Workshop on UOCAVA Remote Voting Systems

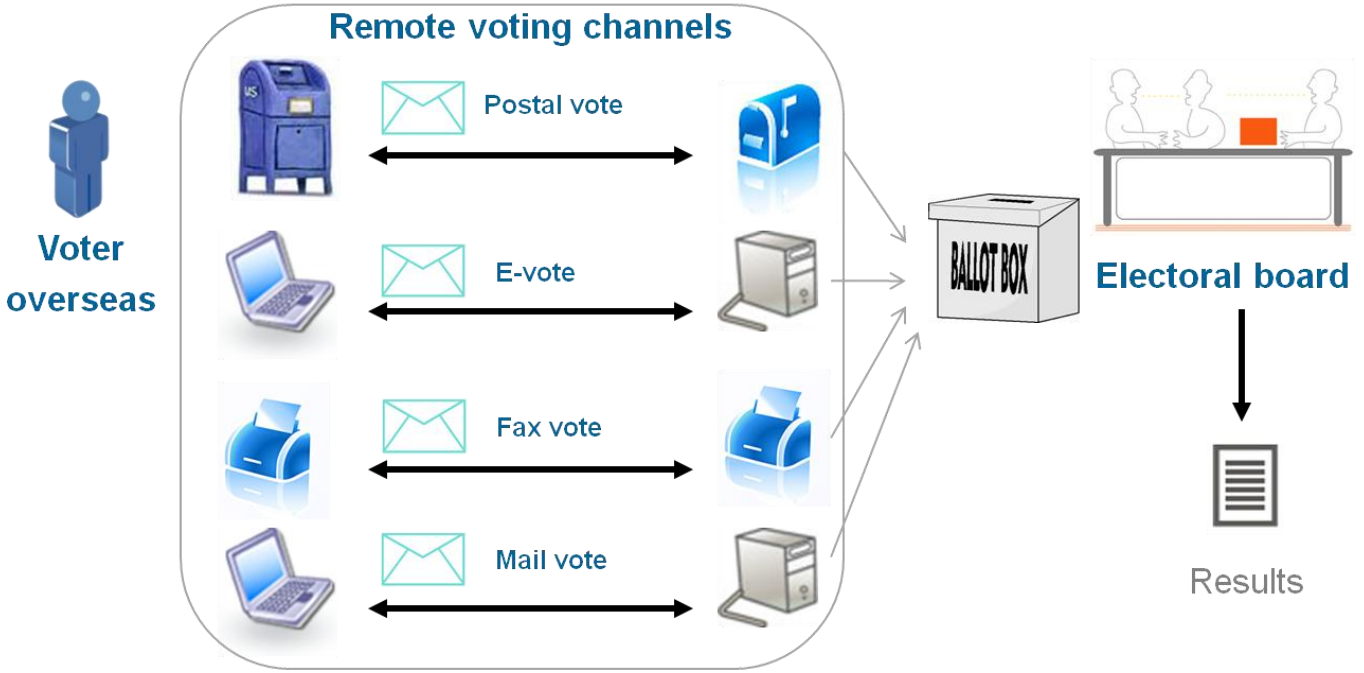
Security Practices and Risk Impact in Remote e-Voting

August 2010

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

scytl
Secure Electronic Voting

Index



- Alternative voting channels such as postal, fax or electronic voting are used to allow overseas voters to cast their votes remotely.
- Is any voting of these voting channels more secure than the others?
- To know it, we should evaluate:
  - Security risks.
  - Security measures: implementation and risk mitigation.

Index

- Introduction
- Security Risks of Remote Voting
- Security Measures and Risk Mitigation in Remote e-Voting
- Conclusions

General Security Risks of Remote Voting

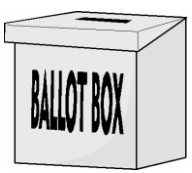
Voter privacy compromise

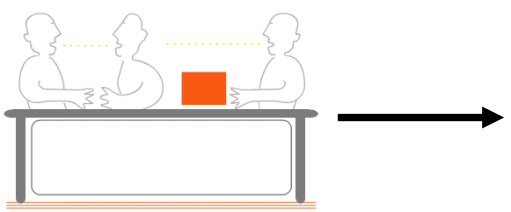
Innacurate auditability

Vote tampering

Vote deletion

Remote voter





Electoral board

Results

Voter coercion and vote buying

Election boycott-denial of service

Unauthorized voters casting votes

Voter impersonation / Ballot stuffing

Intermediate results

scytl Secure Electronic Voting

- Security risks on a voting channel depend on the security controls implemented
  - The security of a voting channel depends on the security controls implemented by the voting platform.
  - Different implementations of the same voting channel could have different risk levels.

- It is of paramount importance to make a risk assessment of the voting channel before deciding its security
  - Which security practices are used on remote e-voting?
  - Which are their impact at risk mitigation?

Index

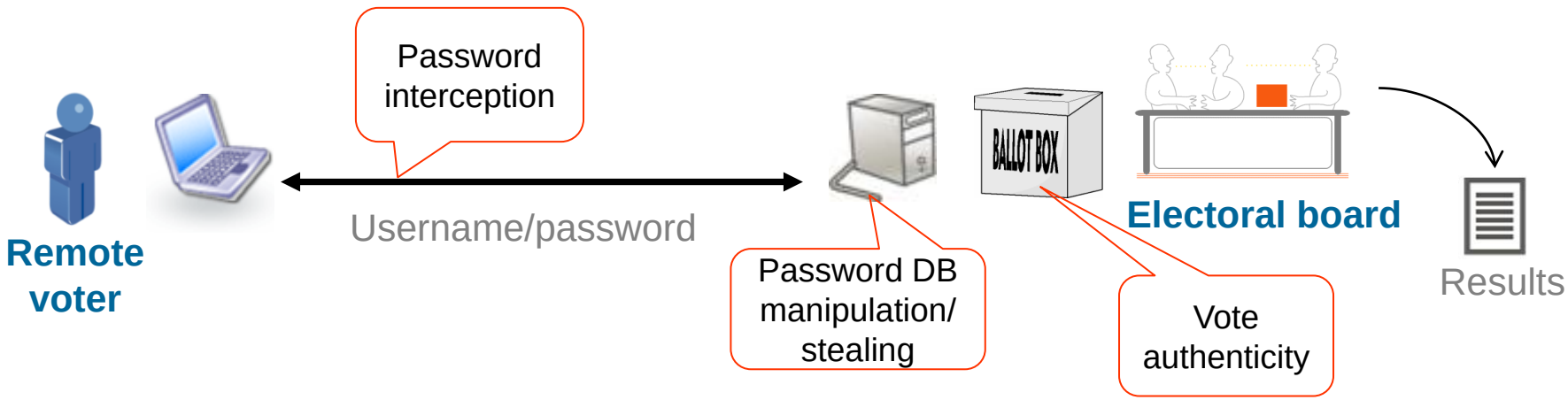
- Introduction
- Security Risks of Remote Voting
- Security Measures and Risk Mitigation in Remote e-Voting
- Conclusions

Authentication (i)

Authentication methods

How can we proof voter identity in a remote way?

- Username and password methods:
  - Username and password values are stored in the voting server to verify voter identity: they are vulnerable to credential stealing.
- **High Risk: Unauthorized voters, voter impersonation and ballot box stuffing**

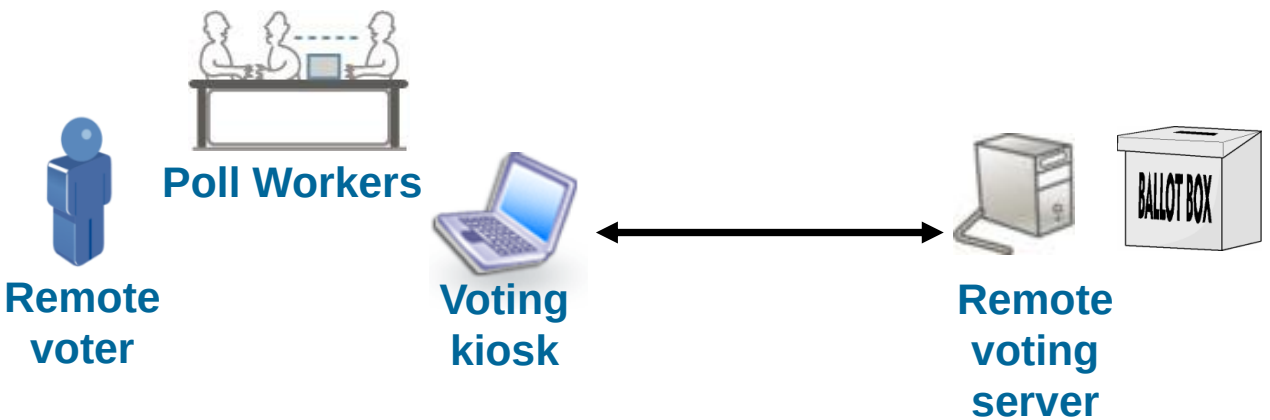


- Digital certificates
  - Digital certificates and digital signatures: provides voter and vote strong authentication. No private credentials are stored in the voting server and (encrypted) votes can be digitally signed.
- **Low Risk: Unauthorized voters, voter impersonation, ballot box stuffing and vote tampering**

Authentication (ii)

Authentication methods (cont.) *How can we proof voter identity in a remote way?*

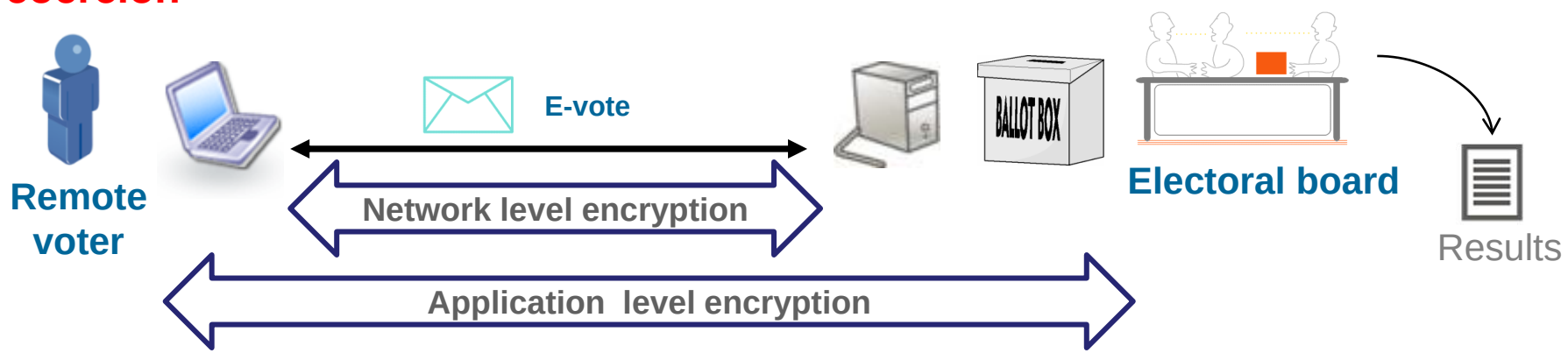
- Supervised kiosk:
  - Voter is identified in-person by poll workers at a remote supervised center
- **Low Risk: Unauthorized voters, voter impersonation, ballot box stuffing and vote tampering**



Vote Secrecy

Vote encryption *How can we protect a vote from eavesdroppers?*

- Network encryption:
  - Voting options are only encrypted while transmitted in the network but processed in clear at the voting server: they are vulnerable to attackers that have access to the server.
- **High Risk: Voter privacy compromise, vote tampering, intermediate results and voter coercion**

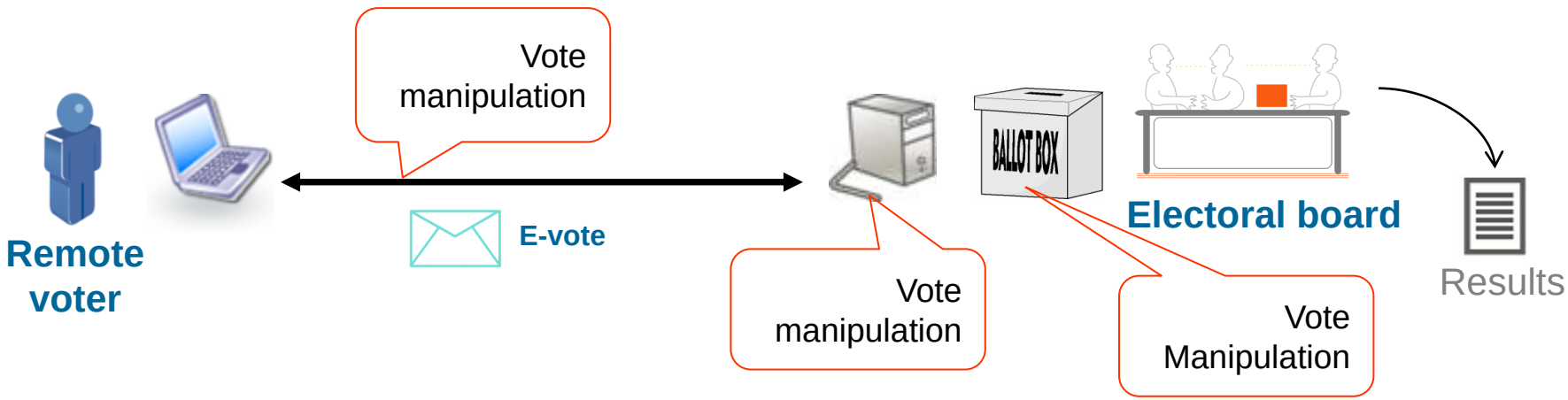


- Application level encryption:
  - Voting options are encrypted in the voting terminal and remain encrypted until the electoral board decrypts them: they are not vulnerable to the server attacks.
- **Low Risk: Voter privacy compromise, vote tampering, intermediate results and voter coercion**

Vote Integrity

How can we protect votes from being modified?

- MAC functions:
  - Vote integrity is protected by means of a voter/server shared MAC key stored in the voting server: they are vulnerable to key stealing.
- **Medium Risk: Vote tampering and vote impersonation/ballot box stuffing**



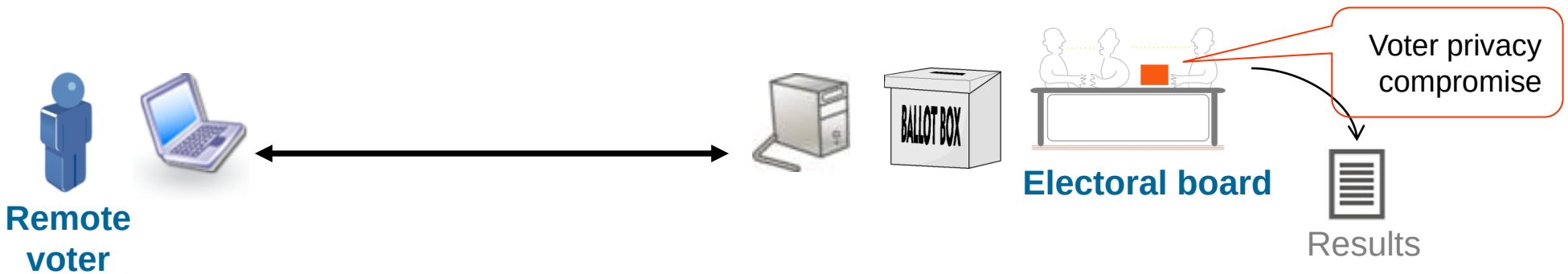
- Digital signatures and Zero knowledge proofs of origin:
  - Private values needed to perform digital signatures and ZK proofs are not stored in the server.
- **Low Risk: Unauthorized voters, voter impersonation, ballot box stuffing and vote tampering**

Election Key Security

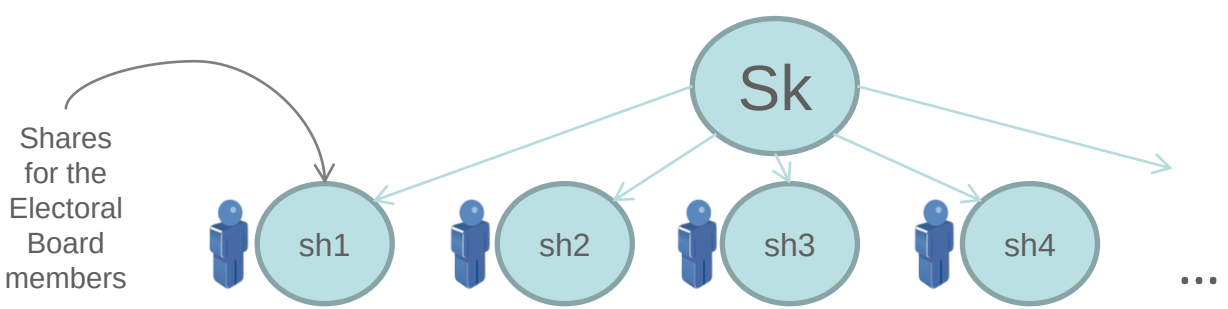
Election private key protection

How can we protect a vote from decryption?

- Access control:
  - Access to the decryption private key is protected by authentication and authorization (ACL) means: vulnerable to brute force attacks.
- **High Risk: Voter privacy compromise, intermediate results and voter coercion**



- Secret sharing schemes:
  - Threshold cryptography is used to create and split the election private key in shares without requiring to store the key as a whole anywhere. A minimum number of Electoral Board members must collaborate with their private key shares to decrypt the votes.
- **Low Risk: Voter privacy compromise, intermediate results, voter coercion and denial of service**

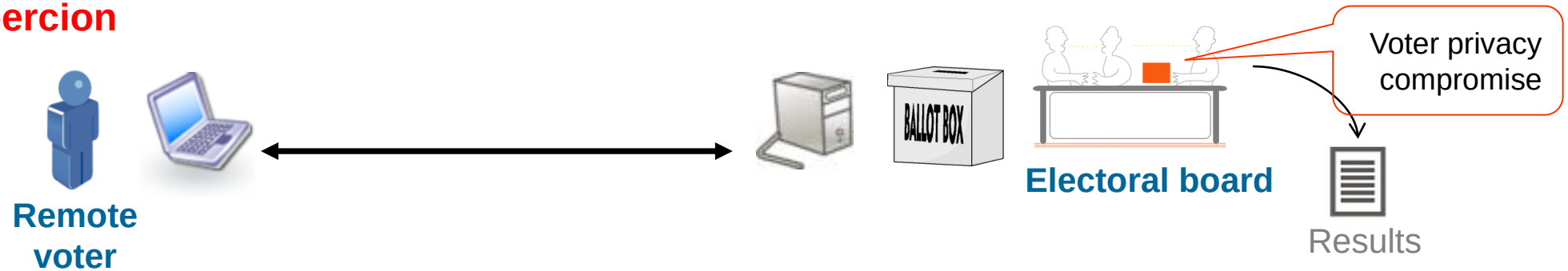


Voter Privacy (i)

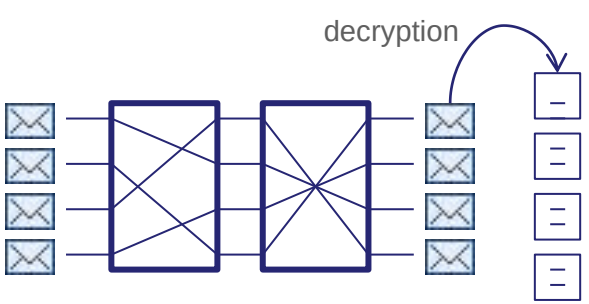
Anonymizing votes during decryption

How to preserve voter anonymity?

- Straight forward decryption:
  - Clear text votes can be correlated with encrypted votes, which could be connected to the voters: voter privacy could be broken.
- **High Risk: Voter privacy compromise, vote tampering, ballot stuffing and voter coercion**



- Mixnets:
  - Encrypted votes are shuffled and decrypted (or re-encrypted and decrypted) several times before obtaining the clear-text votes. Encrypted votes and decrypted ones cannot be directly correlated by position, preserving voter privacy.
- **Low Risk: Voter privacy compromise, vote tampering, ballot stuffing and voter coercion**

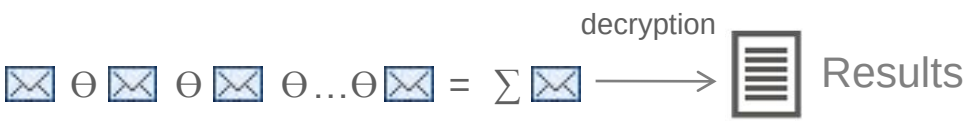


Voter Privacy (ii)

Anonymizing votes during decryption (cont.)

How to preserve voter anonymity?

- Homomorphic tally:
  - Encrypted votes are not individually decrypted. The result is the decryption of the operation of all the encrypted votes.
- **Low Risk: Voter privacy compromise, vote tampering, ballot stuffing and voter coercion**



Election Auditability (i)

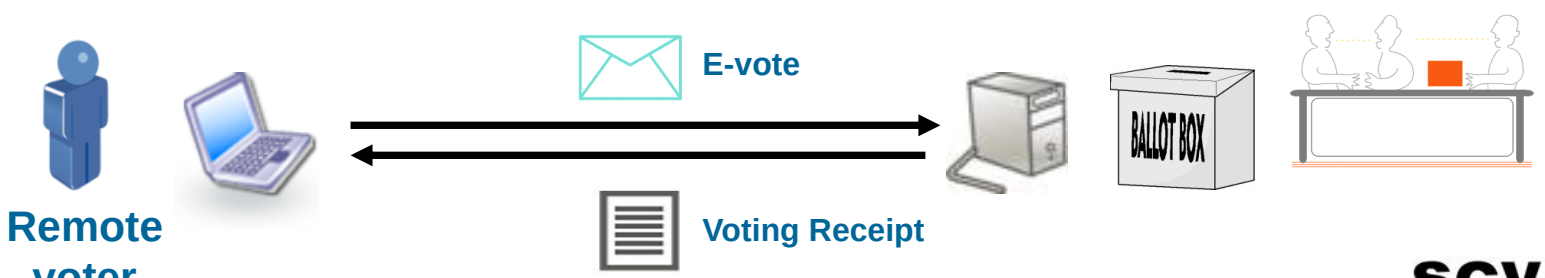
Auditability

How to audit election fairness?

- Standard logs:
  - Sensitive operations are registered in standard log files: logs could be altered without being notice to hide malicious practices.
- **High Risk: Inaccurate auditability, voter privacy compromise, vote tampering, ballot stuffing, voter coercion, etc.**

- Immutable logs:
  - All sensitive operations are registered in cryptographically protected logs and cannot be manipulated. However, processes could generate false traces.
- **Medium Risk: Inaccurate auditability.**

- Standard receipt:
  - Voters receive a proof of casting based on non-cryptographically protected information (i.e., does not provide counted as cast features).
- **High Risk: Inaccurate auditability.**

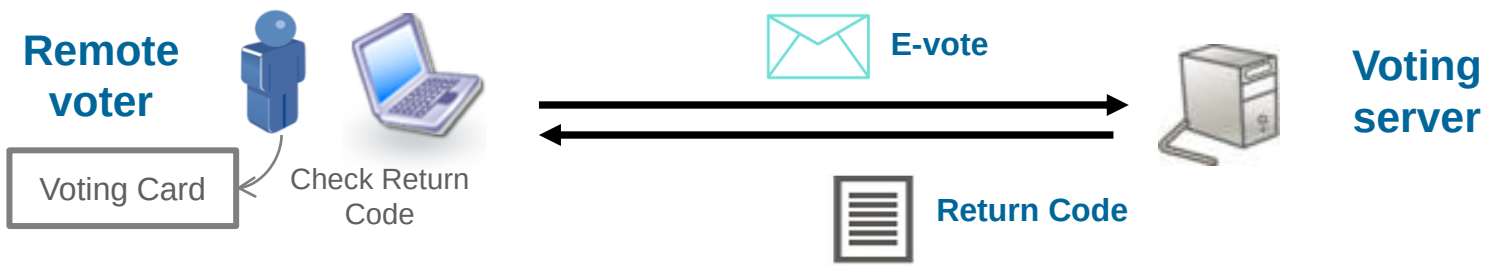


Election Auditability (ii)

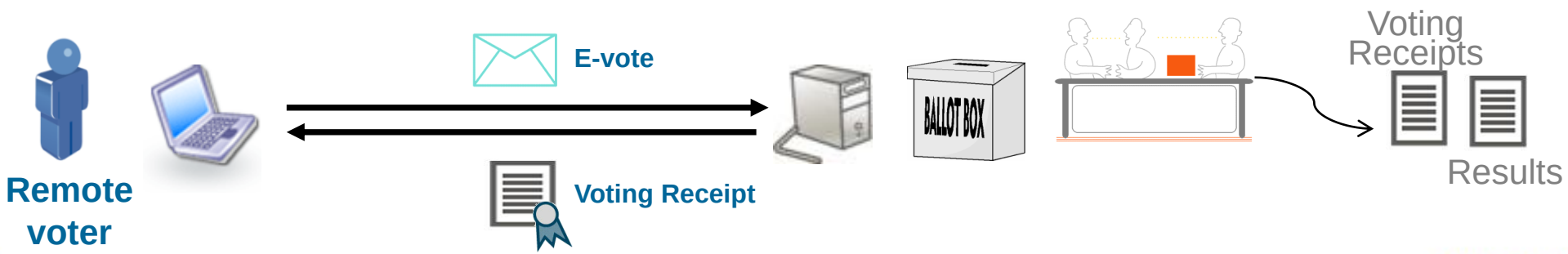
Auditability (cont.)

How to audit election fairness?

- Individual voter verification - cast as intended:
  - Voter is able to verify that the vote recorded by the voting server contains the voting options originally selected by herself. (E.g., Return Codes).
- **Low Risk: Inaccurate auditability.**



- Individual voter verification - counted as cast:
  - Voters are able to verify that their votes have been included in the final tally. This verification must be complemented with the Universal verifiability
- **Low Risk: Inaccurate auditability.**



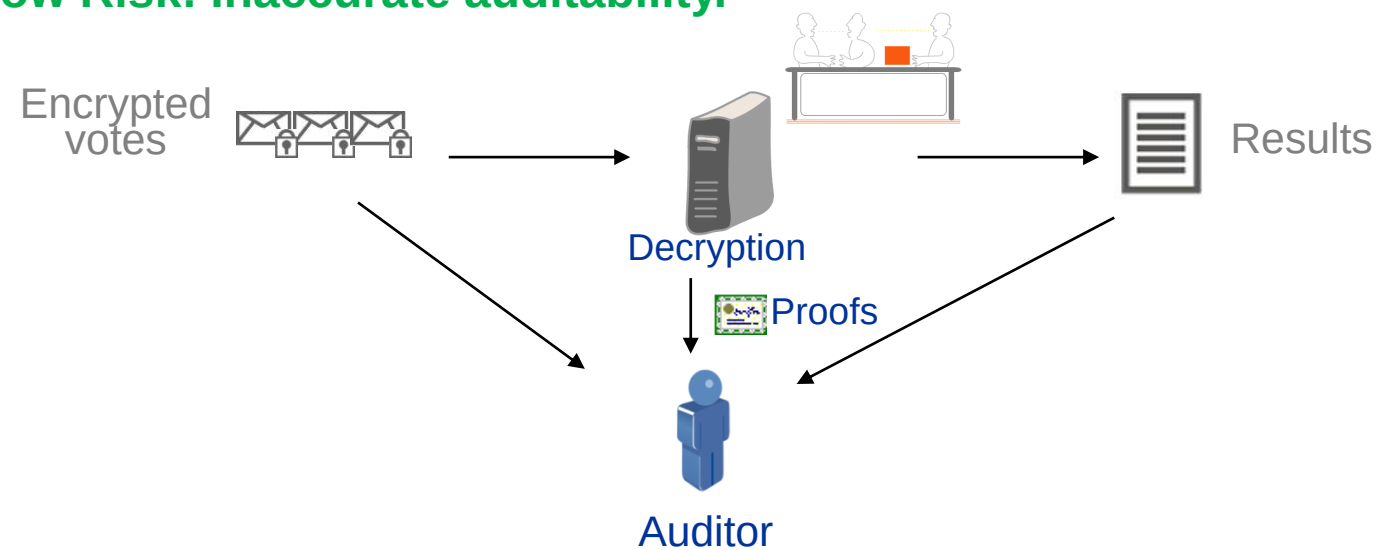
scytl Secure Electronic Voting

Election Auditability (iii)

Auditability (cont.)

How to audit election fairness?

- Universal verifiability:
  - Allows observers or independent auditors to verify the proper decryption of the votes by means of using cryptographic proofs (e.g., ZKP) generated by the decryption process.
- **Low Risk: Inaccurate auditability.**

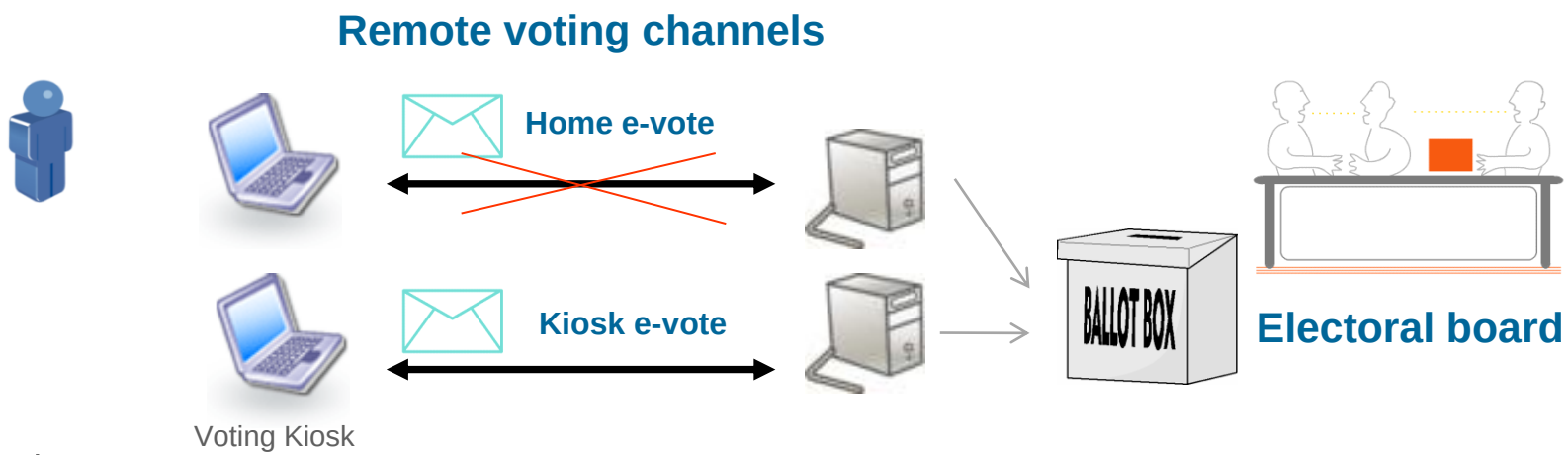


- End-to-end verification:
  - Combination of individual and universal verifiability
- **Lowest Risk!!!: Inaccurate auditability.**

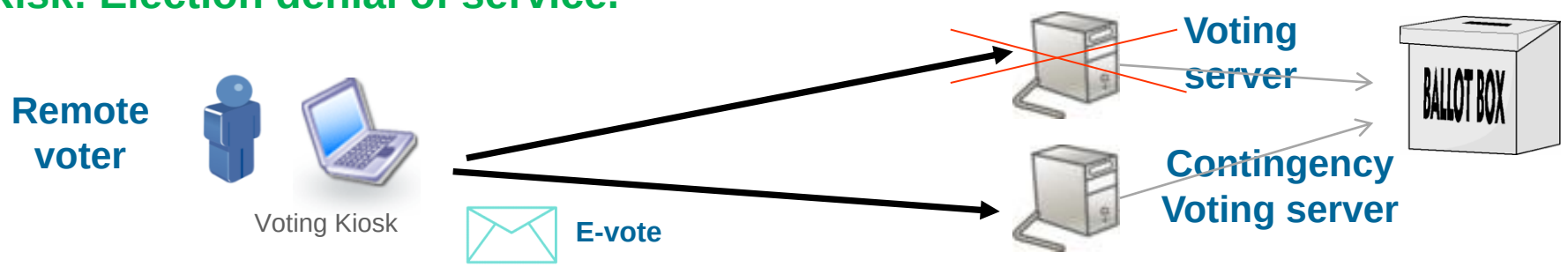
Denial of Service

How to preserve election service availability?

- Multiple voting channel support:
  - Allows voters to react in case the service is not available.
- **Medium Risk: Election denial of service.**



- Kiosk vote:
  - Allows to use private channels (VPNs) and contingency servers
- **Low Risk: Election denial of service.**



scytl Secure Electronic Voting

Index

- Introduction
- Security Risks of Remote Voting
- Security Measures and Risk Mitigation in Remote e-Voting
- Conclusions

Summary (i)

	Security measure	Mitigation	Risks managed
Authentication	Password-based	High Risk	Unauthorized voters, voter impersonation and ballot box stuffing
	Digital certificate	Low Risk	Unauthorized voters, voter impersonation, ballot box stuffing and vote tampering
	Supervised	Low Risk	Unauthorized voters, voter impersonation, ballot box stuffing and vote tampering
Vote encryption	Network encryption	High Risk	Voter privacy compromise, vote tampering, intermediate results and voter coercion
	Application level encryption	Low Risk	Voter privacy compromise, vote tampering, intermediate results and voter coercion
Vote integrity	MAC based	Medium Risk	Vote tampering and vote impersonation/ballot box stuffing
	Digital certificates	Low Risk	Unauthorized voters, voter impersonation, ballot box stuffing and vote tampering

Summary (ii)

	Security measure	Mitigation	Risks managed
Election private key protection	Access Control	High Risk	Voter privacy compromise, intermediate results and voter coercion
	Secret Sharing	Low Risk	Voter privacy compromise, intermediate results, voter coercion and denial of service
Anonymizing votes during decryption	Straight forward decryption	High Risk	Voter privacy compromise, vote tampering, ballot stuffing and voter coercion
	Mixnets	Low Risk	Voter privacy compromise, vote tampering, ballot stuffing and voter coercion
	Homomorphic Tally	Low Risk	Voter privacy compromise, vote tampering, ballot stuffing and voter coercion
Denial of Service	Multiple voting channel	Medium Risk	Election denial of service
	Kiosk vote	Low Risk	Election denial of service

Summary (iii)

	Security measure	Mitigation	Risks managed
Auditability	Standard logs	High Risk	Inaccurate auditability, voter privacy compromise, vote tampering, ballot stuffing, voter coercion, etc.
	Immutable logs	Medium Risk	Inaccurate auditability
	Standard receipt	High Risk	Inaccurate auditability.
	Individual verification - cast as intended	Low Risk	Inaccurate auditability.
	Individual verification – counted as cast	Low Risk	Inaccurate auditability.
	Universal verifiabiliy	Low Risk	Inaccurate auditability.

Conclusions

- Similar security risks are present in any remote voting channel, differences are based on the way these can be exploited and mitigated.

- The security of the voting channel depends on the security measures implemented and how them mitigate the risks.

- Standard security mechanisms fall short to effectively mitigate the security risks of remote e-voting.

- Using advanced cryptographic protocols the security risks can be drastically reduced and election auditability is substantially enhanced.

www.scytl.com