Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Algorithm: GenPermutationCommitment$(\psi, \mathbf{h})$

Input: Permutation $\psi = (j_1, \ldots, j_N) \in \Psi_N$
Independent generators $\mathbf{h} = (h_1, \ldots, h_N)$, $h_i \in \mathbb{G}_q \backslash \{1\}$

for $i = 1, \ldots, N$ **do**
  $r_{j_i} \in_R \mathbb{Z}_q$
  $c_{j_i} \leftarrow g^{r_{j_i}} \cdot h_i \bmod p$

$\mathbf{c} \leftarrow (c_1, \ldots, c_N)$
$\mathbf{r} \leftarrow (r_1, \ldots, r_N)$
return $(\mathbf{c}, \mathbf{r})$

Process Models for Universally Verifiable Elections

Rolf Haenni, **Eric Dubuis**, Reto E. Koenig, Philipp Locher

E-Vote-ID 2018, Bregenz, Austria

▶ Bern University of Applied Sciences BFH, Switzerland

Research Questions

- Only little experience exists for conducting verification processes
- Lack of common understanding of the exact purpose of a verification

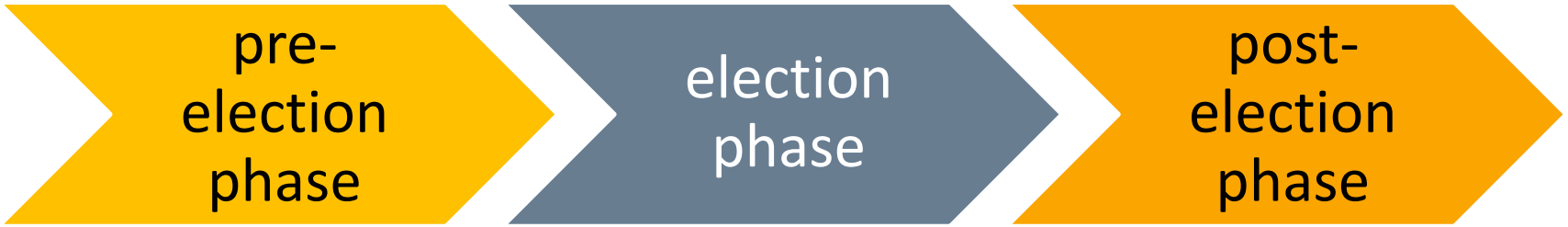
  - What is the exact nature/essence of a verification process?
  - What are its necessary input data elements?
  - What are possible verification results?
  - How differ hybrid election processes from a single-channel election process?

Outline of the Talk

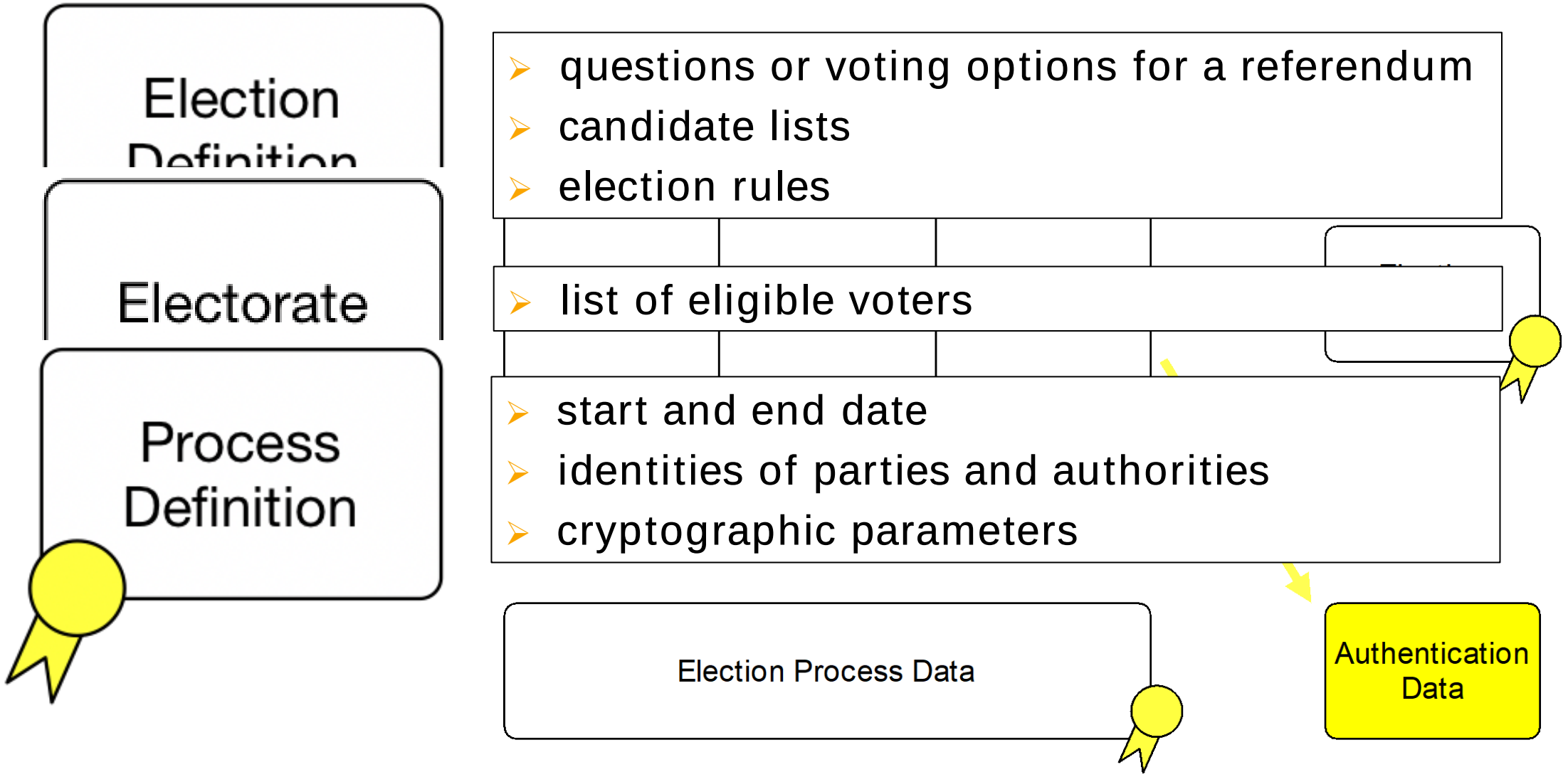
- Single-Channel Election Process
  - An Election Process Model
  - Verification Process
  - Test Categories
  - Impact of Failed Tests
  - (side track) On Developing a Verifier
- Hybrid Channel Election Processes
  - Extension of the Election Process Model
  - Extension of the Verification Process
  - Composing Election Process Models
- Conclusion

Single Channel Election Process

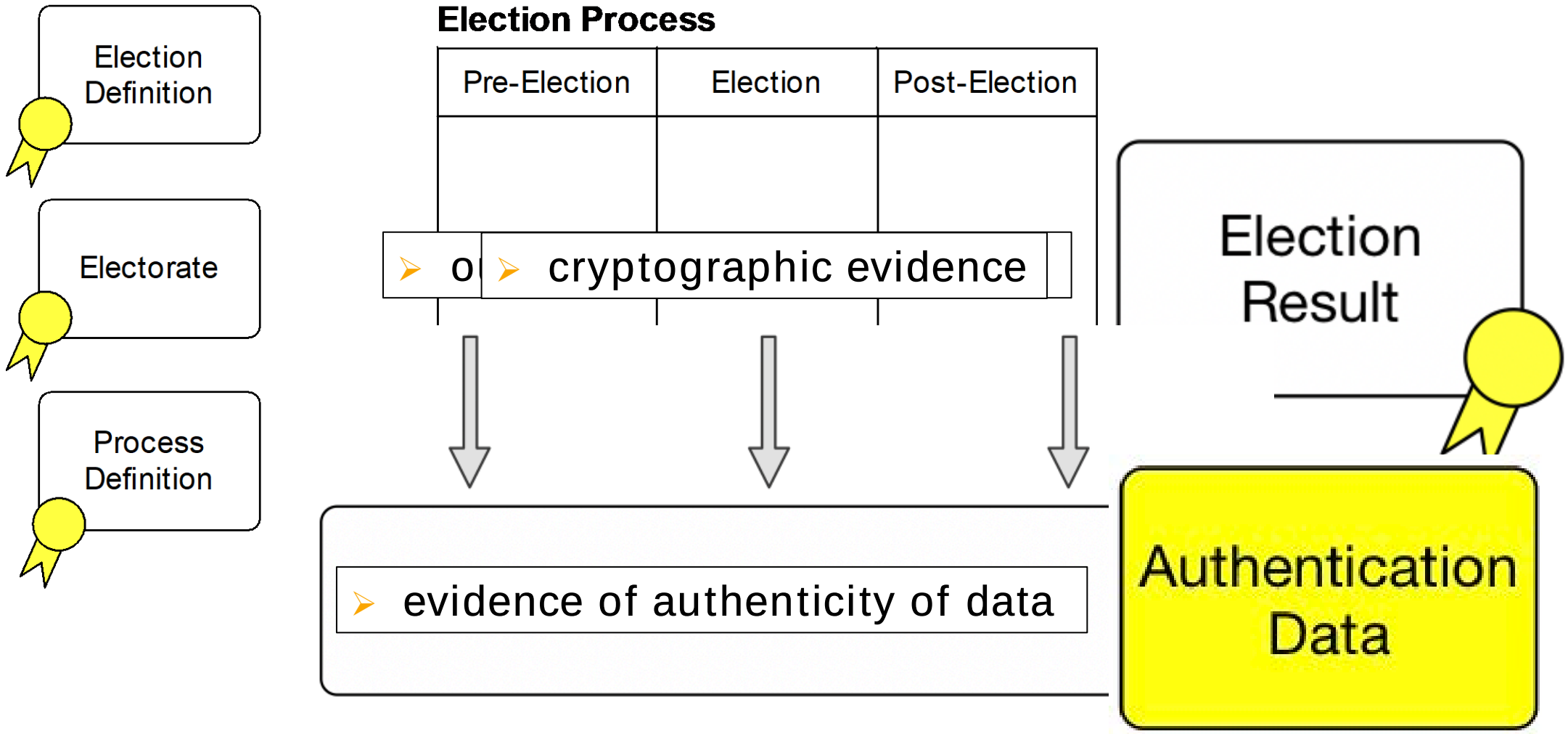
From a Simplified Election Process Model...



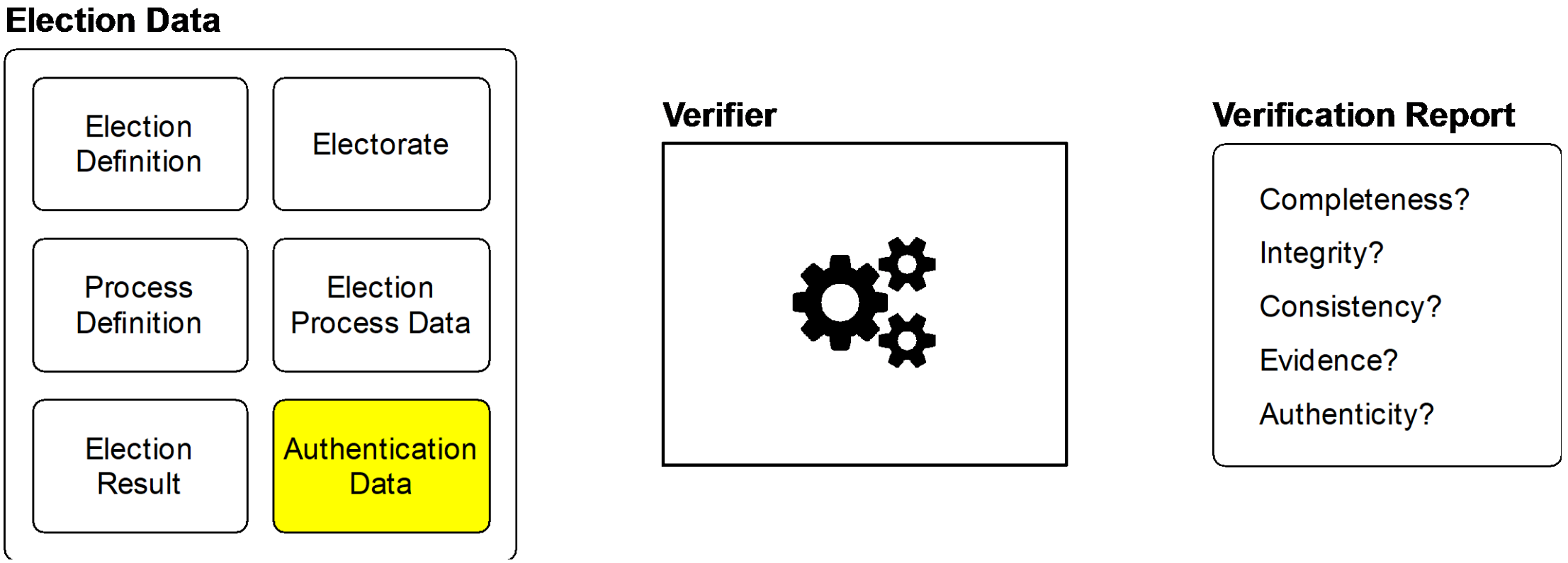
… to a More Elaborated, Detailed Election Process Model



… to a More Elaborated, Detailed Election Process Model

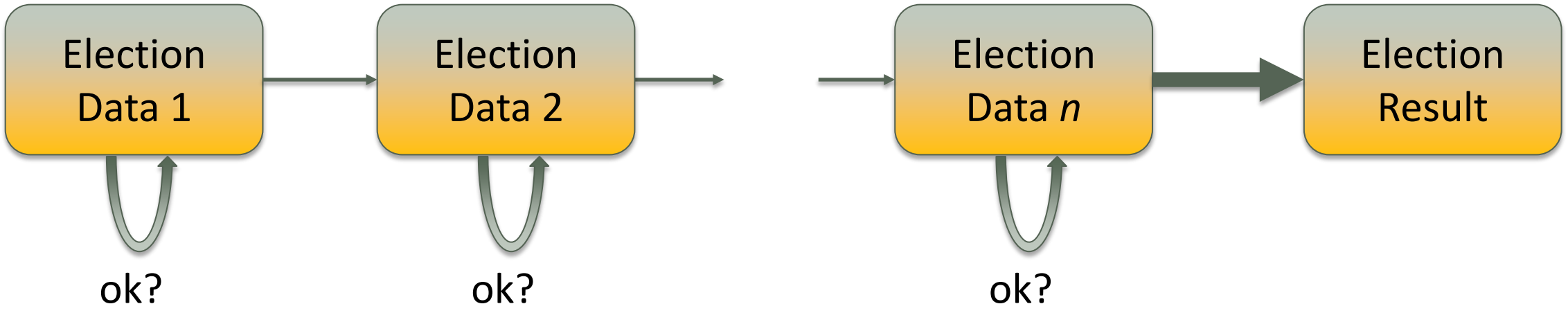


Verification Process



Verification Process Leads to a “Verification Chain”

- A series of tests...
- ... combined together give evidence...
- ... shows that the election result is correct.



Outcome of the Verification Process

Completeness

- Cover data elements the whole election process?
- Data elements sufficient for complete verification chain?

Integrity

- Data elements correspond to the protocol specification?
- Data elements within specified range?

Consistency

- Related data elements consistent with each other?

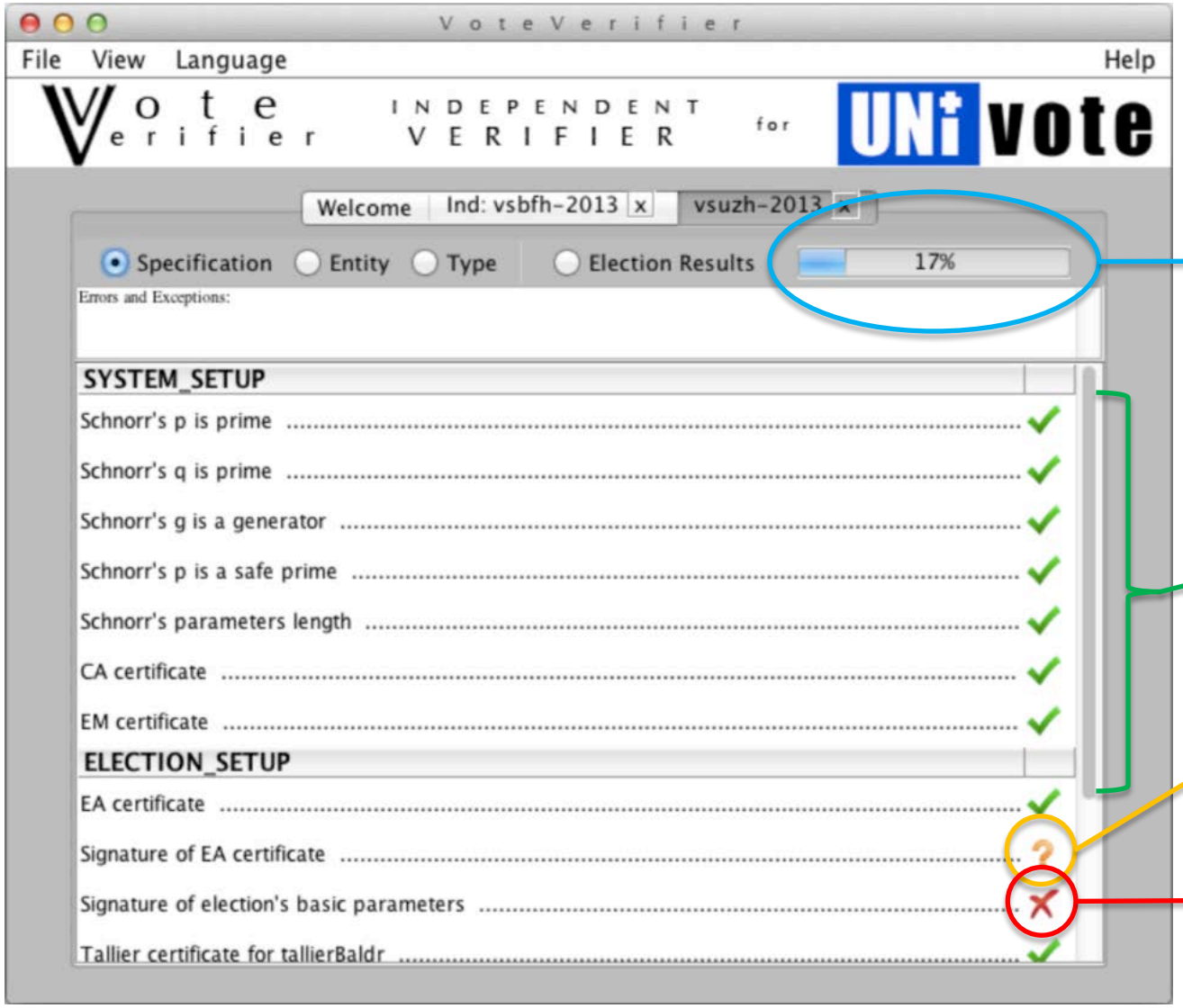
Evidence

- Cryptographic proofs correct?
- Allow to infer the correctness of respective protocol step?

Authenticity:

- Data elements linkable to authorized parties?

Sample of a User Interface of a Verifier



- verification is in progress
- successful verification tests
- verification step dropped due to missing certificate
- failed signature test

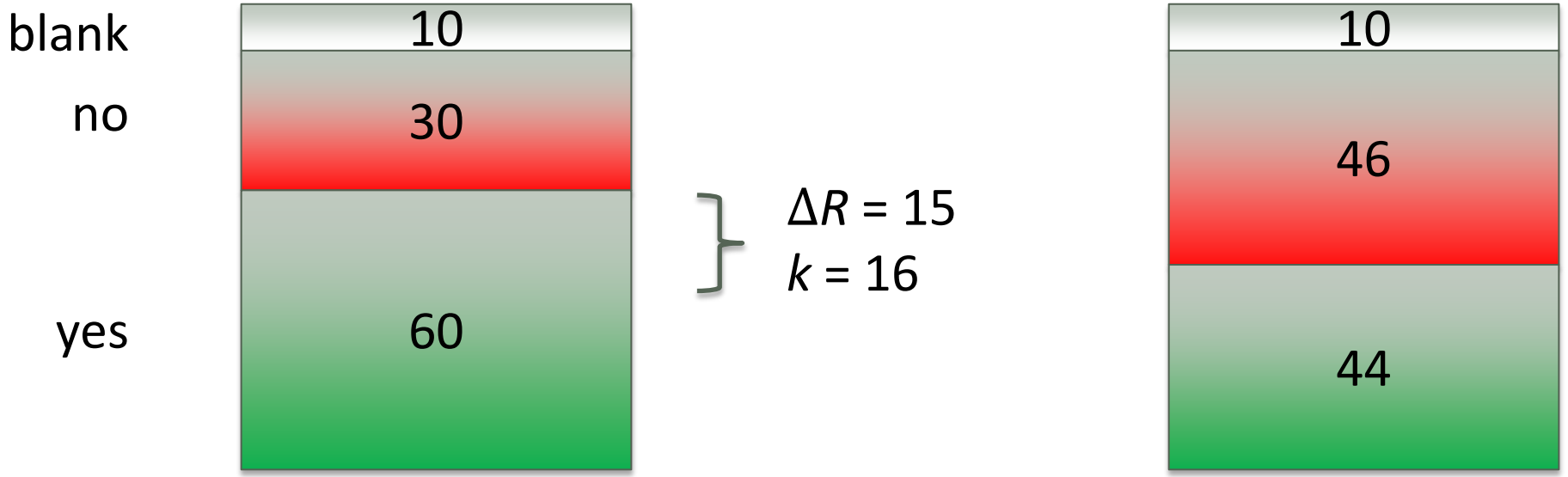
Impact of Failed Tests

3 evaluation criteria

- Maximum number of affected votes?
- Violated security goal?
- Recovery possible via repeating some steps of election process?

1st Evaluation Criterion: Impact of *k* Affected Votes

- *N* votes in total
- *k* affected votes, $0 \leq k \leq N$
- Let ΔR, $1 \leq \Delta R \leq N/2$, be the amount of affected votes to change the outcome
- If $0 \leq k < \Delta R$ ➔ invalidation of election (perhaps) not justified
- However, if $k \geq \Delta R$ then repetition of election cannot be avoided



2nd Evaluation Criterion: Security Goal Violation

If a test fails relative to a single submitted vote, which security goal is violated?

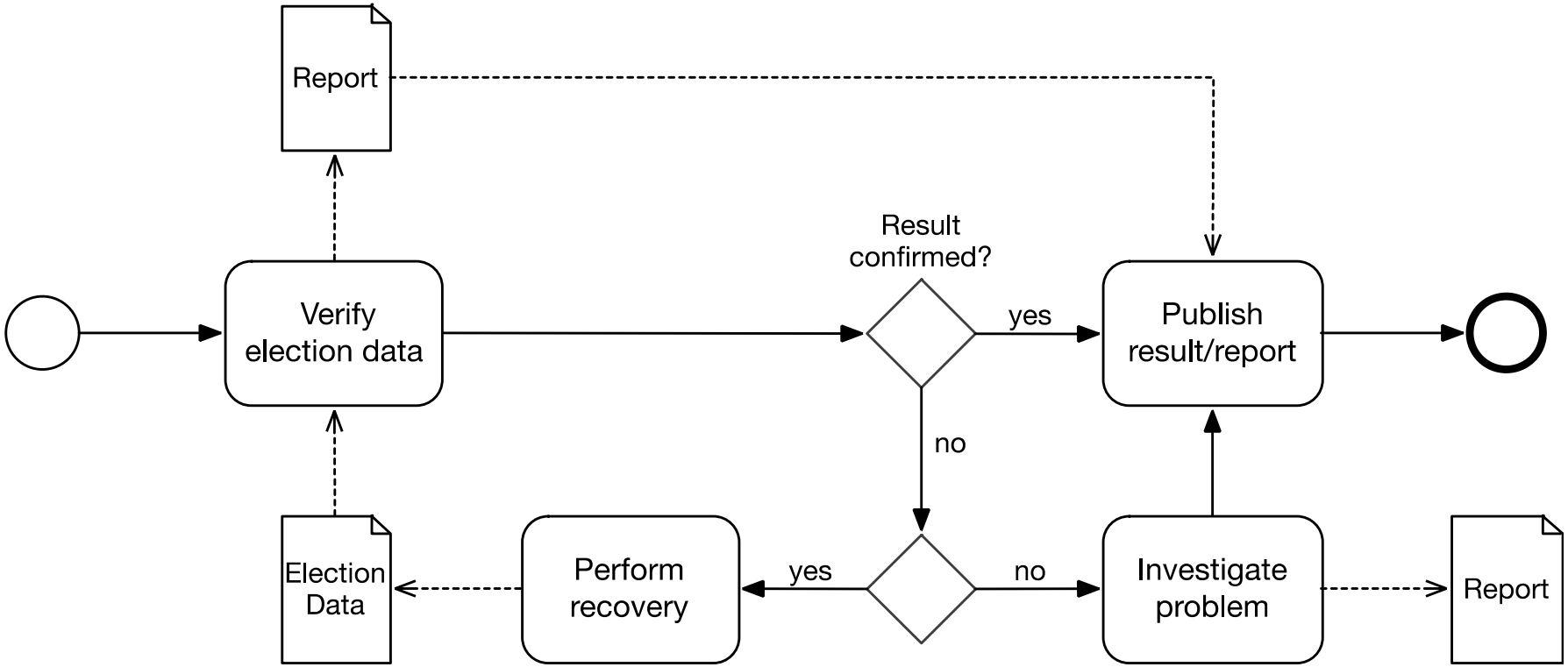
- Vote secrecy?
- Vote integrity?
- Vote secrecy & integrity?

1st and 2nd Evaluation Criteria Combined

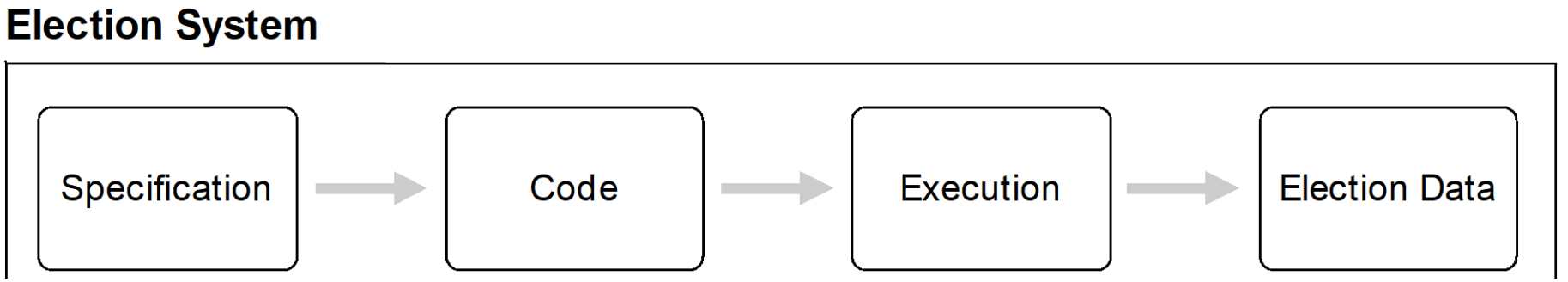
	Vote Secrecy	Vote Integrity	Vote Secrecy & Integrity
k=0	Result confirmed	Result confirmed	Result confirmed
$k < \Delta R$	Result confirmed Initiate investigation Stop using the system	Result questionable Initiate investigation Stop using the system	Result questionable Initiate investigation Stop using the system
$k \geq \Delta R$	Result confirmed Initiate investigation Stop using the system	Result not confirmed Initiate investigation Stop using the system	Result not confirmed Initiate investigation Stop using the system

3rd Evaluation Criterion: Repeating some Steps

- If signature is missing, can signature generation be repeated?
- …



On Developing a Verifier



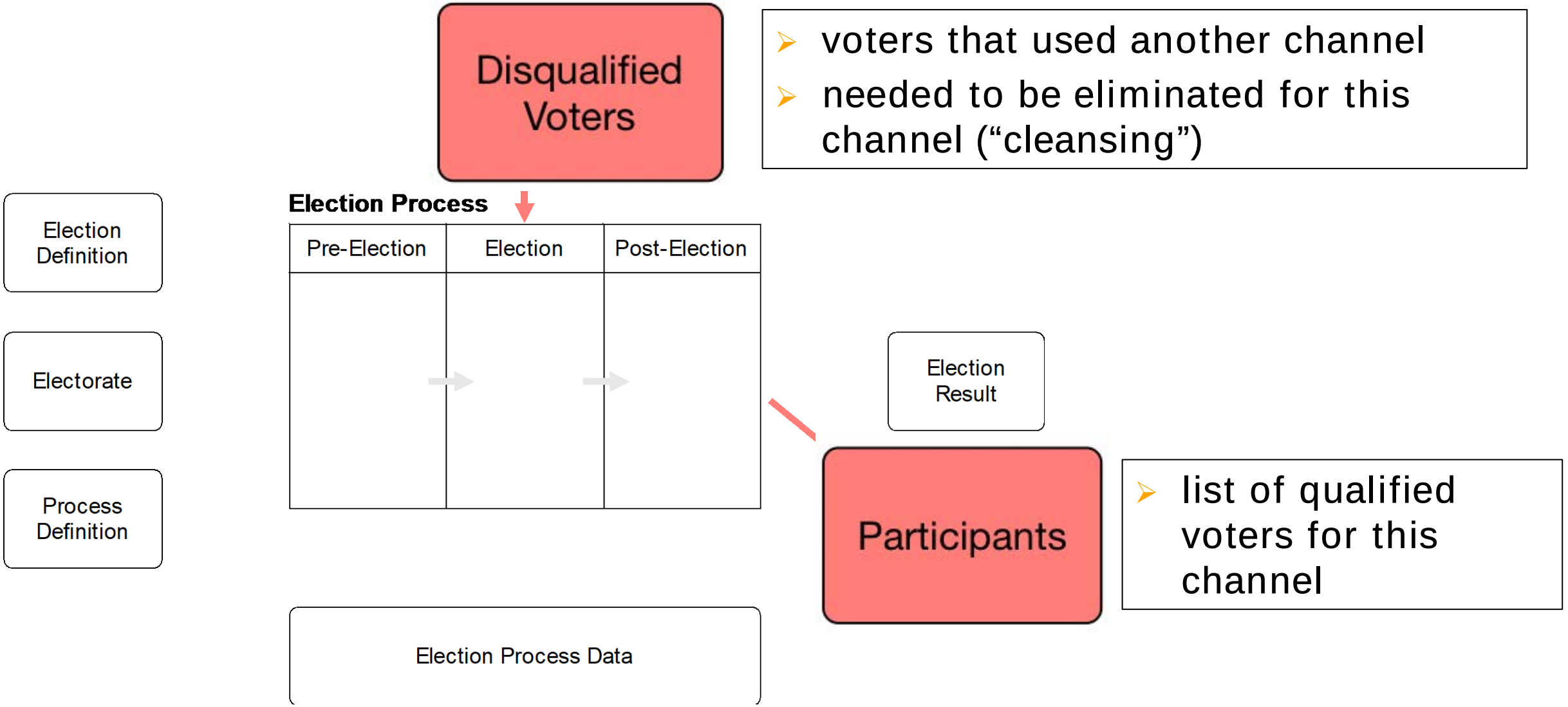
Hybrid Election Processes

Multiple Channels

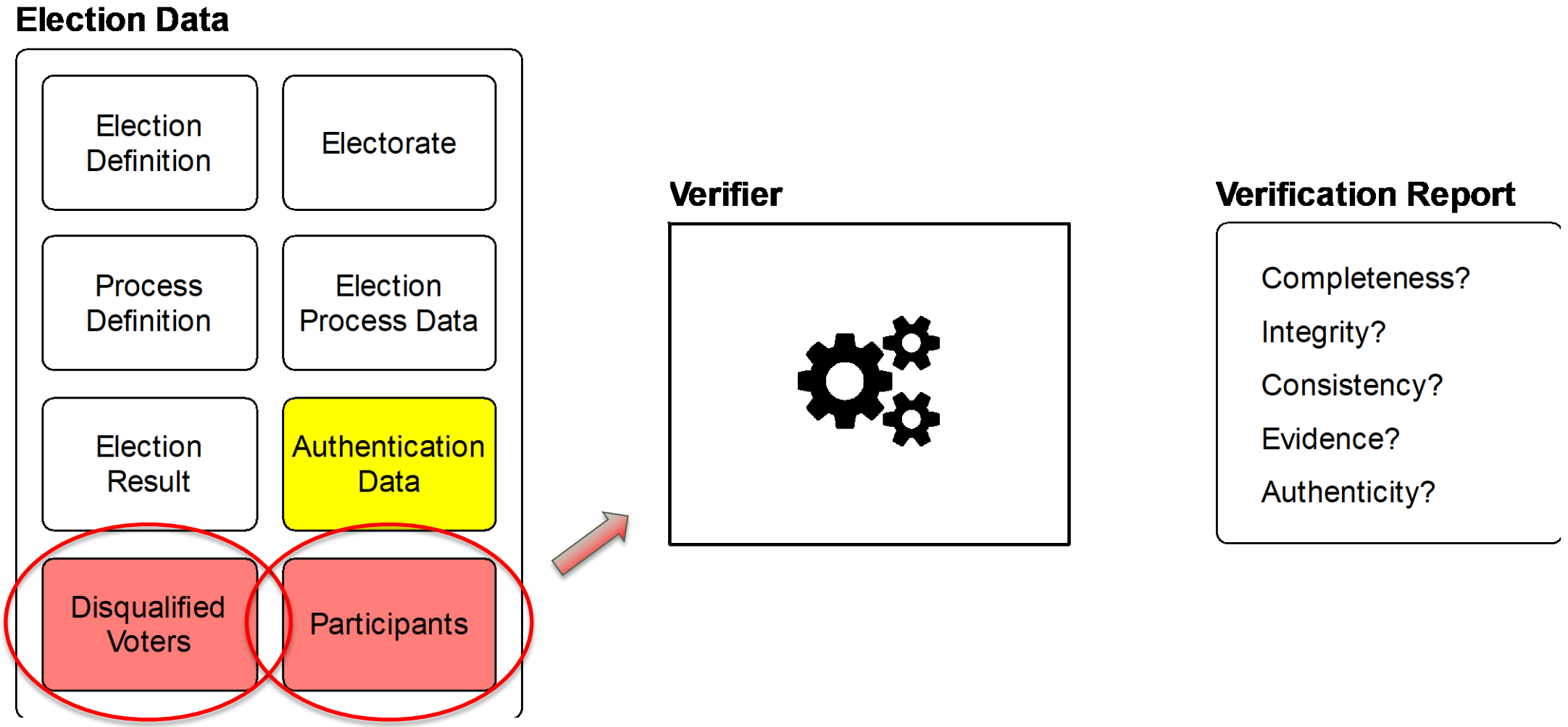
- Multiple channels to cast votes
- Voters can choose their preferred channel
  - Prior to an election ➔ easy
  - Spontaneously ➔ hybrid election process

- How to conduct the verification of the electronic votes, if postal voting or in-person voting is in place simultaneously?

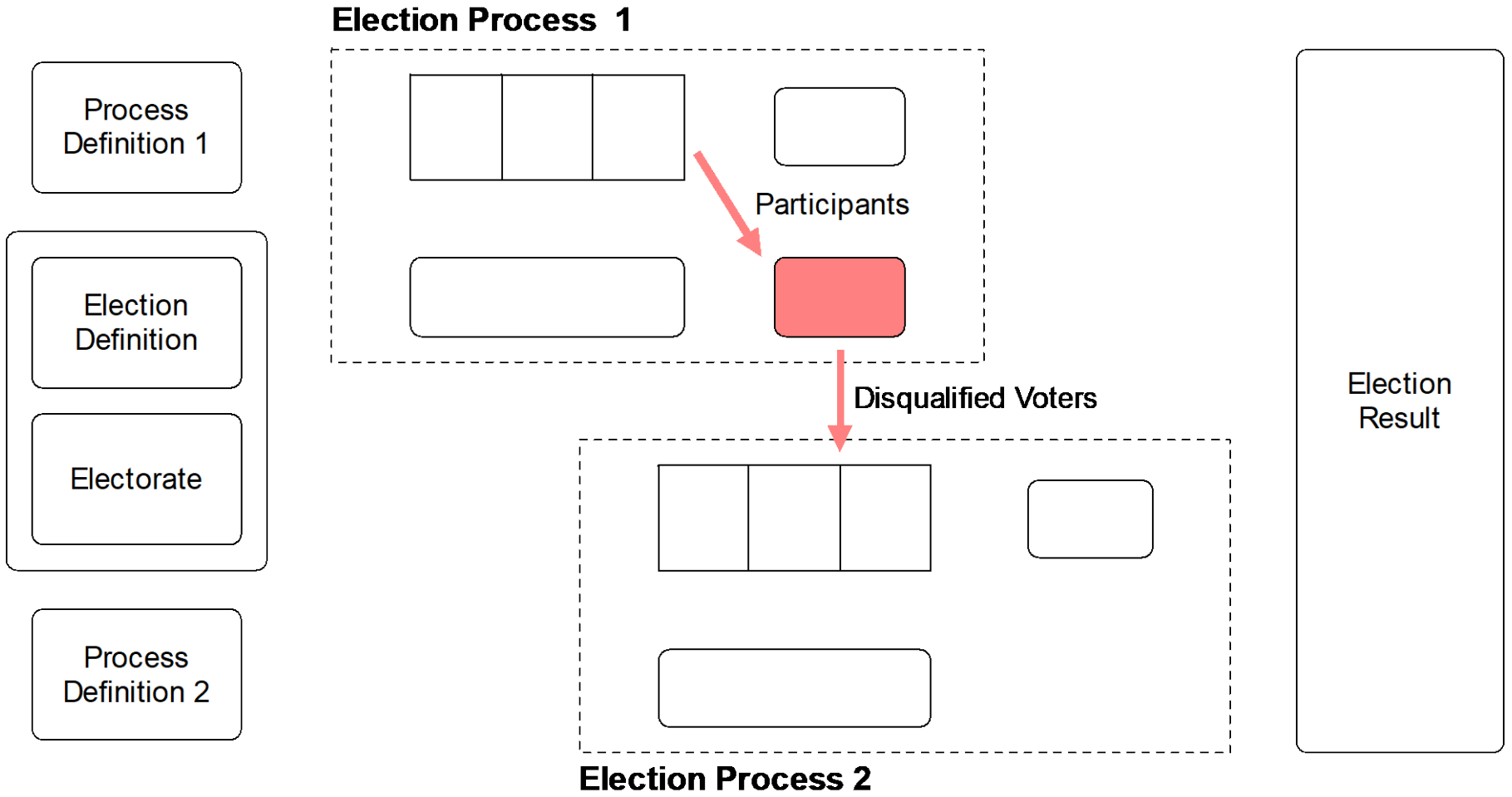
Extension of the Election Process – Cleansing



Extension of the Verification Process

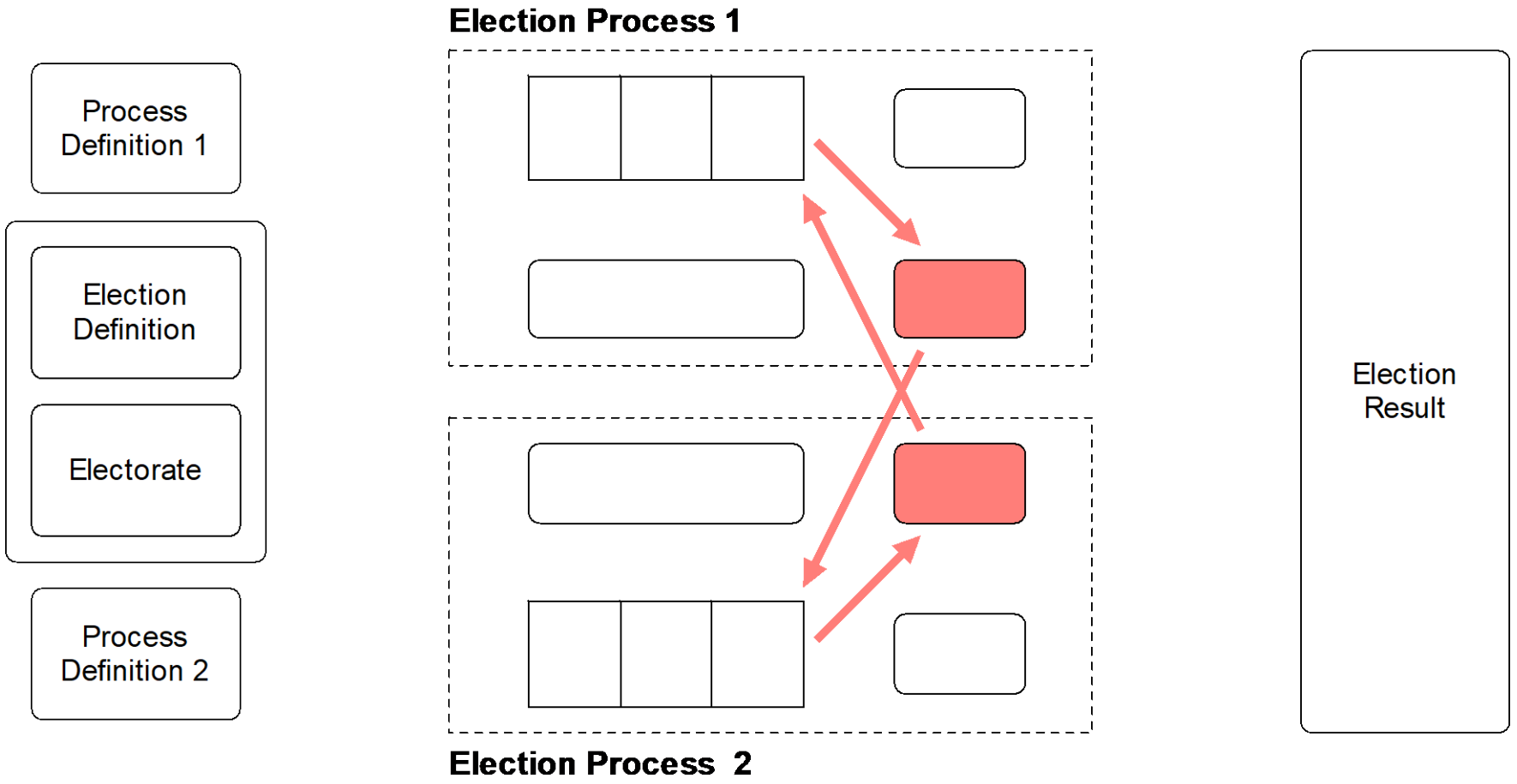


Composing Election Processes: Serial Composition



- temporal availability is exclusive
- election period of EP 1 strictly precedes the election period of EP 2
- list of participants of EP 1 defines disqualified voters for EP 2

Composing Election Processes: Parallel Composition



- temporal availability is ***not*** exclusive
- election period of EP 1 and EP 2 ***overlap***
- data exchange between the channel is ***mutual***
- voter may appear in both channels ➔ ***prioritization*** needed

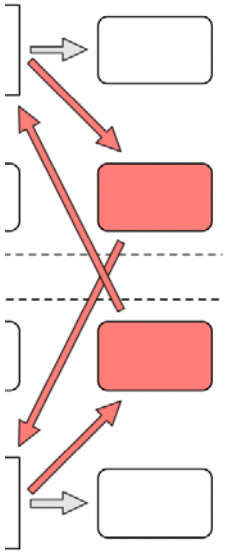
Prioritization Policies (I)

- **Prioritization of the physical channel**
  - Paper votes can be counted regardless the list of participants of the electronic channel
  - Double-vote elimination only relevant for the electronic channel
  - Current practice in Switzerland

- **Prioritization of the electronic channel**
  - Rules apply in the opposite way
  - Makes counting in the polling station more complicated
    E.g., separating paper ballots from the signed right-to-vote identity card

Prioritization Policies (II)

- **Prioritizing the First or the Last Submitted Vote**
  - Most complicated, since channels are mutually dependent
  - Requires exchange lists of participants
    - “single-step”, at the end of the election phase
    - dynamically
      - requires the adding of ***timestamps*** to the lists of participants



Conclusion

Conclusion / Take away

- "Verification" means to establish a "***verification chain***"
  - Various kinds of election data serves as input
  - In order to 100% correct, a series of tests must be satisfied for all data elements
  - Impact of failed tests
  - Developing a verifier ➔ a formal, public specification of the verification software is needed
- Hybrid channel election processes
  - Introduced ***extensions*** of the election process model and the verification process
  - Our model allows to ***recursively compose*** election processes in order to accomplish hybrid election processes

Thank you

Berner Fachhochschule
RISIS, E-Voting Group
Switzerland