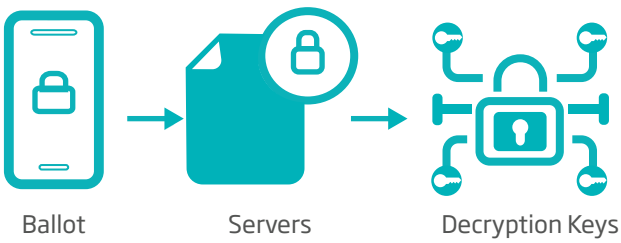
Scytl

Online Voting Security

Scytl

Competitors

Encryption



1

End-to-End Encryption. Prevents external (such as man-in-the-middle) and internal employee attacks.

Basic encryption, such as https and database encryption. Vulnerable to man-in-the-middle attacks and internal employee access to ballots.

Authentication

2

Secure two-factor authentication & a unique digital signature ensures only eligible voters can access the system.

Front-end multi-step authentication provides a false sense of security without the back-end security to back it up.

Verifiability

3

Stand-up to public scrutiny. Advanced universal verifiability features allow voters and auditors to verify ballots were cast and counted accurately.

Internal employees with access can manipulate votes. Voters & auditors cannot verify that the ballot was counted nor that the submitted ballot choices were counted.

@scytl_us | info@scytl.us | 813-490-7150

www.scytl.us

Scytl

Online Voting Security

Scytl	Competitors

Log Technology

Patented Immutable Logs

Trace all system action, flag attacks, and provide objective, irrevocable proof of a fraud-free election.

4

Basic Logs

Basic logging does not prevent malicious or internal actors from changing the actions logged in the system.

Audits

Audited and proven by some of the most demanding governments in the world, including the U.S. FVAP.

5

Minimal or not created to enable third party audits.

Anonymity

Advanced cryptographic mixing techniques ensure voter data is anonymous at all times and follow best practices for irrevocable personal data destruction.

6

Claim they purge unnecessary data, but do not provide third party validation on data practices. System administrators can easily trace ballots to voters.

@scytl_us | info@scytl.us | 813-490-7150

www.scytl.us