



eVoting – Chance oder Gefahr ?

Alexander Prosser





Wo liegen die Schwierigkeiten ?

Warum eigentlich eVoting ?

Wo liegen die Schwierigkeiten ?

Warum eigentlich eVoting ?

eVoting = Internetwahlen

**=> Beitrag beschäftigt sich nicht mit
Wahlmaschinen, DRE etc., da kein
erkennbarer Mehrwert.**

<http://e-voting.at>



Persönlicher Hintergrund:

Forschungsgruppe e-voting.at

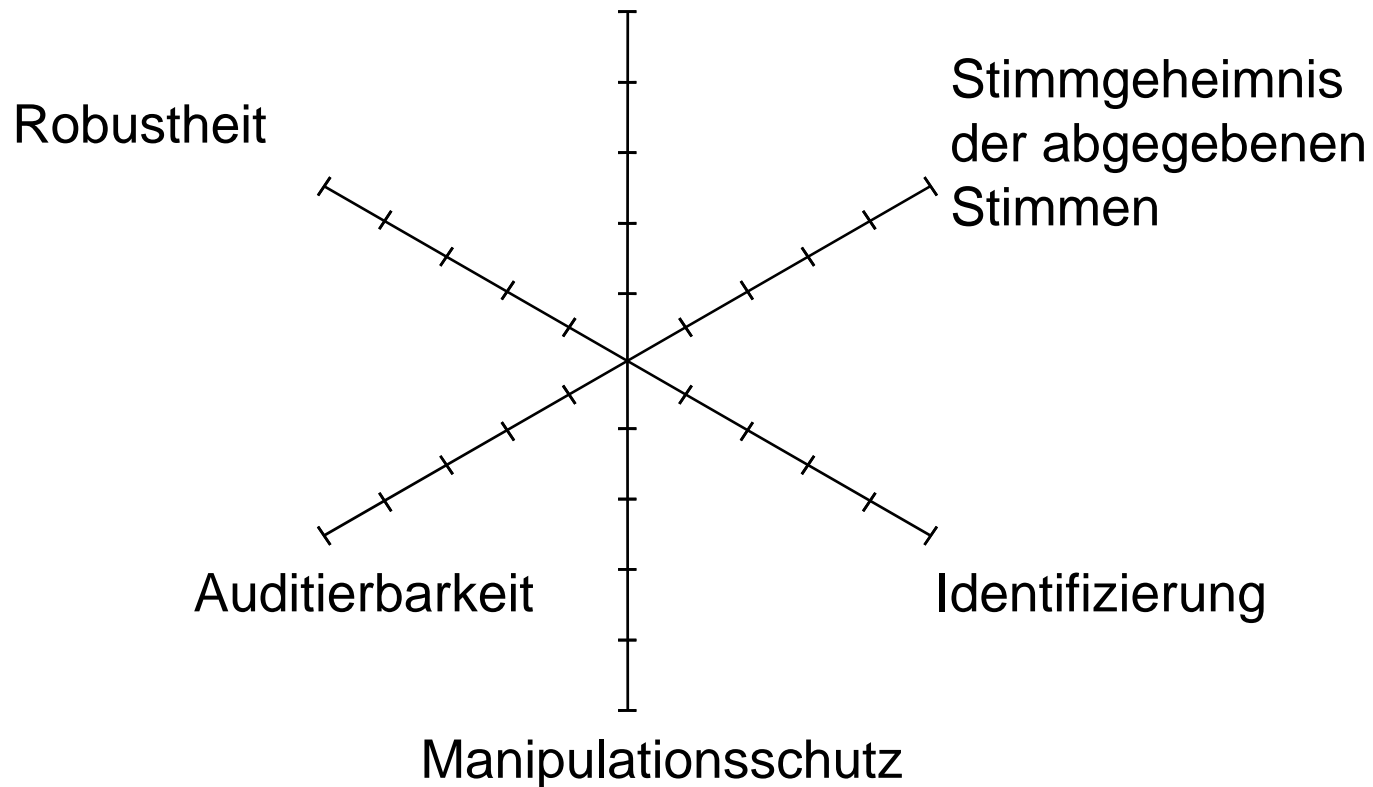
- Kryptographie
- Prozesse
- Akzeptanz

Alle 3 Internetwahlpiloten in Österreich
Gründer EDEM Tagungsserie



Anforderungen an ein eVoting-System:

Sicherheit gegen Stimmenkauf und Zwang





Technische vs. organisat. Sicherung:

Org. Sicherung => Verlass auf Menschen

In letzter Konsequenz immer org. Sicherung

Die entscheidenden Fragen:

- wer bzw. welche Koalition ?
- eine oder mehrere Stimmen ?



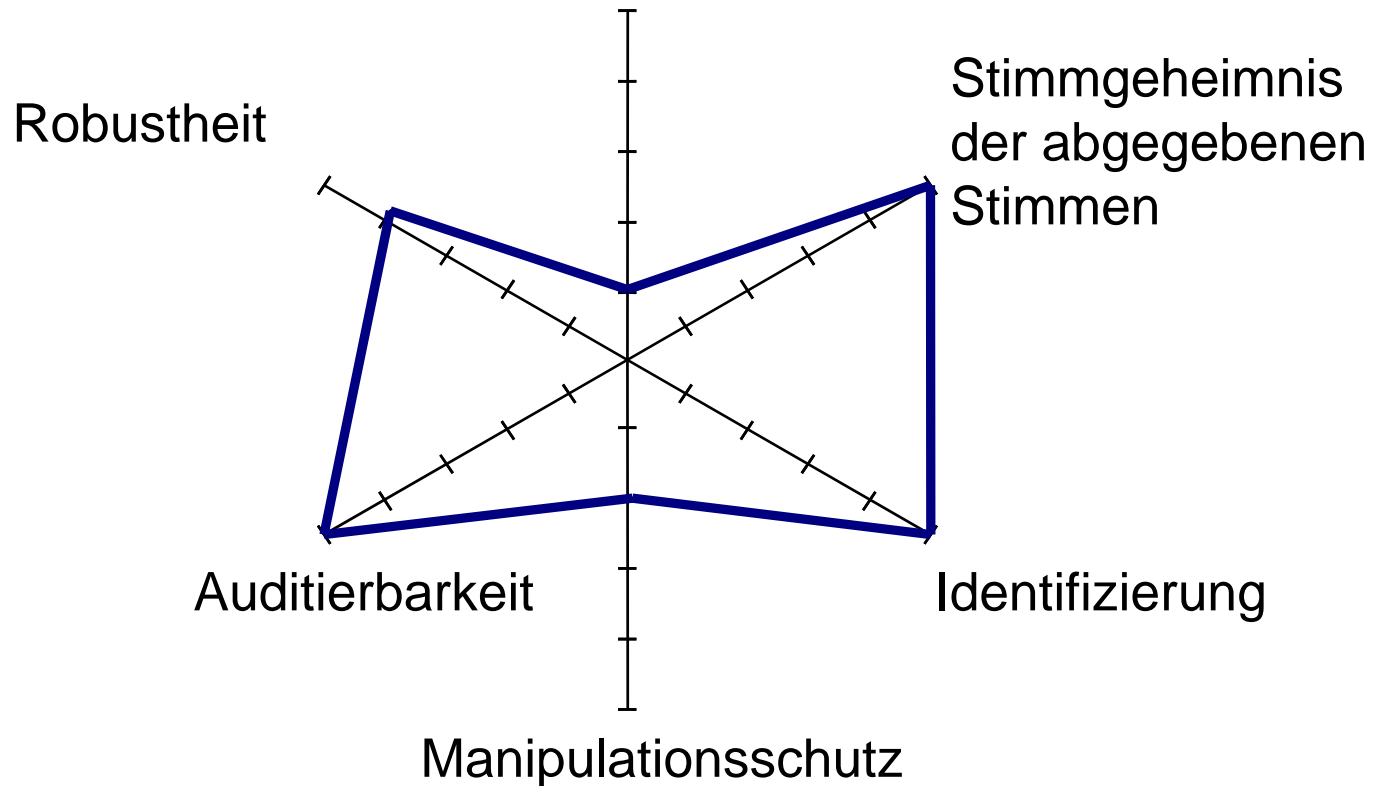
Technische vs. organisat. Sicherung:

	eine Stimme	alle Stimmen einer Einheit*	alle Stimmen
ein Einzelner			
eine Koalition unter Einschluss des Wählenden			
....			
die Wahlkommission			

* Sprengel, Wahlkreis, etc.

Beispielsystem:

Sicherheit gegen Stimmenkauf und Zwang





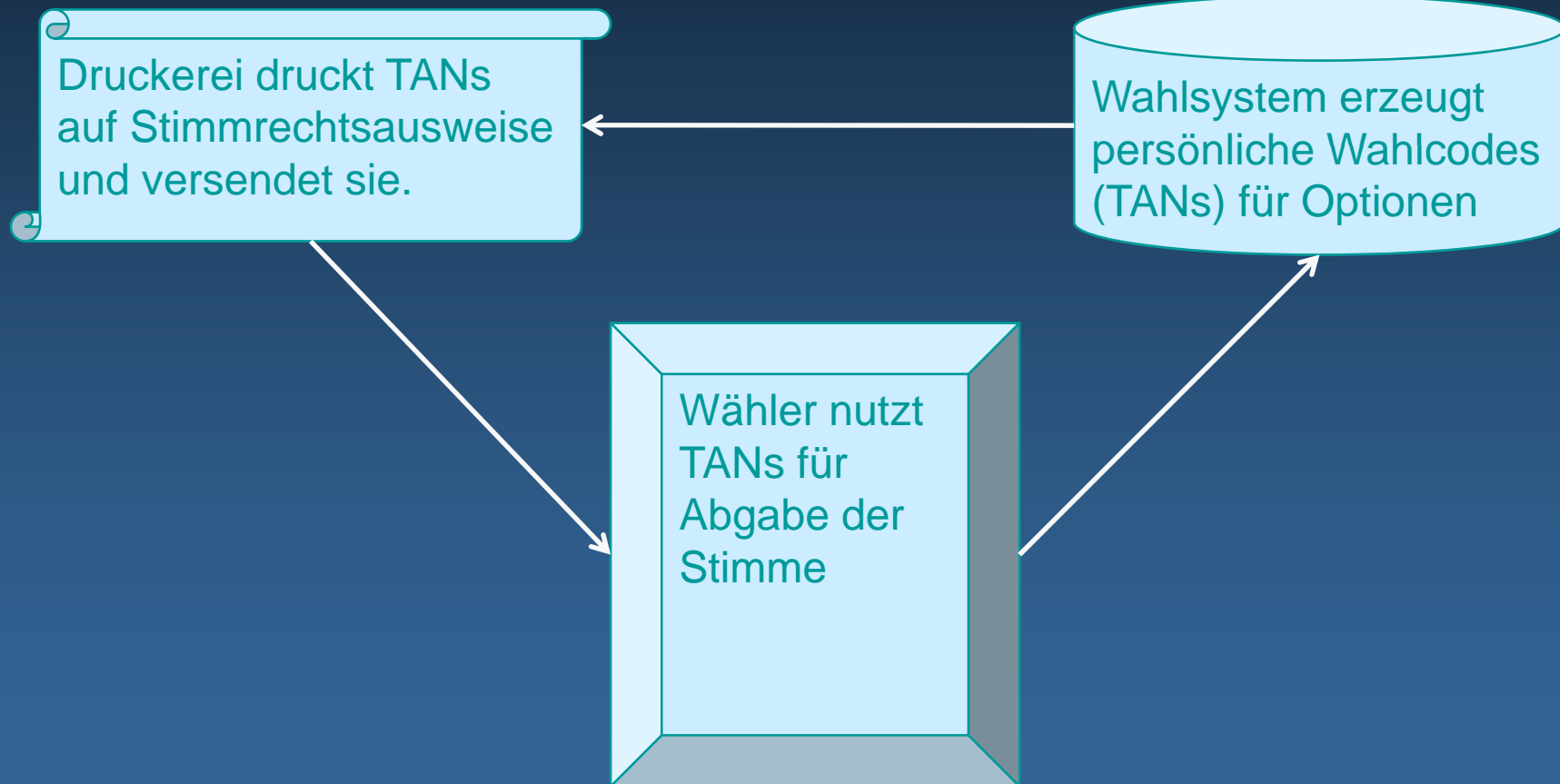
Mindeststandards:

Europarat: Rec 2004(11) für politische Wahlen

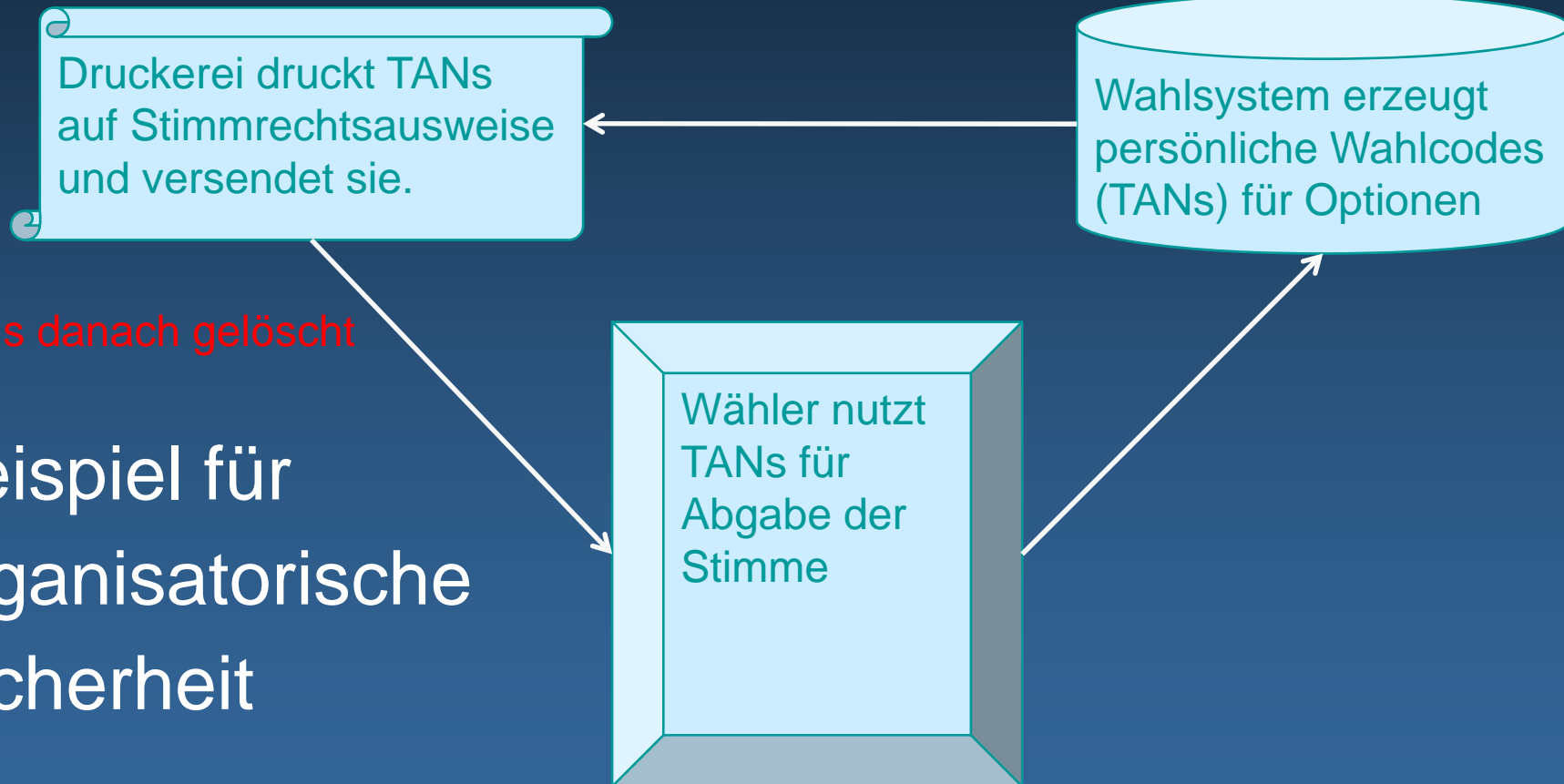
BSI: Schutzprofil eVoting für Vereinswahlen
=> Annahme eines sicheren Wahlserver

Relevante Wahlprotokolle

Anonymisierung durch TAN:



Anonymisierung durch TAN:

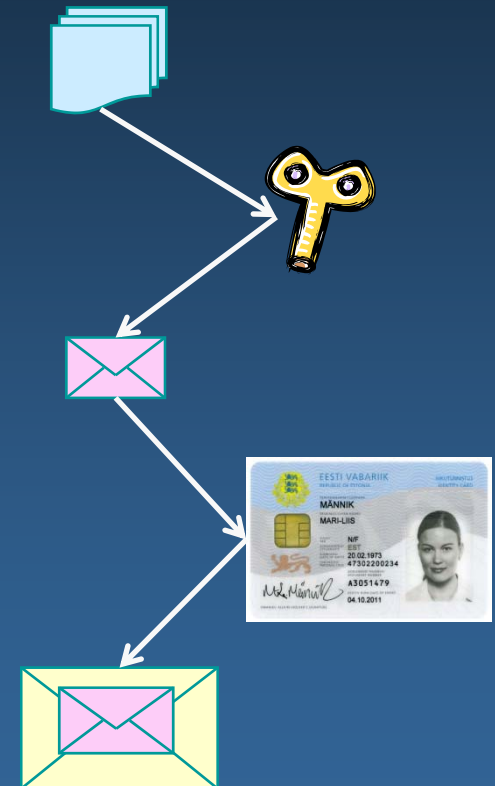


TANs danach gelöscht

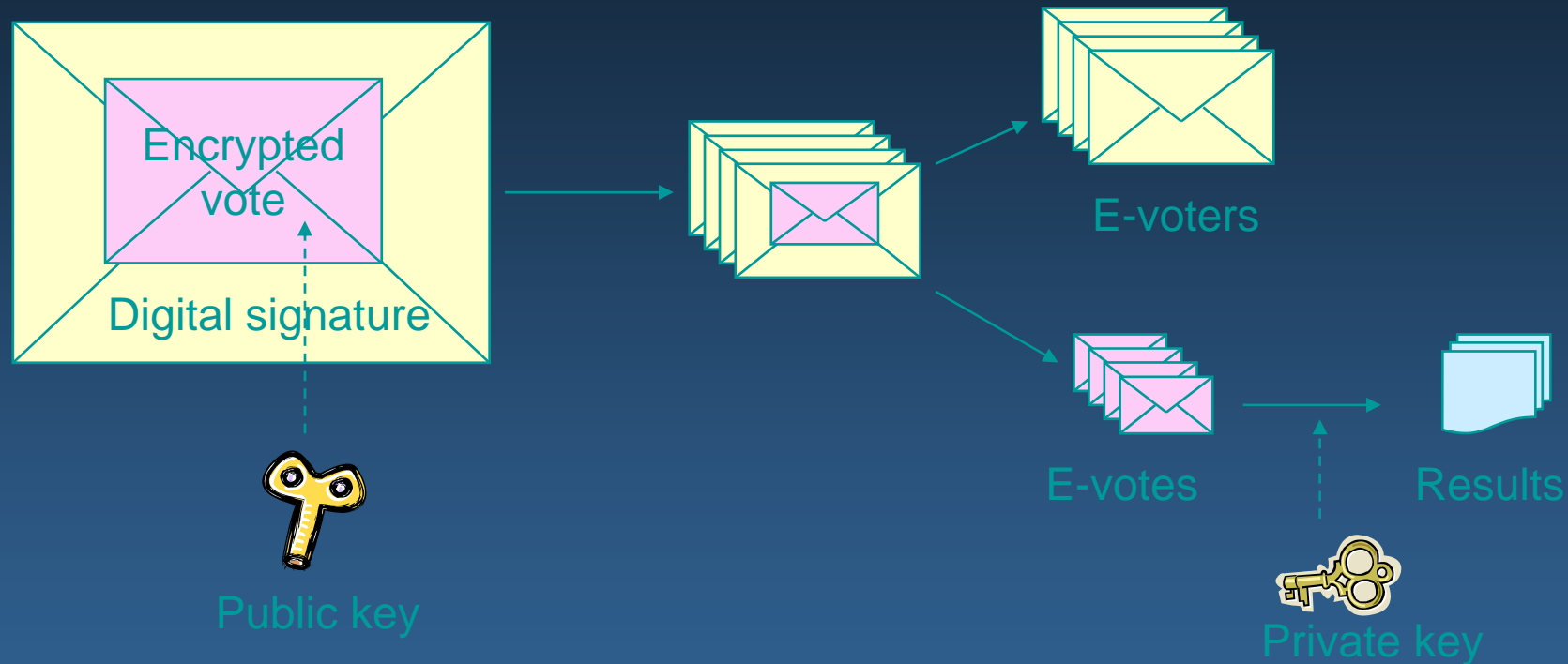
Beispiel für organisatorische Sicherheit

Envelope System:

1. WählerIn füllt Stimmzettel aus
2. Stimme wird mit öffentlichem Schlüssel der Wahlkommission verschlüsselt => „Inner envelope“
3. Stimme wird von WählerIn digital signiert => „Outer envelope“

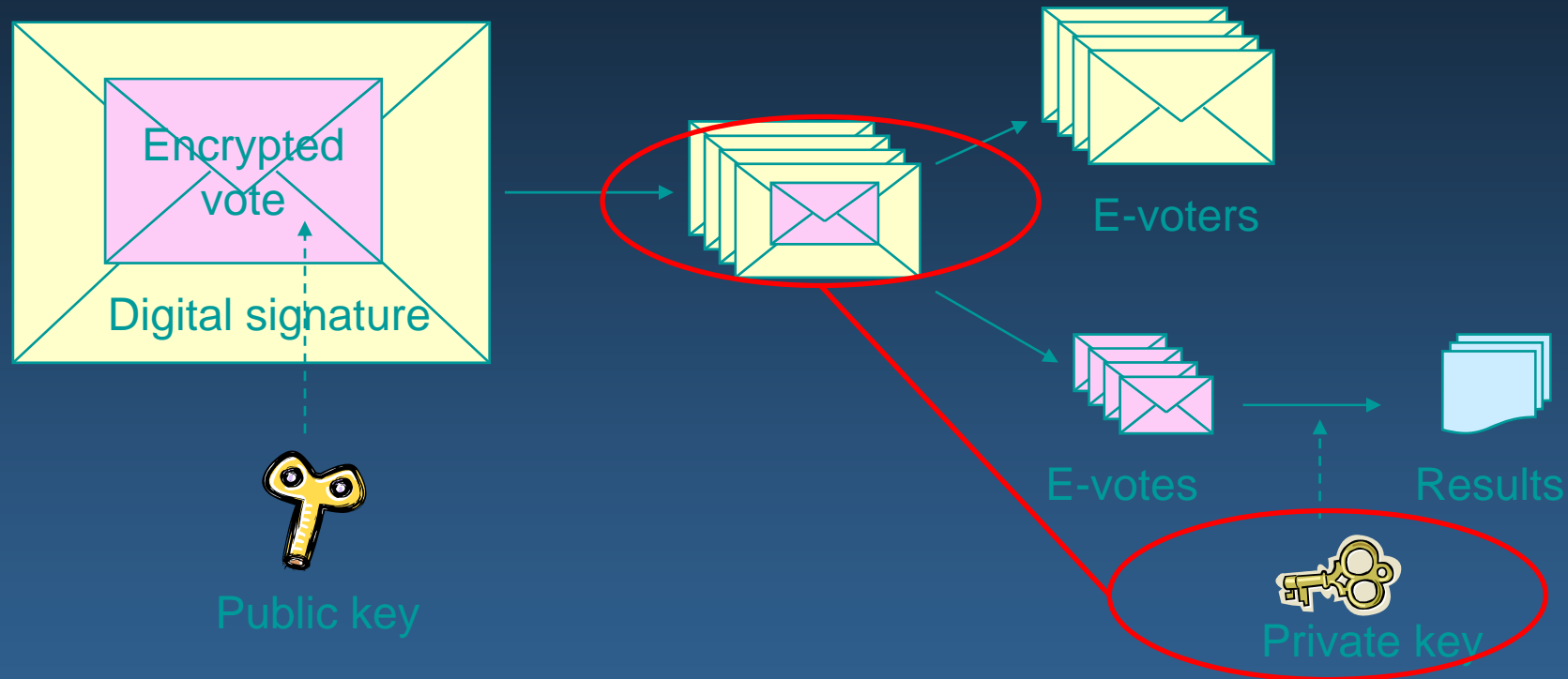


Envelope System:



Wiederholte ersetzende Stimmabgabe möglich

Envelope system:



“This transfer of authority is essential, as anybody having the signed votes in the outer envelope and the private key to the inner envelope would be able to break voter secrecy”

Anonymer Kanal (MIX):

„Mischen“ als Analogie zu physischer Urne

Mehrere Mischer in Serie

Chaum (1981), Hirt und Sako (2000)

Probleme liegen in manueller Bearbeitung und

Auditierbarkeit



Homomorphismus :

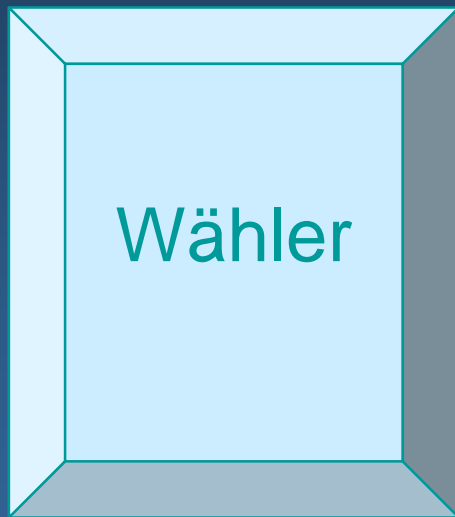
Stimme (ja/nein):

Summe/Produkt:

110110111000

verschlüsselt

entschlüsselt



10110100

Server

Anzahl ja
Anzahl nein



Homomorphismus:

Additiv und multiplikativ

Cohen und Fischer (1985), Benaloh (1987)

Schoenmakers (1999) => Cybervote

Anonymisierung sehr gut

Themen sind Nachvollziehbarkeit und Audit
(summarische Fortschreibung des Ergebnisses)



Blinde Signatur (Chaum 1982):

(sehr informelle Beschreibung):

Normale Signatur (komplette Nachricht):

1. Signatur: $t \Rightarrow t^d$

2. Prüfung: $(t^d)^e = t$

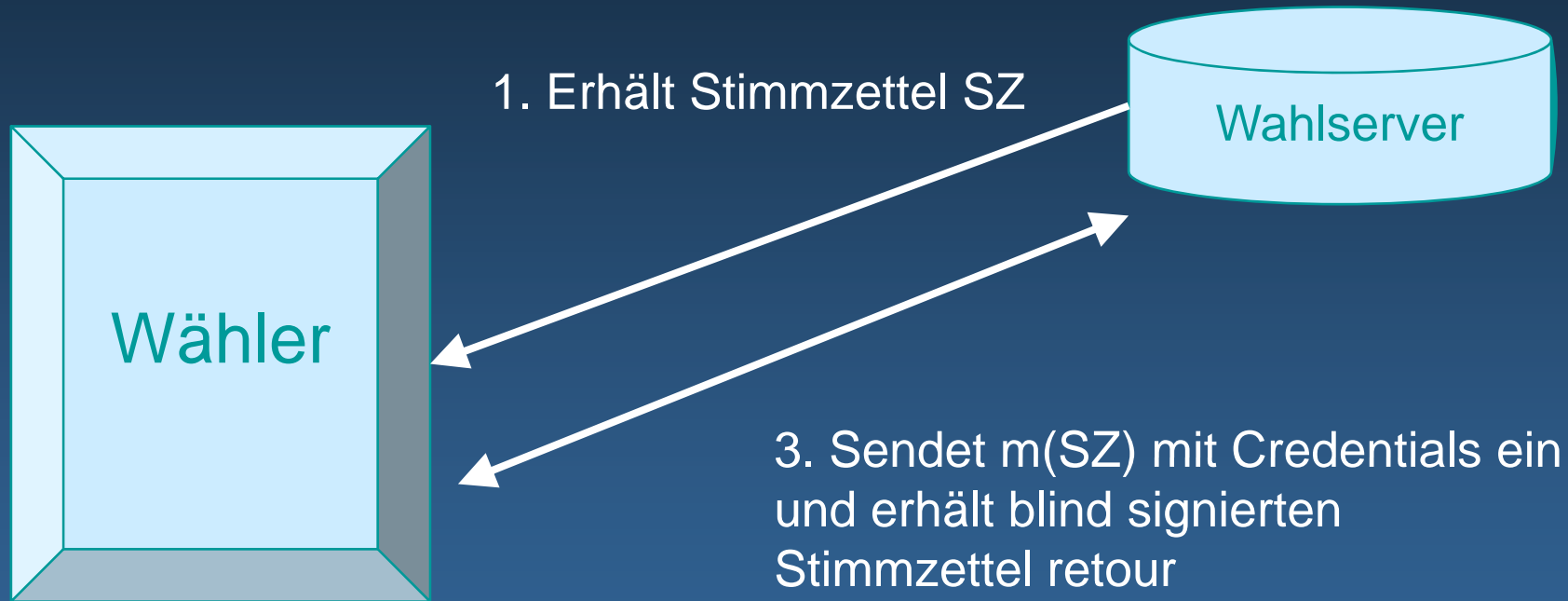


Blinde Signatur:

Blinde Signatur (kompletter Text):

1. Vorbereitung: $t * r^e$
2. Signatur: $(t * r^e)^d$
3. Entpacken: $(t * r^e)^d / r = t^d * r/r = t^d$
4. Prüfung: wie bei normaler Signatur

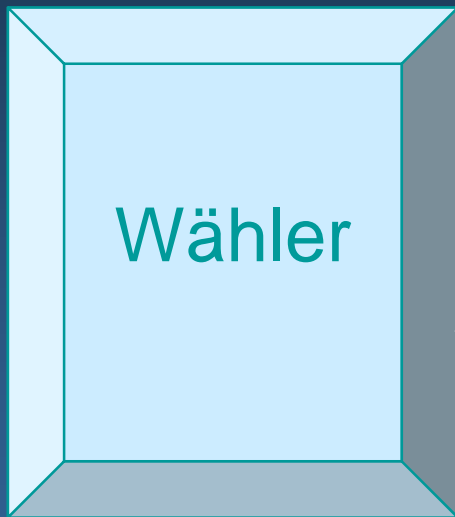
Blinde Signatur auf Stimmzettel:



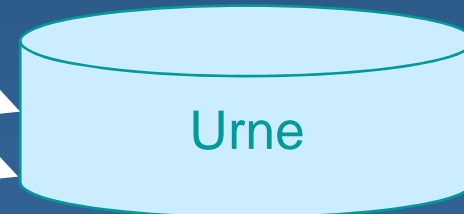
2. Füllt SZ aus, wählt (m, m') und verschlüsselt zu $m(SZ)$

Blinde Signatur auf Stimmzettel:

4. Entpackt $m(SZ)$



5. Reicht $m(SZ)$ ein
und erhält laufende Nummer n



6. Reicht m' und n ein



Blinde Signatur auf Stimmzettel:

Fujioka et al. (1993)

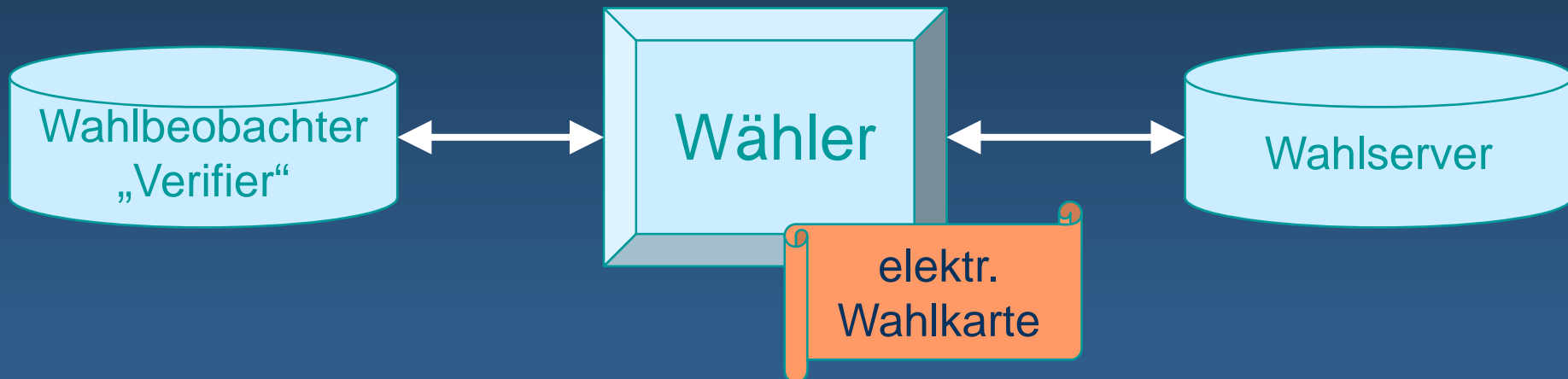
Sako (1994), Okamoto (1997)

Zahlreiche Implementierungen

Probleme mit Nachvollziehbarkeit und Robustheit

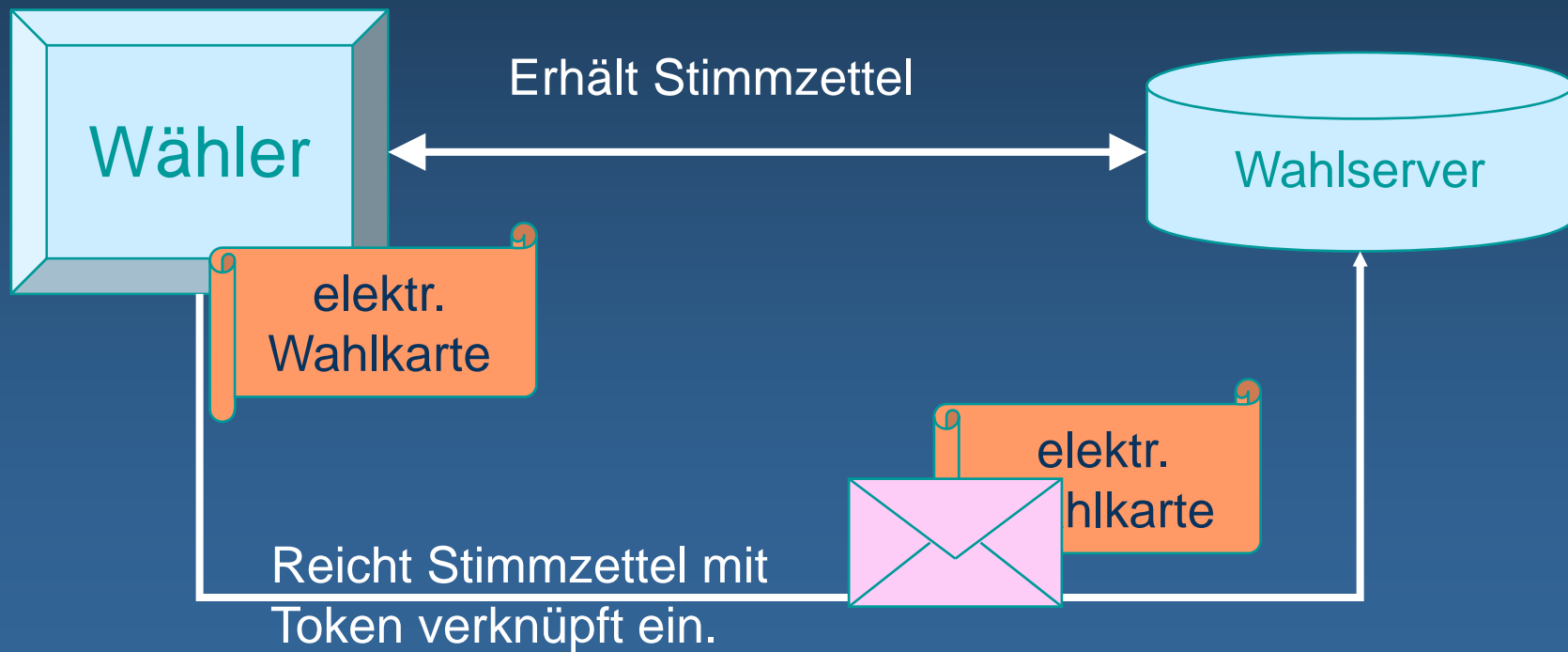
Blinde Signatur auf Token:

1. Lösen eines Token („elektronische Wahlkarte“):



Blinde Signatur auf Token:

2. Verwenden des Tokens:





Blinde Signatur auf Token:

Prosser und Müller-Török (2002)

Anonymisierung sehr gut

Auditierbar, mehrfache ersetzende Stimmabgabe

„Eingebaute“ Wahlbeobachtung

Zwei Interaktionen mit dem Wählenden

=> Prosser und Bagnato (2008) einstufig

Fragen der Implementierung

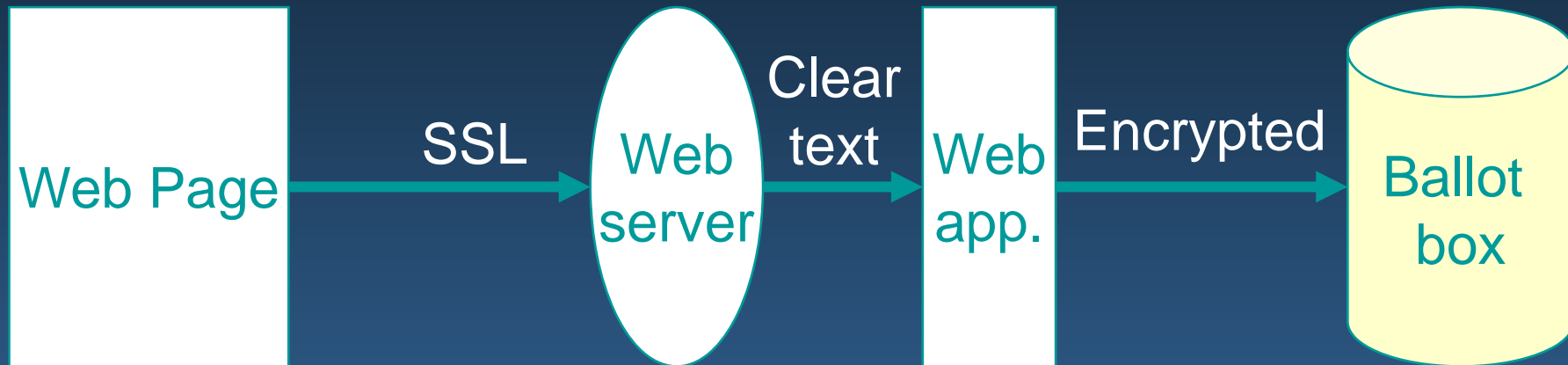
1. „Wahlclient“

2. Transparenz

Software

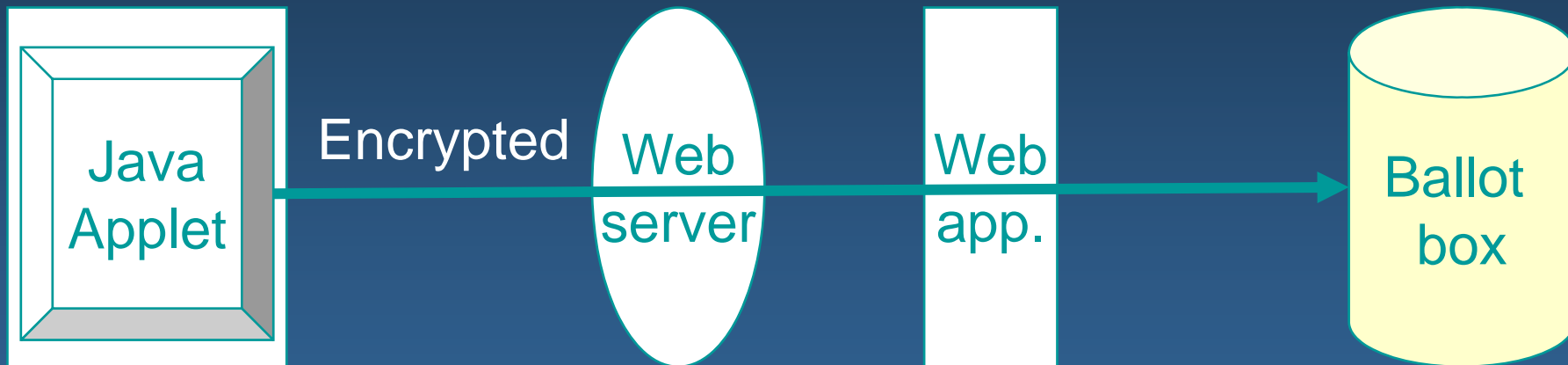
Systemumgebung

Standard web page



Falsifizierbare Hypothese:
Ohne Wahlclient sind Wahlrechtsgrundsätze nicht technisch (sondern nur organisatorisch) garantierbar.

(Java) voting client



„End-zu-End“ Verschlüsselung: WählerIn zu Wahlkommission

Fragen der Implementierung

1. „Wahlclient“

2. **Transparenz**

Software

Systemumgebung



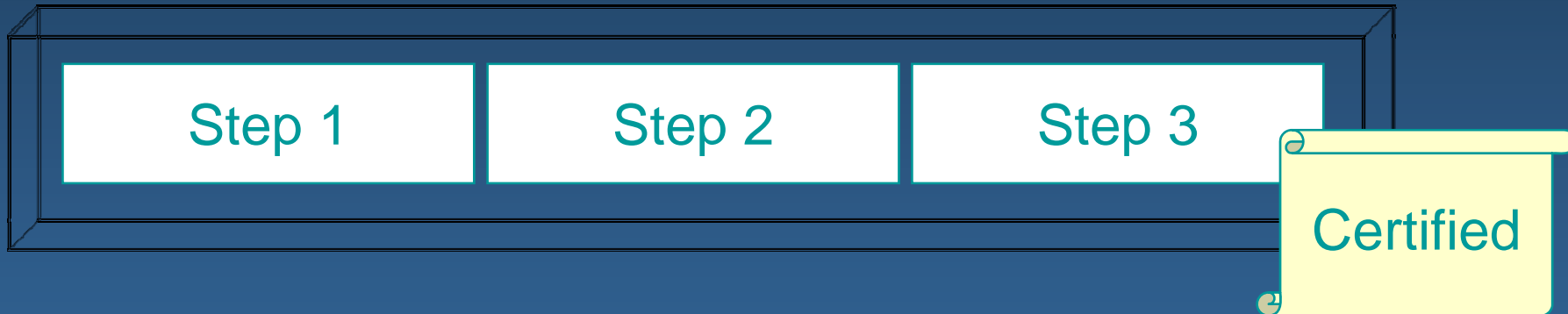
Beispiel U.K. 2007

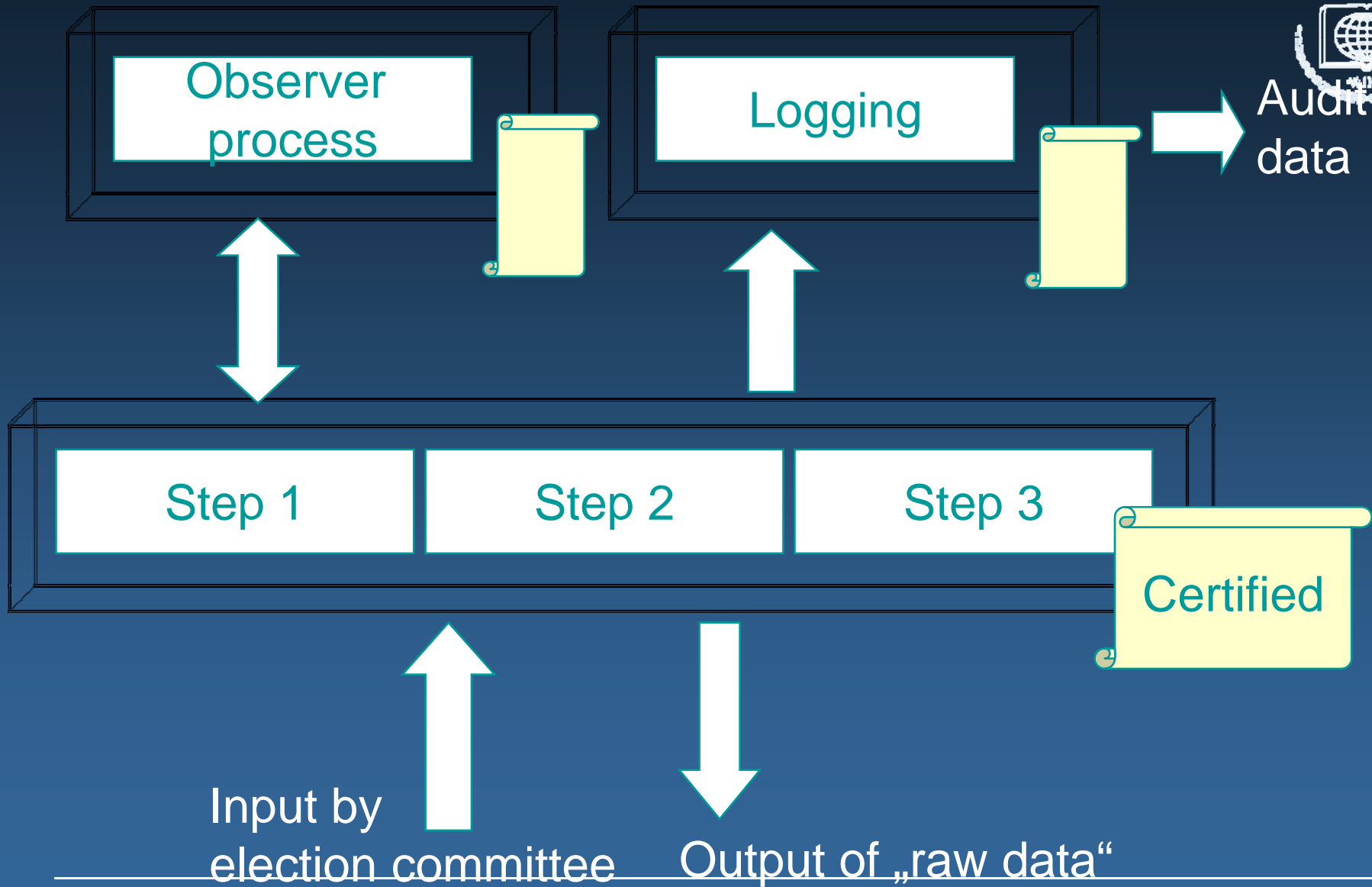
- “[...] the eBallot Box were downloaded from the hosting provider to a PC at the counting centre [...]. The contents were then copied to a CD and transferred to a separate PC without network connectivity. The eBallot Box was then opened. Ballot results and receipts were then exported onto CD and passed to a separate machine for counting. The opening of the ballots and mixing of the associated receipts was a process managed by [VENDOR] technical staff and required detailed knowledge of the software to complete (e.g. command line processing of software functions).”
- “However, the import of evoting results into the vote tallying application [...] identified errors in the underlying data records for a small number of ballots. These errors prevented the import of any e-voting results until the issue was resolved. [...] Once the reason for the error was identified the affected ballots were modified manually before the import process could continue.”



Missverstandene Transparenz (=manuelle Bearbeitung)







Fragen der Implementierung

1. „Wahlclient“

2. **Transparenz**

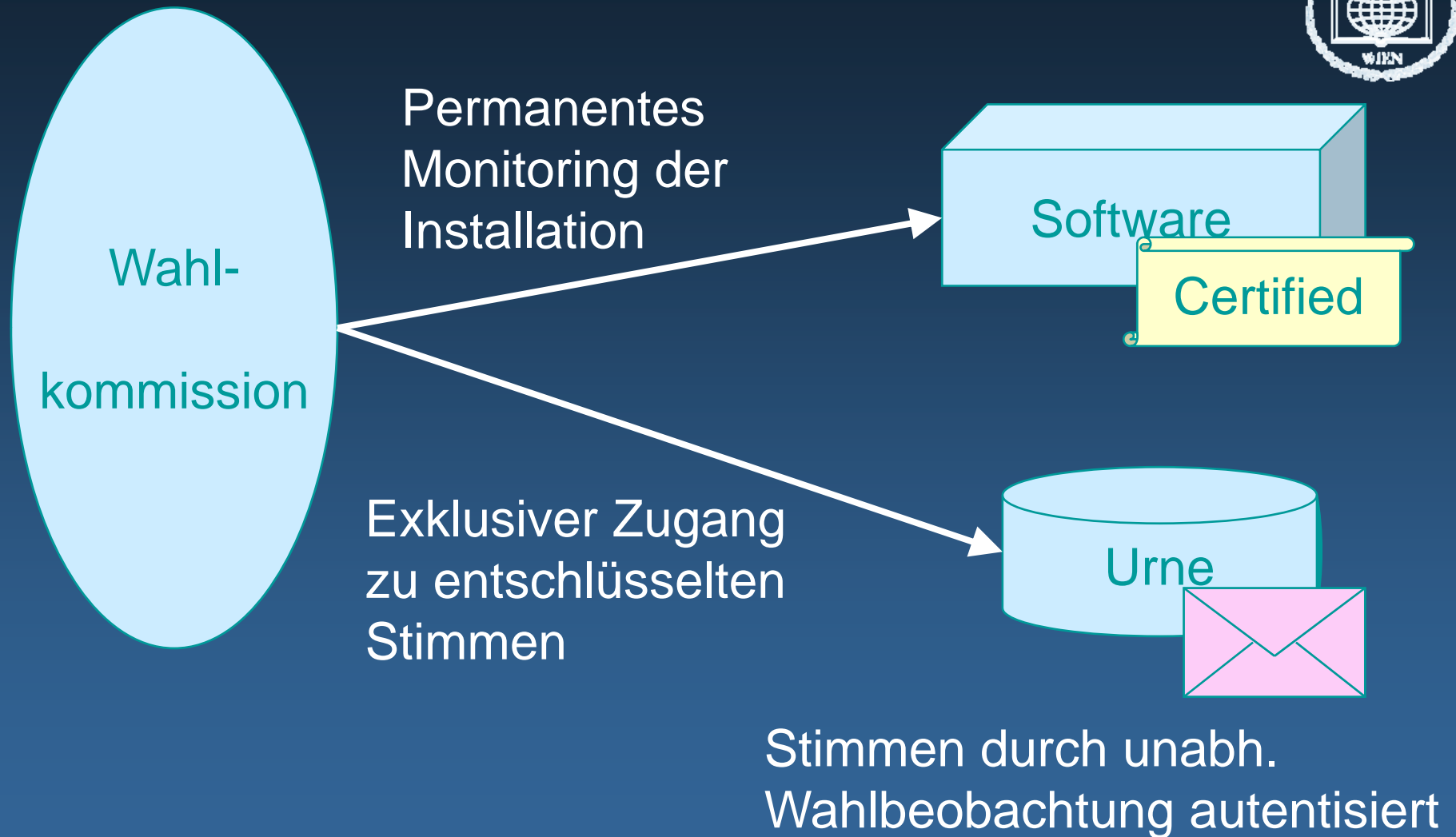
Software

Systemumgebung



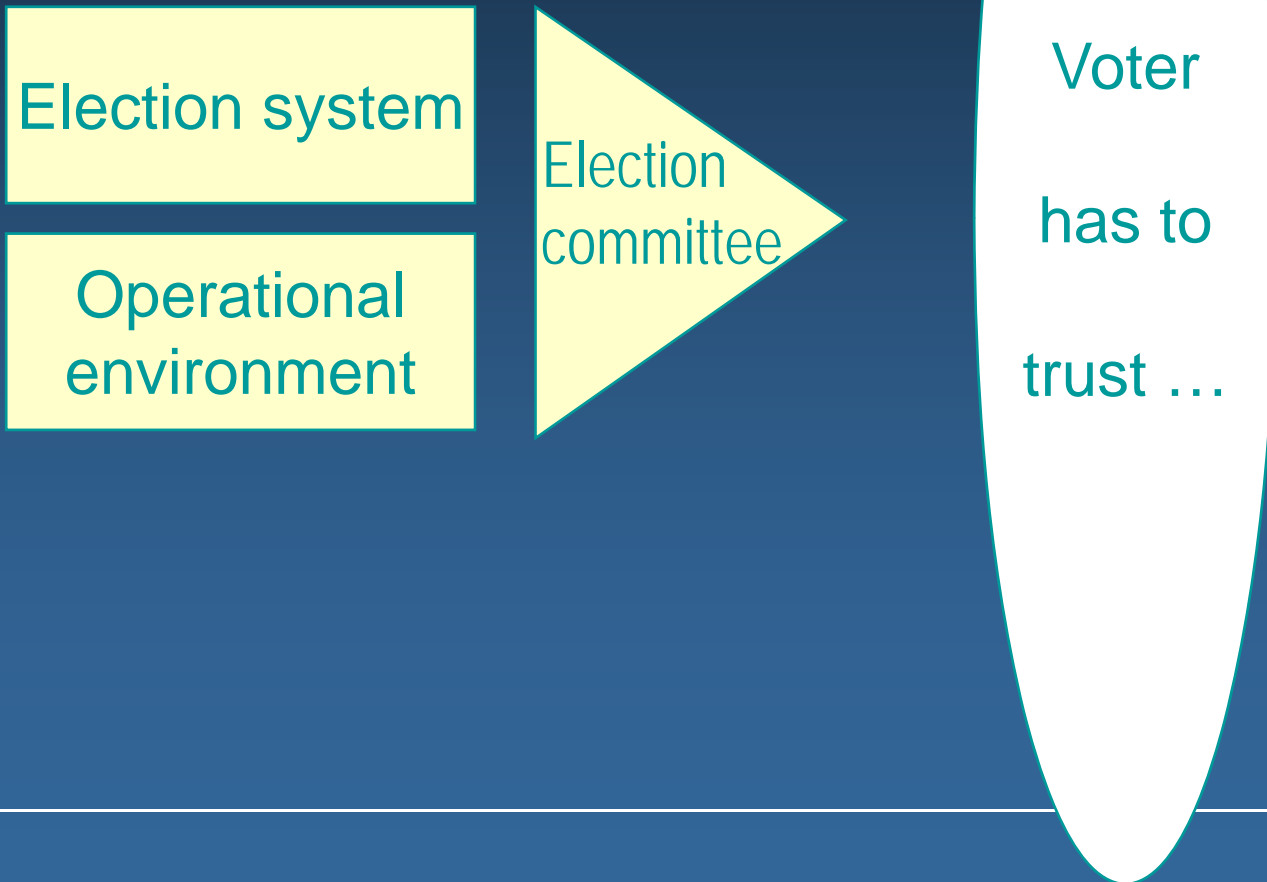
Beispiel U.K. 2007

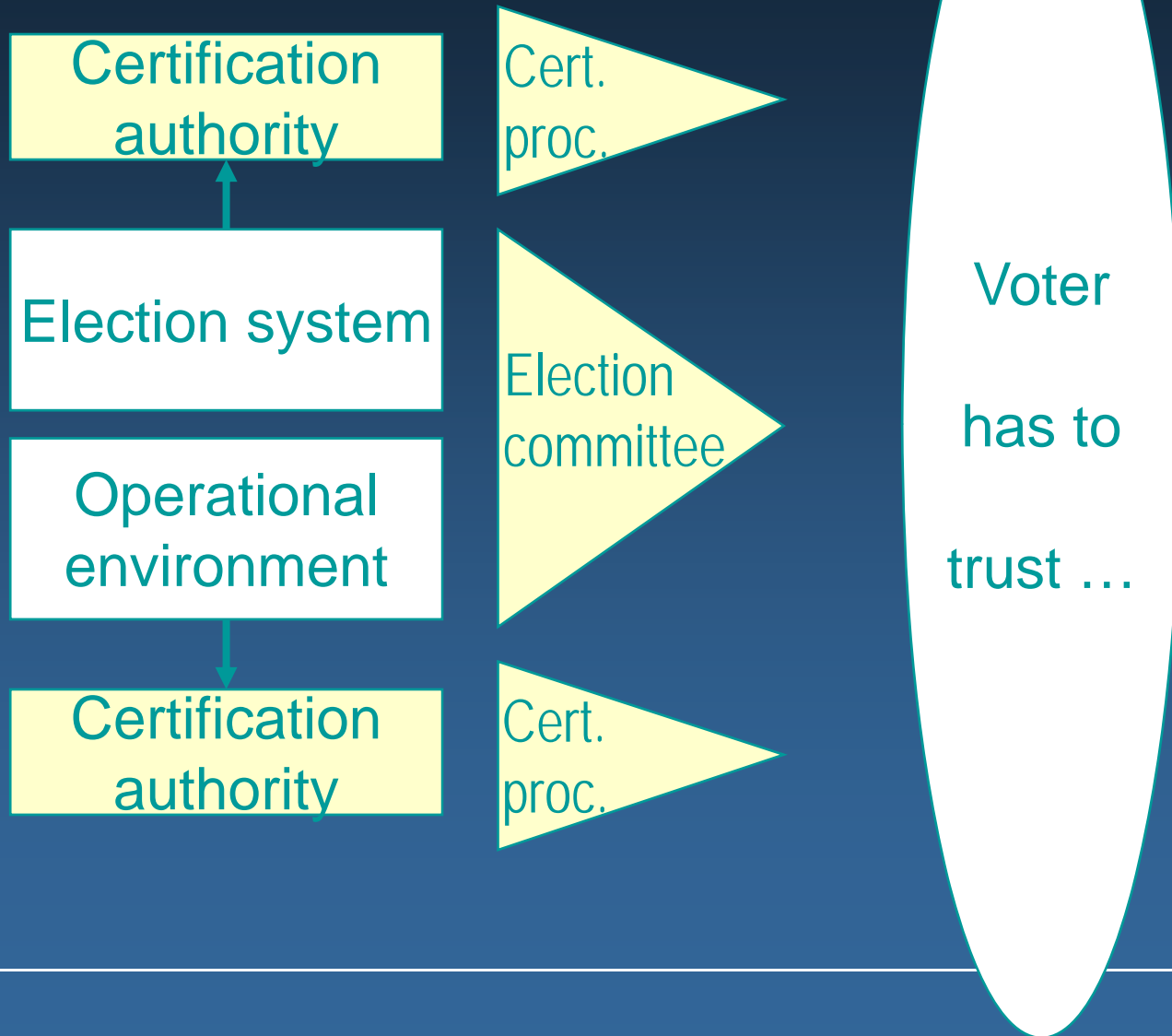
- In [...] technicians were observed using a USB key to transfer files between computers.
- In [...] a submission from a party present at the count indicates that files and directories had to be moved around and even deleted to restore software operation.
- [Election] observers were not permitted to view the servers holding ballots nor approach the floor they were held on [...]. In the case of [...] very few details of their server setup were shared [...].

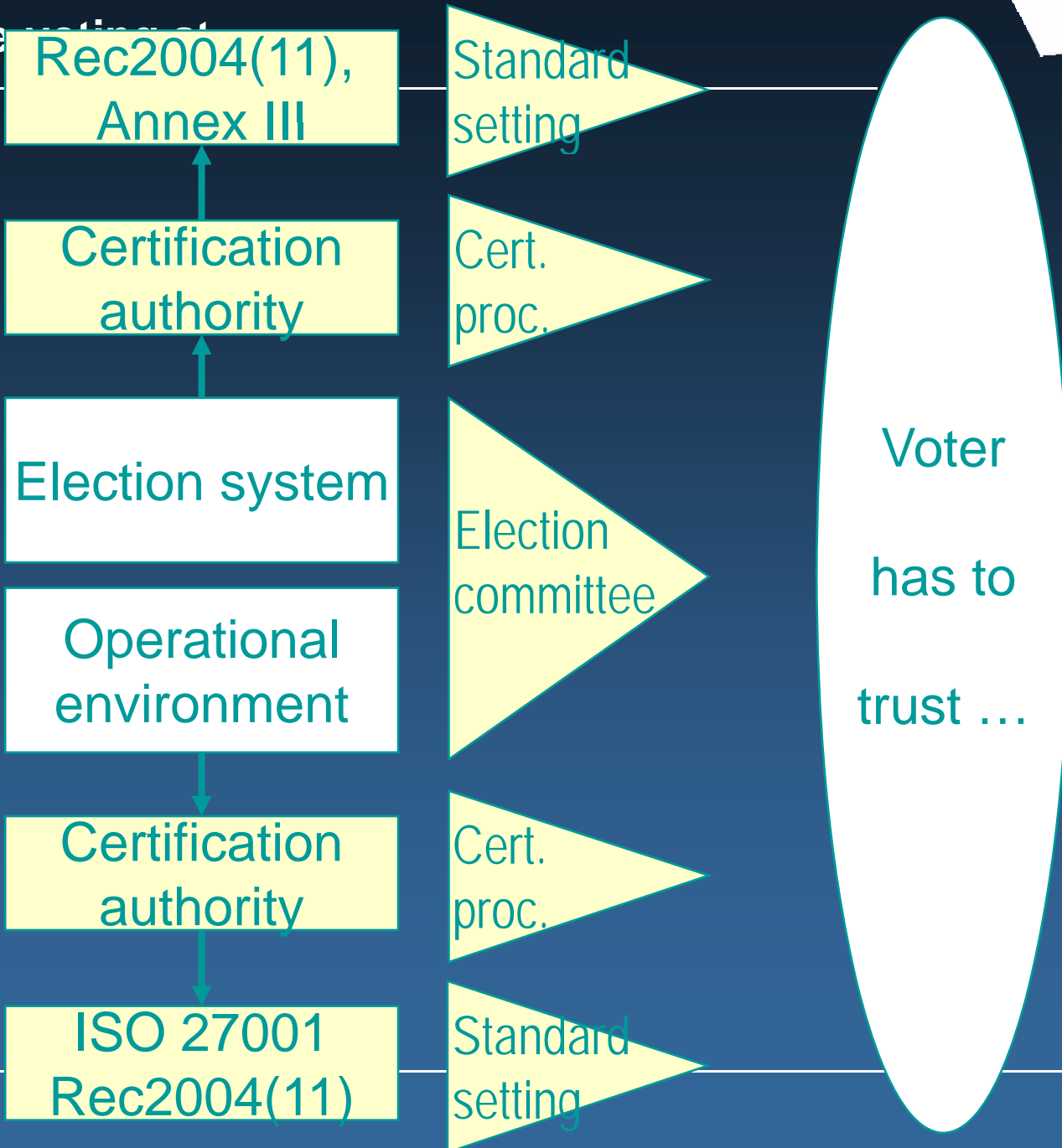




Vertrauen







<http://e-nitiative.at>

Rec2004(11),
Annex III

Standard
setting

Certification
authority

Cert.
proc.

~~Election system~~

Election
committee

~~Operational
environment~~

Certification
authority

Cert.
proc.

ISO 27001
Rec2004(11)

Standard
setting

Voter
has to
trust ...





Warum eVoting ?

**Falsifizierbare Hypothese:
eVoting ist sicherer als die Briefwahl**

**Damit ist die Frage eVoting j/n gleich
der Frage Distanzwahl j/n**

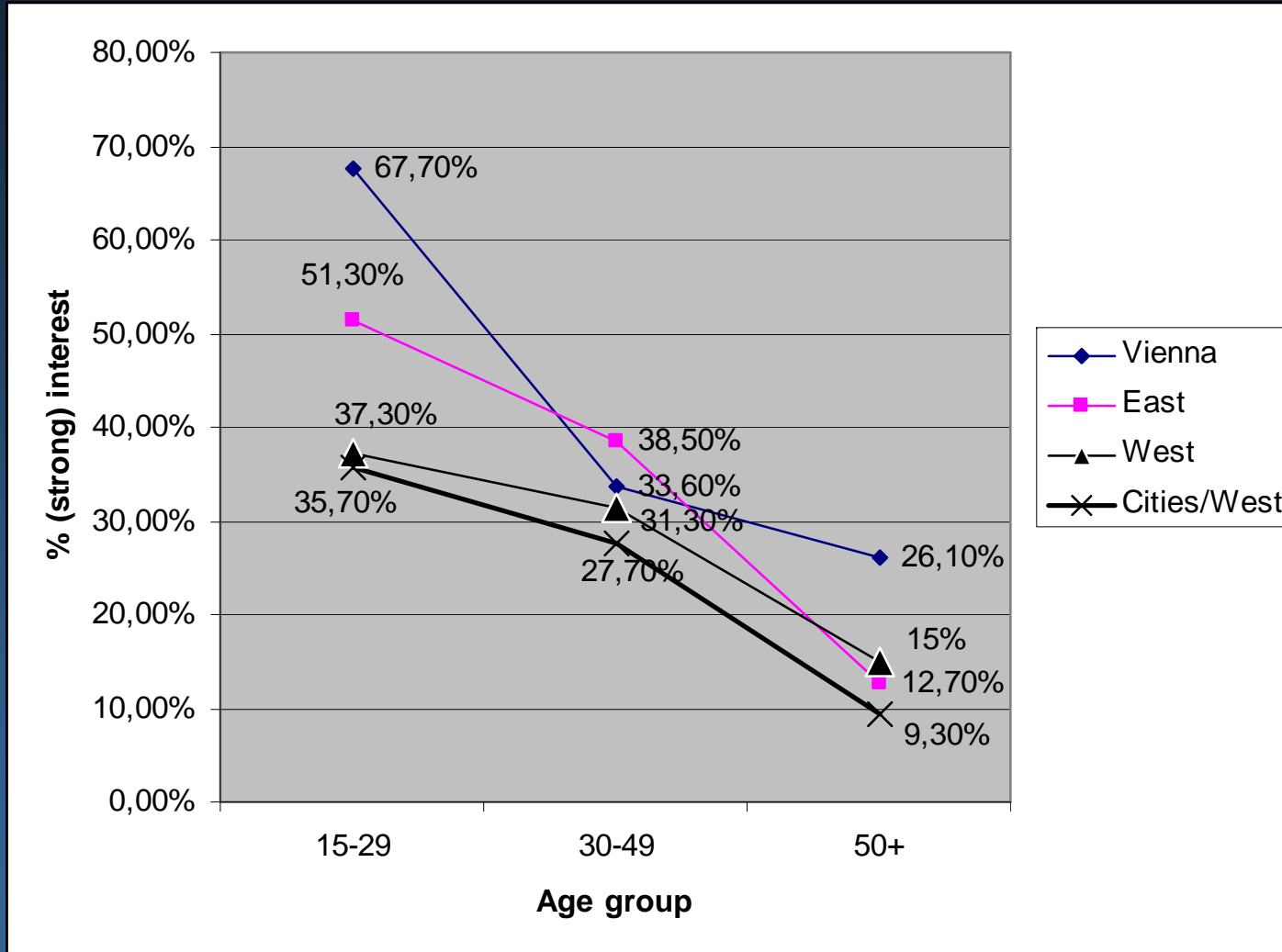


Daten Erhebung 2007 (Straßeninterviews):

	2007		2004	
	<i>Interest eVoting</i>	<i>Interest ePart.</i>	<i>Interest eVoting</i>	<i>Interest ePart.</i>
Vienna	38,00%	14,90%	44,00%	14,00%
East	30,70%	16,40%		
Cities West	21,80%	10,10%		
West	26,70%	12,10%		

Overall: 29,9% (n=1500)

Vienna: n=297, Cities West: n=129, (Rural) West: n=554, (Rural) East: n=520;
Vienna 2004: n=300





Bereitschaft Wahlkanal „in Zukunft“ zu verwenden:

Wahllokal:	85,1%
Briefwahl:	45,9%
SMS:	15,0%
Vorauswahl:	18,3%
Internetwahl:	37,7%

Österreichweit, n=1500

Fazit:



Die Anforderungen an eVoting-Systeme sind bekannt und kodifiziert (Rec 2004(11)).

Die Schwierigkeiten, die bei Piloten bisher aufgetreten sind, sind unnötig.

=> Verfahren

=> Software Engineering (vom Entwurf weg)

=> QS und Zertifizierung

Distanzwahl ist logische Konsequenz einer mobiler werdenden Gesellschaft.

Einsatzgebiete eVoting:

- => Kein Ersatz für „Wahlsonntagsszenario“
- => wo Distanz überbrückt werden muss
- => wo Wahlen an Werktagen stattfinden
- => wo bisher ausschließlich Distanzwahl eingesetzt wird

„eDemokratie-Paket“:

=> eDeliberationsplattformen

- Politik
- Verwaltungsverfahren

=> eKonsultationen

=> eAbstimmungen