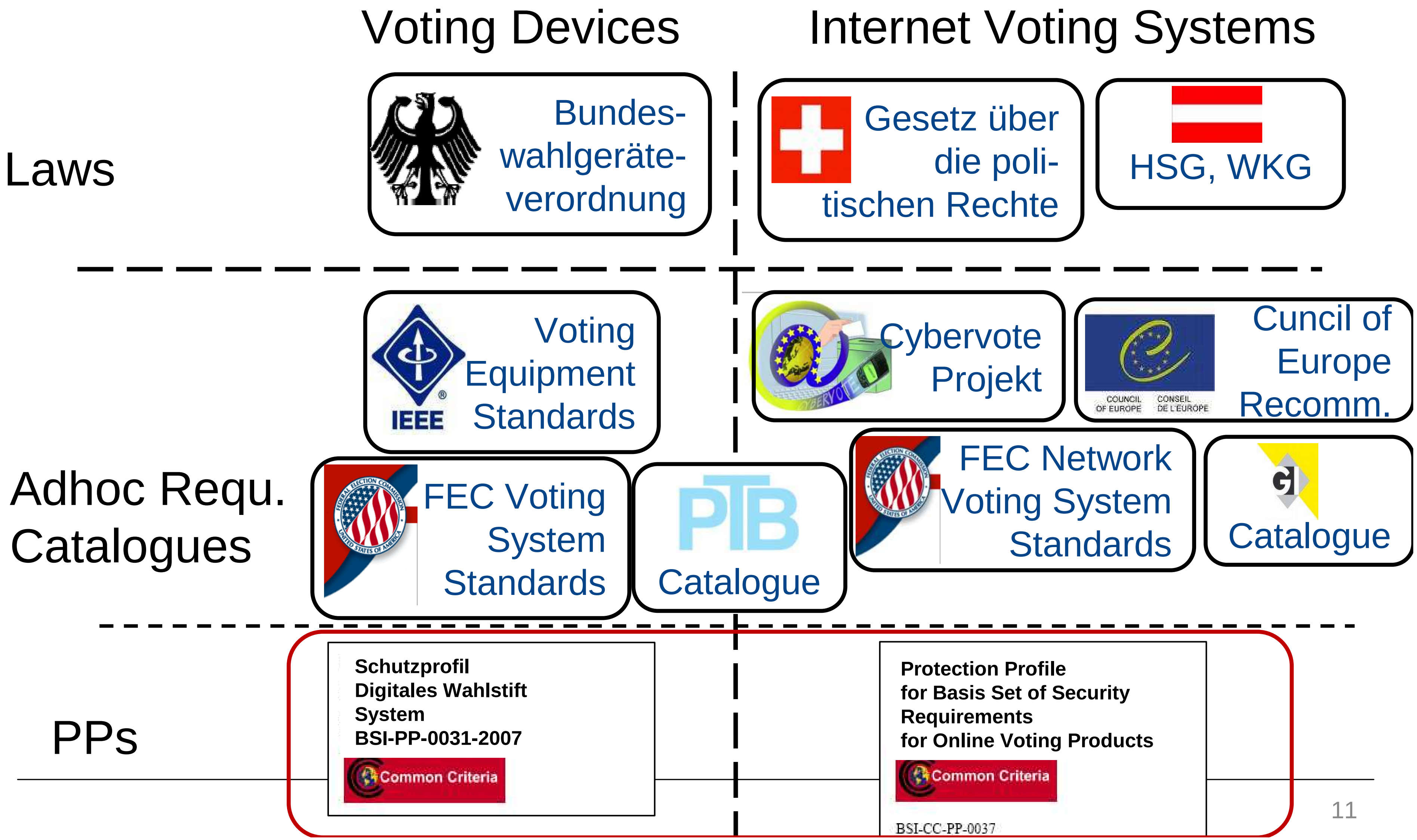
„Work in Progress!!“

- Template of ITGS modules

- ToDo‘s:

1. Defining requirements to the operational environment of remote voting software
2. Mapping to ITGS modules and thus safegurds

IT-Grundschutz – Requirements to the operational environment

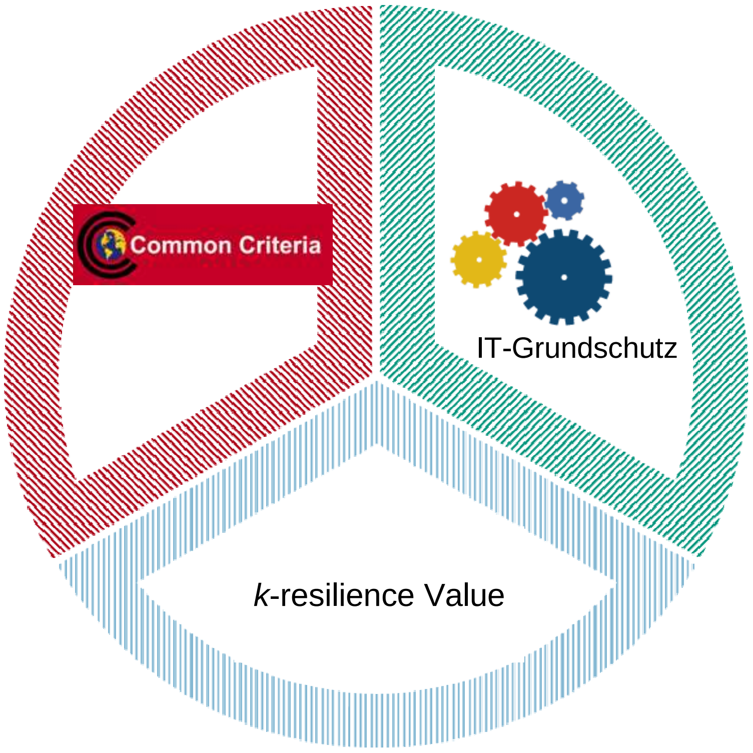


	Voting Devices	Internet Voting Systems
Laws	Bundeswahlgeräteverordnung	Gesetz über die politischen Rechte HSG, WKG
Adhoc Requ. Catalogues	Voting Equipment Standards FEC Voting System Standards PTB Catalogue	Cybervote Projekt Cuncil of Europe Recomm. FEC Network Voting System Standards Catalogue
PPs	Schutzprofil Digitales Wahlstift System BSI-PP-0031-2007 Common Criteria	Protection Profile for Basis Set of Security Requirements for Online Voting Products Common Criteria BSI-CC-PP-0037

IT-Grundschutz - Safeguards

- **Protection of the software (A. Election Server)**
  - S 2.17: Entry regulations and controls
  - S 1.58: Technical and organisational requirements for server rooms
  - **Availability (A.Availability)**
  - S 2.314: Use of high-availability architectures for servers
- **Secure storage**
  - S 4.168: Selection of a suitable archive system
  - S 1.60: Appropriate storage of archival media
  - **Assistance and training**
  - S 3.5: Training on IT security safeguards
  - S 2.198: Making staff aware of IT security issues
  - **Personnel**
  - S 3.2: Commitment of staff members to compliance with relevant laws, …
  - ….

k-resilience Value

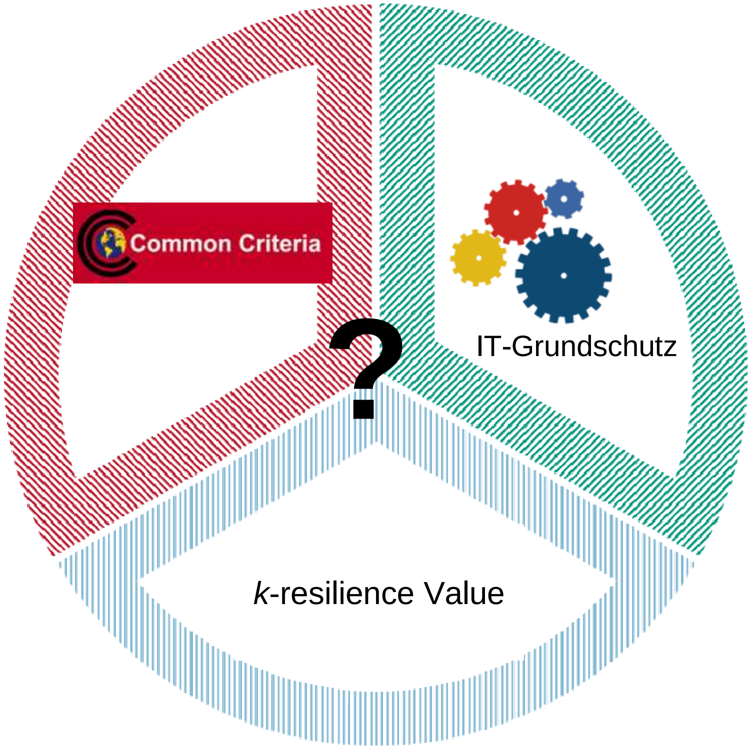


The k-resilience value helps to understand the power of possible insider threats; that is which people/ component needs to be trusted.

- (k out of N)-resilient
- $(k_1 \wedge \ldots \wedge k_m)$ out of $(N_1,\ldots,N_m)$- resilient
- $(k_1 \vee \ldots \vee k_m)$ out of $(N_1,\ldots,N_m)$- resilient

→ Propositional logic term
→ Conjunctive normal form

Future Work



Common Criteria

- Experiences with Basis Protection Profile
- Integration of verifiability

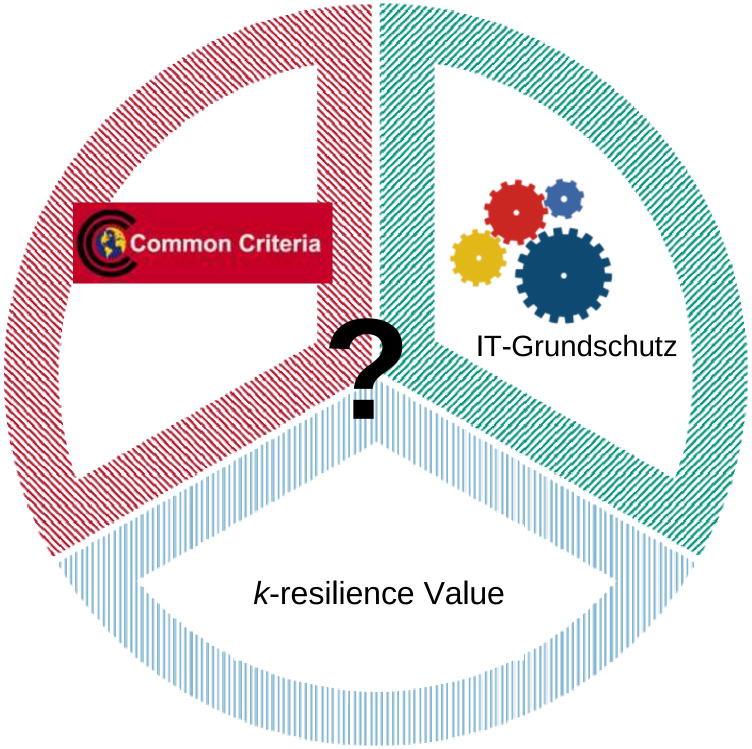
IT-Grundschutz

- voting specific moduls

k-resilience

- standardization

Future Work



Other Approaches

- Evaluation regarding
  - cryptographic protocols
  - data protection issues
  - usability issues

Integration in

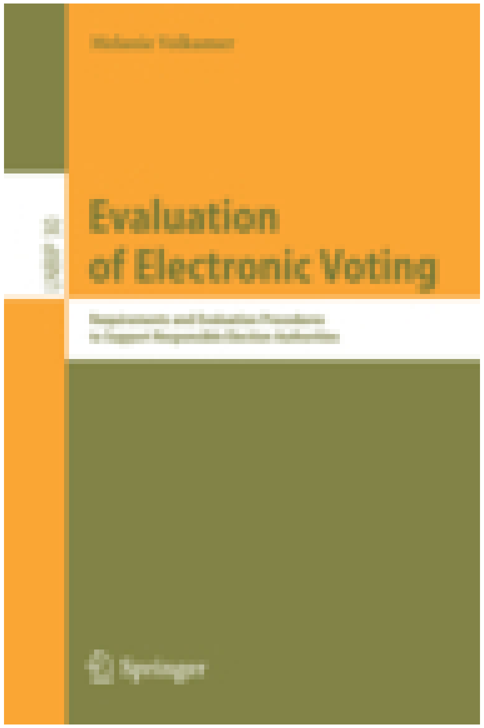
- legal context
- election observation context

Questions to be answered

- who‘s doing the evaluation/certification?
- who pays?
- how often/re-certification

Thank you for your attention!

Questions?



www.cased.de

Center for Advanced Security Research Darmstadt

melanie.volkamer@cased.de

http://www.springer.com/computer/information+systems/book/978-3-642-01661-5