swiss e-voting
competence center

Swiss E-Voting Workshop 2010

Verifiability in Remote Voting Systems

September 2010

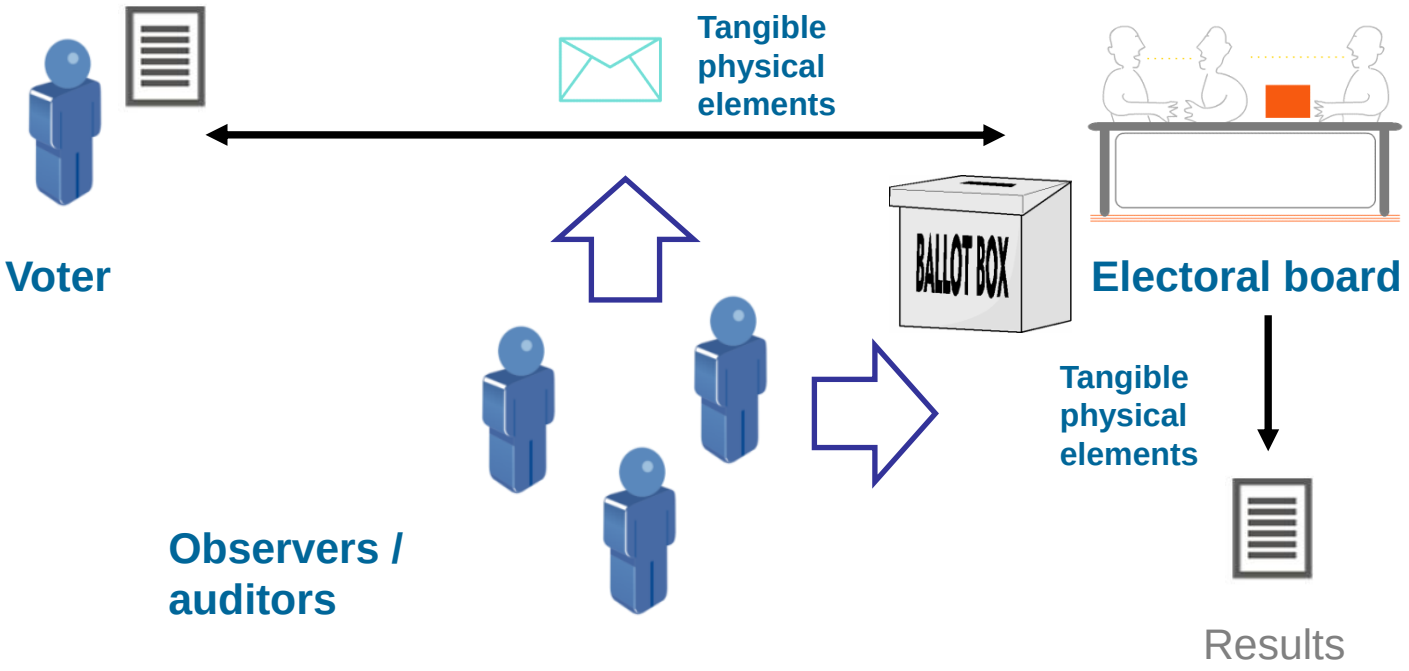
Jordi Puiggali
VP Research & Development
Jordi.Puiggali@scytl.com

scytl
Secure Electronic Voting

Index

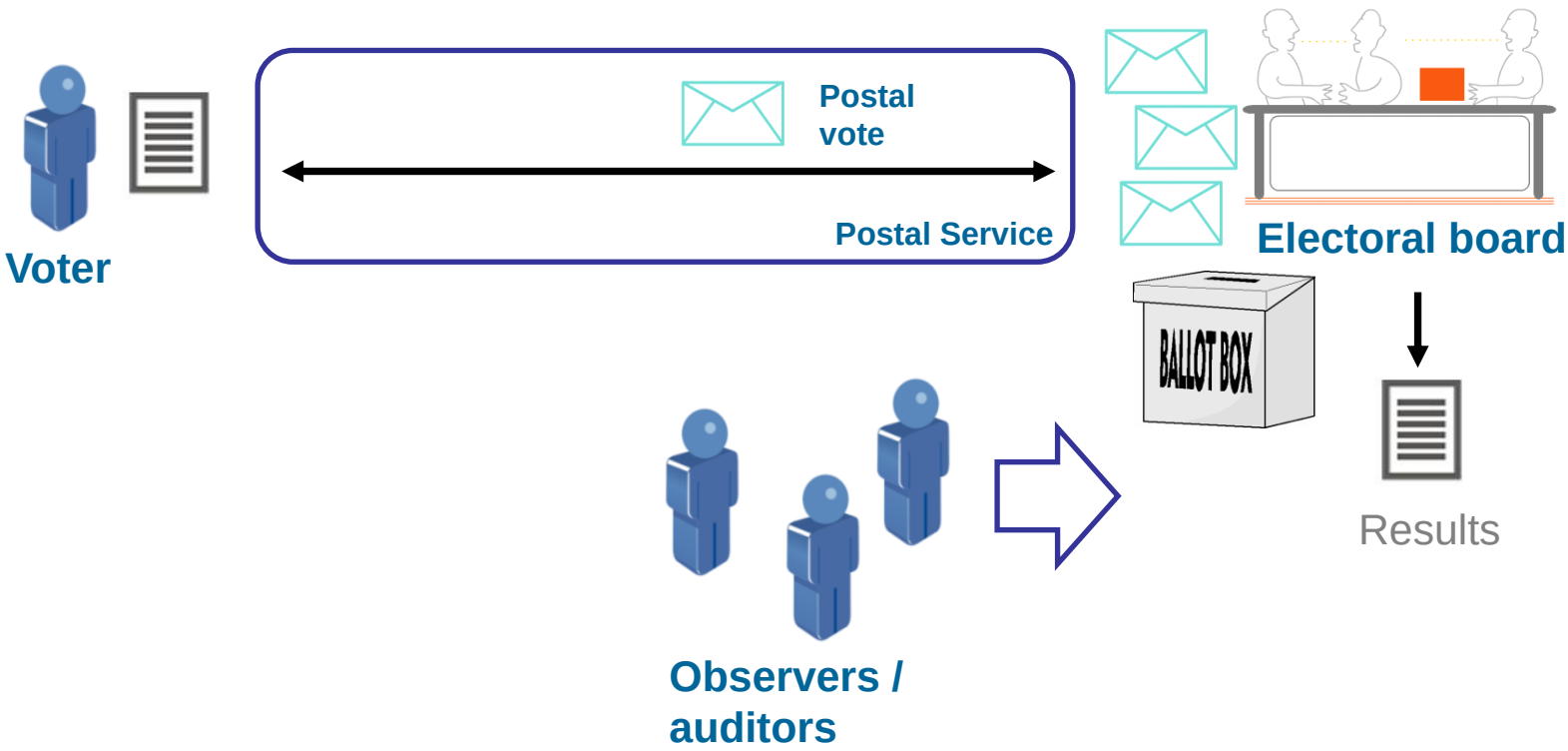
- Auditability in e-voting
- Types of verifiability
- Verifiability methods for e-voting
- Conclusions

Auditability in traditional voting



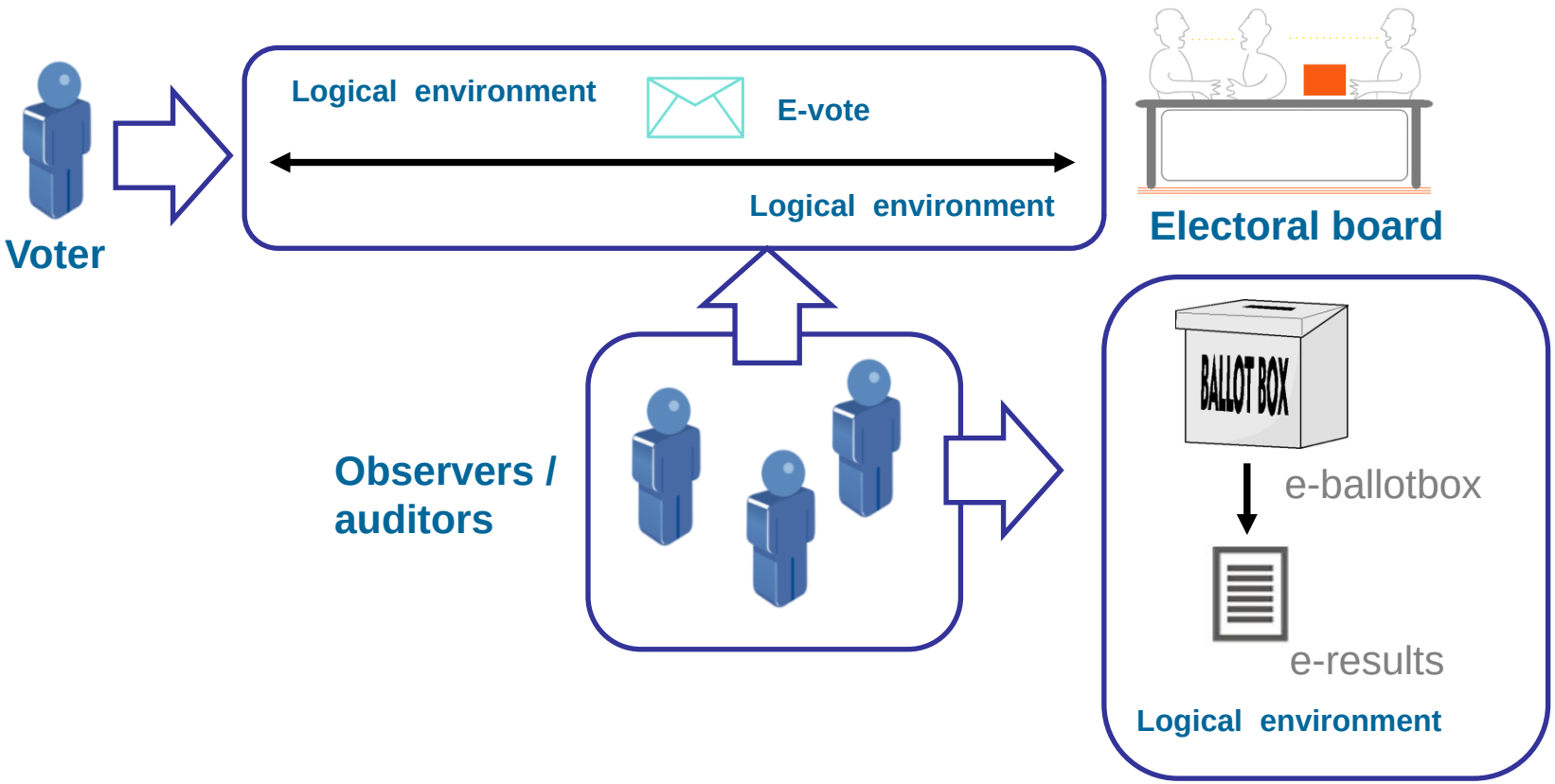
- Votes and processes (e.g., counting) are based on tangible elements.
  - Audit can be done by voters, observers and independent auditors by human means when the processes are carried out
  - Observers can monitor the behavior of other observers to detect any fraud practices

Auditability in postal voting



- The audit of the vote delivery process and storage in the ballot box is difficult if not impossible:
  - Voters only can verify the selection they made but cannot verify if the same vote is received by the Electoral Board
  - Observers can audit the opening of the votes stored in the Ballot Box, but they have no access to the vote delivery process and have limited access to the process of storing the postal votes in the ballot box

Auditability in e-voting



- Votes and processes are happening in a logical dimension:
  - Audit cannot be done by human means
  - Difficult to monitor the behavior of other observers

Index

- Auditability in e-voting
- Types of verifiability
- Verifiability methods for e-voting
- Conclusions

Types of verifiability

Based on who can verify

- Individual verifiability
  - This verification process is voter centered: only the voter that casts the vote is able to implement the verification process
  - This verification process is focused on preserving voter privacy and preventing vote selling/coercion practices

- Universal verifiability
  - This verification process is focused on the public and therefore, it is not only restricted to voters
  - This verifiability is focused on auditing the correct behavior of the processes related to the election, such as the vote decryption and counting
  - To preserve voter privacy, universal verifiability shall not allow to trace individual votes to voters

Types of verifiability

Based on what is verified

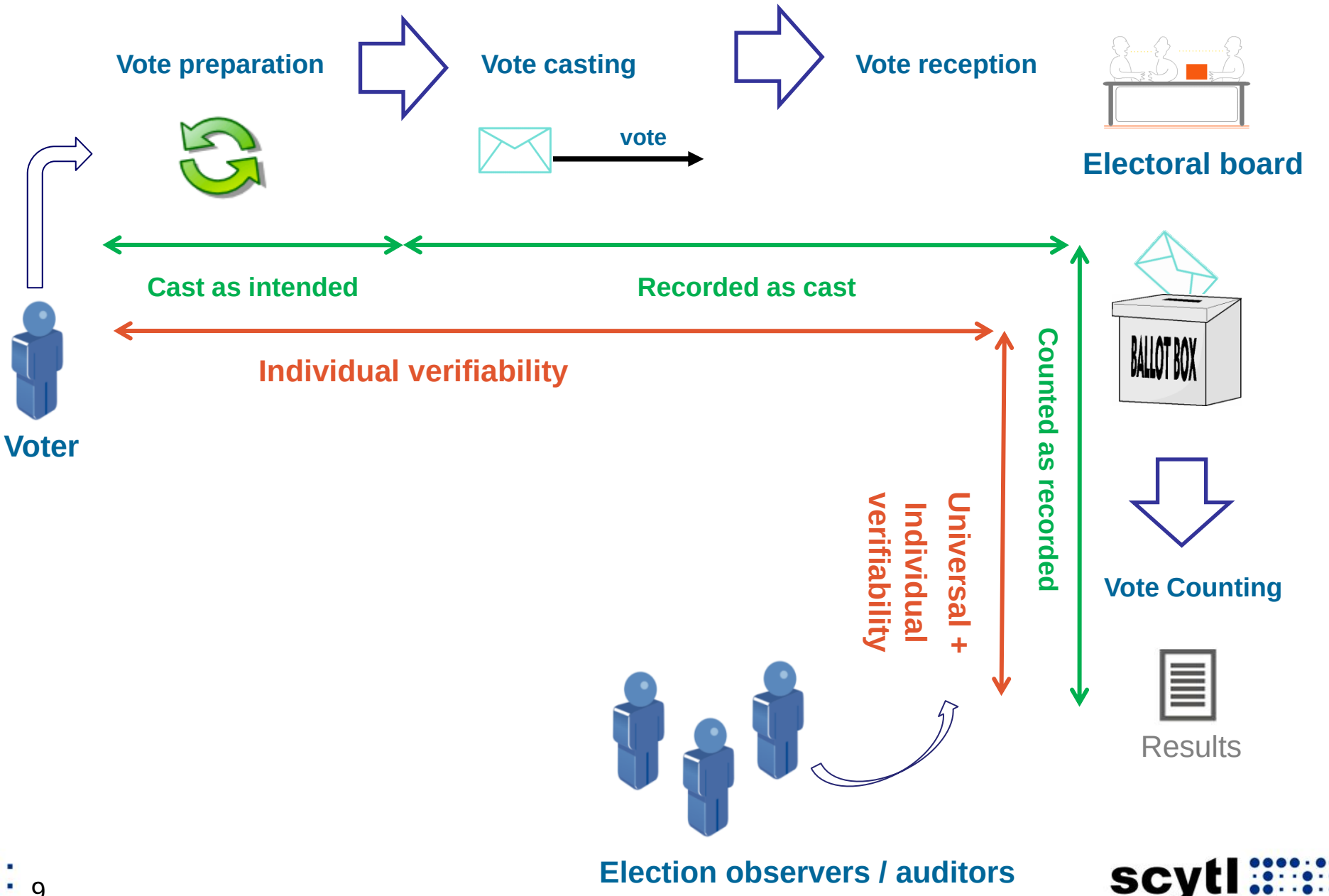
- Cast as intended
  - The main objective of this verification process is to allow voters to verify that their cast votes really represent their voter intent
  - This verification process is individual (only voter knows her voter intent)

- Recorded as cast
  - The main objective of this verification is to confirm that the voter intent has been properly stored (recorded) in the ballot box
  - This verification process is mainly individual (only voter knows her voter intent)

- Counted as recorded
  - The objective of this verification is similar to any open audit processes in traditional elections: auditors and observers can verify that votes belong to valid voters and are not manipulated when counted
  - This verification supports individual voter verification (presence of votes in the ballot box used for counting), and universal verification (verification of the ballot box opening process)

End-to End verification = cast as intended + recorded as cast + counted as recorded

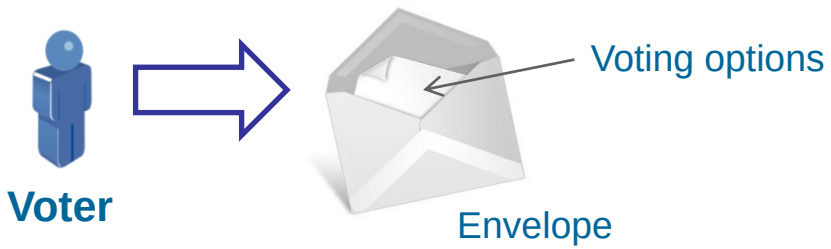
Verifiability and election processes



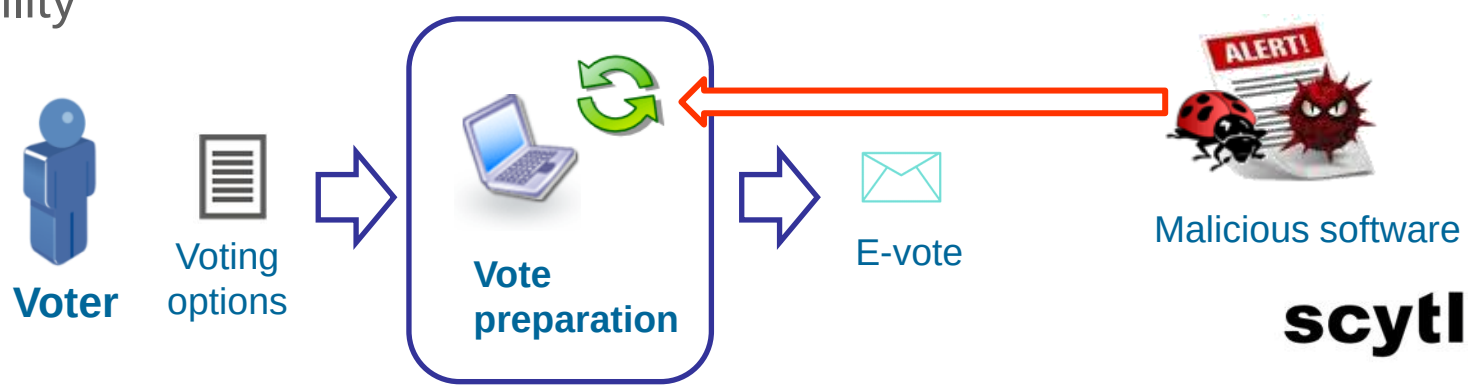
scytl Secure Electronic Voting

Cast as intended risks

- Postal voting scheme:
  - The voter herself introduces the ballot with her voting preferences in the envelope
  - Cast as intended verification is inherent to this scheme



- Remote electronic voting scheme:
  - Voter preferences are represented as en electronic vote
  - The voter cannot verify by human means if the electronic vote really represents her intent
  - Encryption and digital signature prevent manipulation but do not provide verifiability



Recorded as cast risks

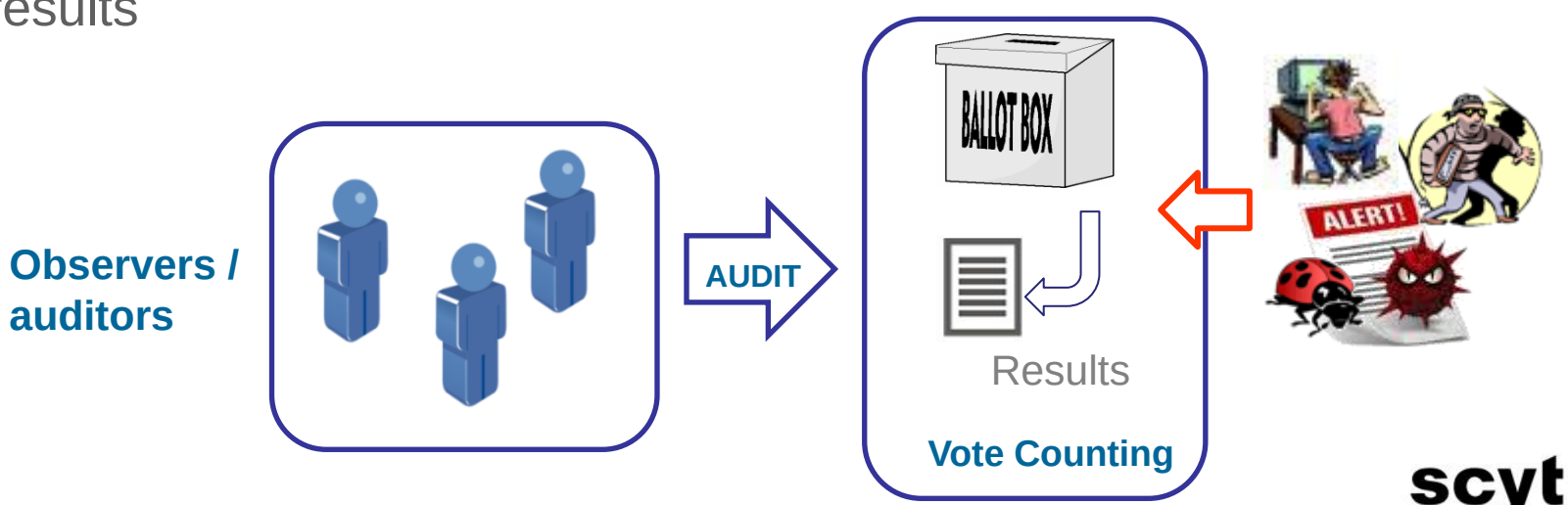
- Postal voting scheme:
  - The vote can be intercepted, deleted or modified while being transported to the counting center
  - The voter has no means to ensure that the vote received by the election officials contains her intent

- Remote electronic voting scheme:
  - The vote can be intercepted, deleted or modified while being sent to the voting platform
  - Encryption and digital signature prevent manipulation but does not provide verifiability

Counted as recorded risks

- Postal voting scheme:
  - The storage of the postal votes is not easy to monitor by auditors
  - Mainly the counting process can be directly overseen by observers and independent auditors to ensure the integrity of the results

- Remote electronic voting scheme:
  - Votes and processes are happening in a logical dimension: audit cannot be done by human means
  - Malicious software or intruders could change the values of the received votes or change the counting process behavior to influence the election results



Index

- Auditability in e-voting
- Types of verifiability
- Verifiability methods for e-voting
- Conclusions

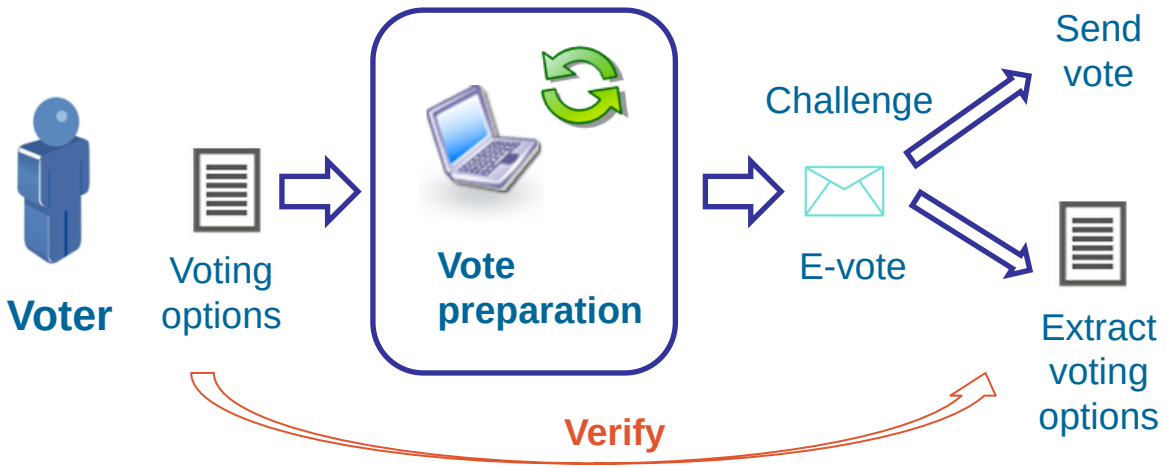
Verification techniques

- Vote encryption challenge
  - Cast as intended
- Return codes
  - Cast as intended and recorded as cast
- Bulletin Board
  - Recorded as cast
- Voting receipts
  - Counted as recorded
- Universal verifiable decryption
  - Homomorphic tally
  - Universal verifiable Mixing

Vote encryption challenge

➢ Cast as intended verification

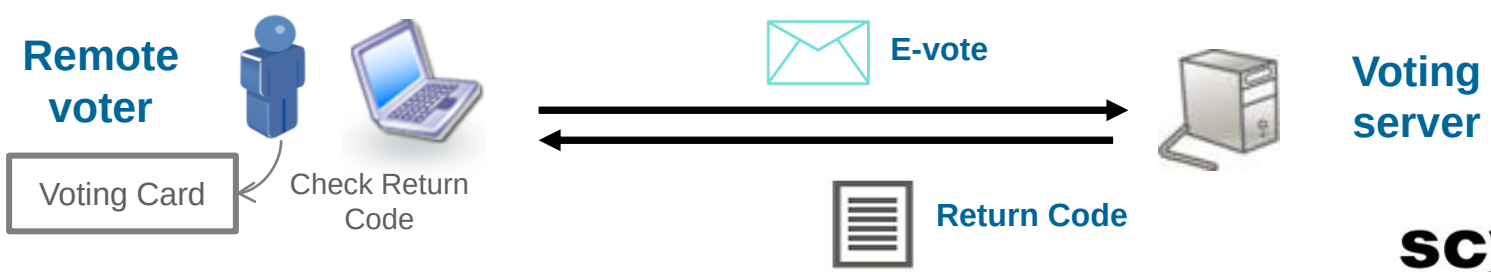
- The vote is encrypted and the application generates an encryption proof (e.g., hash of the encrypted vote)
- The voter can challenge the application to verify the proper encryption of the vote before casting it:
  - Challenge: voter asks the application for showing the secret random parameters used to encrypt the vote
  - Verification: voter uses the random parameters and the encryption proof to verify if the encrypted vote contains her voter intent
  - New encryption: the vote is encrypted again with new random parameters, and a new encryption proof is generated
- Probabilistic verification



Return Codes

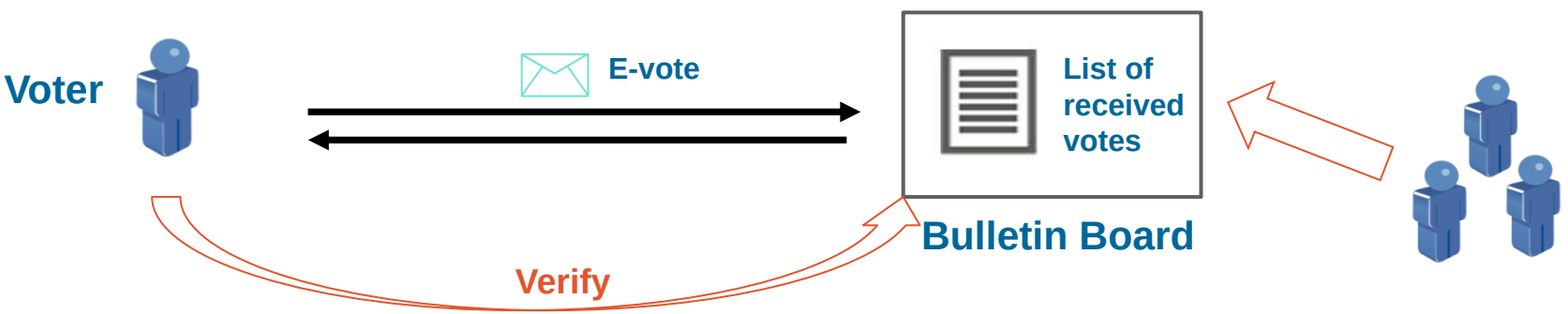
- Cast as intended verification
- Recorded as cast verification

  - Voter has a Voting Card with a set of voter unique Return Codes related to the voting options
  - When casting a vote, the voting platform calculates Return Codes from the received encrypted vote and sends them to the voter
  - The voter uses the Voting Card to verify that the received Return Codes match her selected candidates.
  - Usually two approaches:
    - Pre-encrypted ballots: Voting Card also contains vote casting codes per candidate
    - Voter encrypted ballots: the vote is encrypted in the voting terminal (does not use pre-encrypted codes per candidate)



Bulletin Boards

- Generic tool for verifiability, usually used for recorded as cast verification
  - Public broadcast channel/repository where:
    - Election data (e.g., encrypted votes) is published only by authorized parties
    - Once published, data cannot be deleted or modified
  - The list of received votes can be published in the Bulletin Board, so voters can verify their votes have been properly received and stored

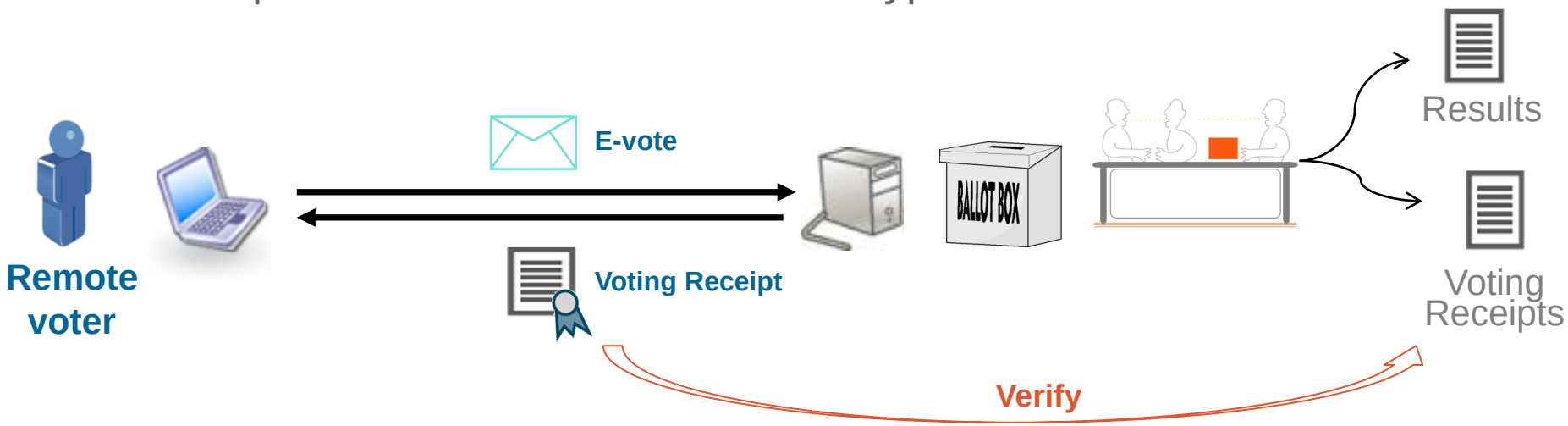


  - Sensitive data (e.g., votes connected to voting order or voter identities) should not be published for privacy issues

Voting Receipts

➢ Counted as recorded verification

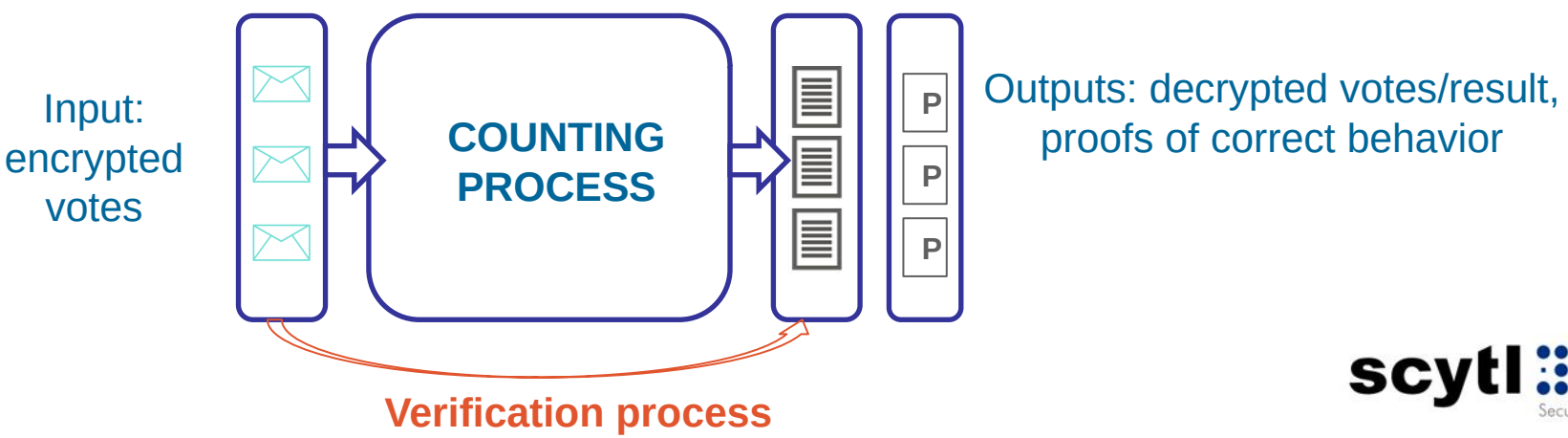
- When a vote is received in the voting platform, a Voting Receipt is generated and sent to the voter
- Voting Receipts are generated and published at the time of vote counting:
  - Voters can verify the presence of their votes during the vote counting process, checking the list of Voting Receipts
- Voting Receipts are digitally signed to prevent bogus complaints.
- Usual approaches:
  - Receipts based on random challenges
  - Receipts based on a hash of the encrypted vote



Universal verifiable decryption

➢ Counted as recorded verification

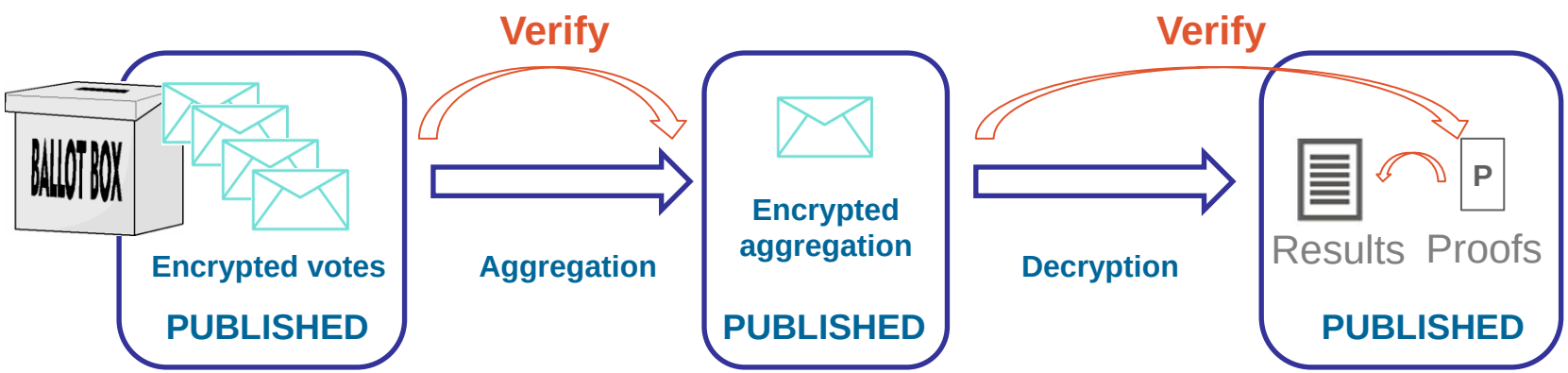
- Objective
  - Audit process based on the input and output data of the counting process
    - Inputs:
      - Encrypted votes
    - Outputs
      - Decrypted votes / decrypted result
      - Cryptographic proofs of correct behavior of the cryptographic processes (e.g., Zero Knowledge Proofs)
  - Audit process shall preserve the privacy of voters and the integrity of the election
    - Shall not allow the correlation of encrypted votes and decrypted ones



Homomorphic Tally

- Encrypted votes are operated. The result of this operation is then decrypted
  - The decryption result is the operation (homomorphic properties) of the plaintext votes
    - For instance, the number of the times each voting option has been selected

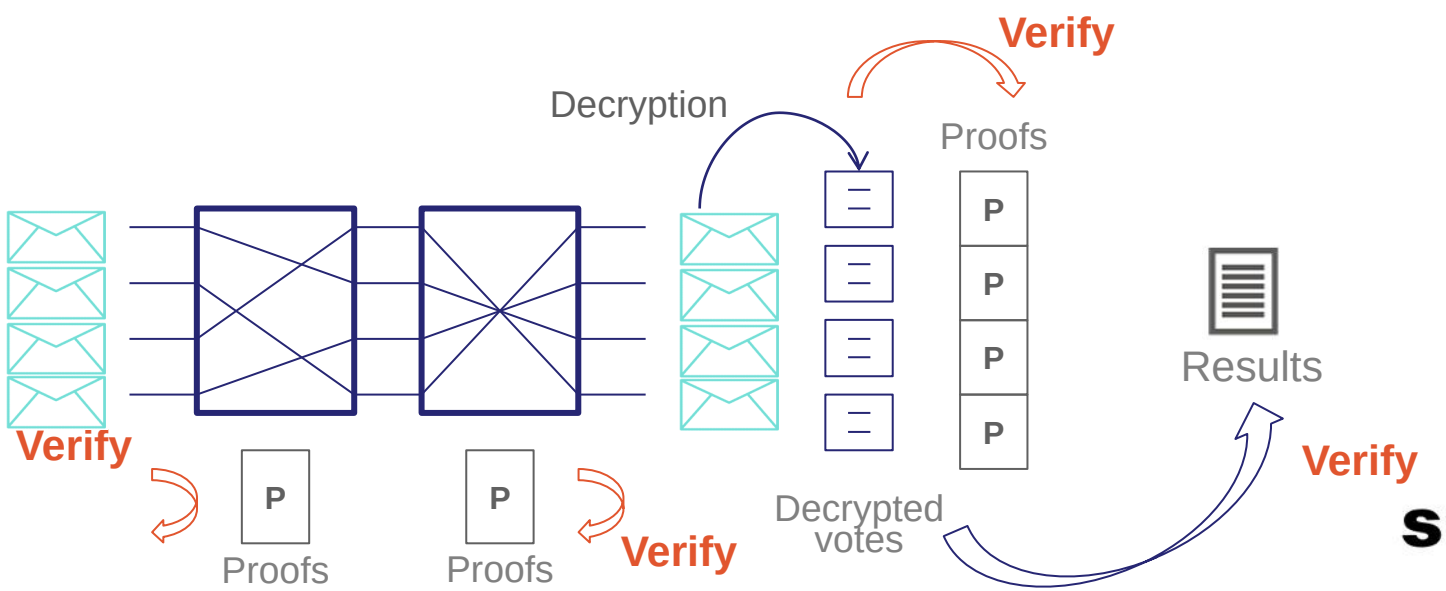
- Verification:
  - Anyone can calculate the result of the operation using the encrypted votes
  - The process generates proofs of correct decryption of the result that can be verified by anyone



Universal verifiable Mix-nets

- Several nodes shuffle and re-encrypt/decrypt the votes for breaking the correlation between the original input order and the output one
  - The shuffled and re-encrypted/decrypted vote output from one node is used as the input of another one
  - The vote contents are obtained (decrypted) at the last node

- Verification:
  - Each mix-node calculates proofs of correct shuffling and correct re-encryption/decryption
  - All the proofs are verifiable by anyone to detect that the input and output votes are based on the same original votes (i.e., have not been changed)



Analysis (i)

Technique	Pros	Cons
Vote encryption challenge	Does not require logistics (e.g., Voting Cards)	Usability problems: voters need the assistance of mathematical tools for verifying Does not provide recorded as cast verification (requires voting receipts to achieve it)
Return codes – Pre-encrypted Ballots	Usability: vote verification can be done by comparing codes	Vote cards can be manipulated to cheat the voter Logistics: requires delivering vote cards to the voters
Return codes – Voter encrypted Ballots	Usability: vote verification can be done by comparing codes More robust against manipulation of vote cards	Logistics: requires delivering vote cards to the voters
Bulletin Board	Facilitates the universal verification of the election	Could compromise voter privacy at long term if not properly implemented

Analysis (ii)

Technique	Pros	Cons
Voting receipts – hash value	Prevents disclosure of the encrypted/decrypted votes	Requires universal verifiable methods to achieve counted as recorded properties
Voting receipts – challenge value	Prevents disclosure of the encrypted/decrypted votes Allows to verify the proper decryption of the vote (partial counted as cast verification)	Requires universal verifiable methods to achieve full counted as recorded properties
Universal verifiable - Homomorphic Tally	Fast method for simple (only selection) and small range (few candidates) elections	Flexibility: does not support write-in candidates and have problems with preferential elections Scalability: the number of encryption operations per voter is proportional to the number of possible voting options
Universal verifiable - Mixing	Flexibility: do not pose limitations in the format of the vote Scalability: drastic reduction of cryptographic operations in medium/large range elections	Is slower in small range elections (compared with homomorphic tally)

Index

- Auditability in e-voting
- Types of verifiability
- Verifiability methods for e-voting
- Conclusions

Conclusions

- Remote voting schemes pose verifiability issues:
  - Postal voting: some processes cannot be verified by the voter or by auditors (recorded as cast verification)
  - Remote electronic voting: voting processes are carried out in a logical dimension

- Individual and Universal verification processes need to provide the following verification properties to be End-to-End verifiable:
  - Cast as intended
  - Recorded as cast
  - Counted as recorded

- Advance cryptographic techniques are focused to achieve these verification properties
  - There are not techniques that achieve all the objectives and therefore, multiple techniques must be combined
  - It is important to analyze and understand the limitations and drawbacks of the techniques before designing a final solution

Any questions?

www.scytl.com