TRIP: Coercion-Resistant Registration for E-Voting with Verifiability and Usability in Votegral

Louis-Henri Merino, Simone Colombo, Rene Reyes, Alaleh Azhir, Shailesh Mishra, Pasindu Tennage, Mohammad Amin Raeisi, Haoqian Zhang, Jeff R. Allen, Bernhard Tellenbach, Vero Estrada-Galiñanes, Bryan Ford

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Federal Office for Defence Procurement

EPFL

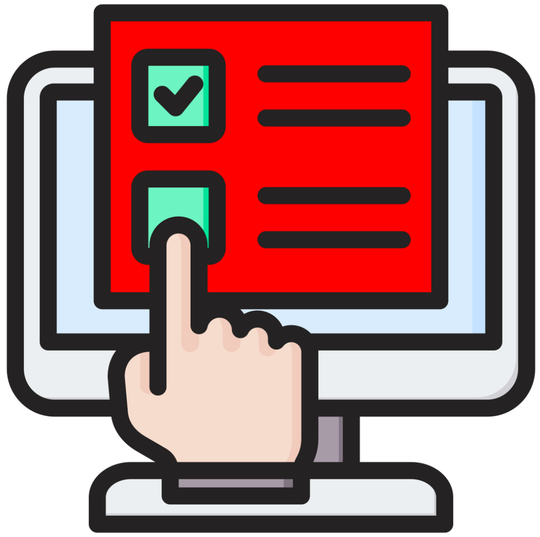
Massachusetts Institute of Technology

Online Voting Systems

Home **Hotel**

Cast **votes** on your **own** device from **anywhere**

Online Voting Systems



~~Cast votes on your own device from anywhere~~

Cast **the coercer's** vote

Recent Examples of Coercion

October 25, 2024 11:42 CET

By RFE/RL's Moldovan Service

Moldovan Police Accuse Pro-Russian Oligarch Of $39M Vote-Buying Scheme

Elena Castro & Randy Roth

Advisor: Gautam Nair, Section Leader: Rema Hanna

John F. Kennedy School of Government, Harvard University

In fulfilment of the requirements for the Master in Public Administration in International Development

March 12, 2022

The Potential Future of Vote Buying[1]

Online voting is **susceptible** to **more scalable** coercion threats

1. Austgen, James, et al. *DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs*. arXiv:2311.03530, 6 Nov. 2023.

Roadmap

- **Coercion-Resistance**
- TRIP Registration Protocol
- Limitations and Conclusion

Real and Fake Voting Credentials[1]

Real Vote

Intended Vote

Fake Vote(s)

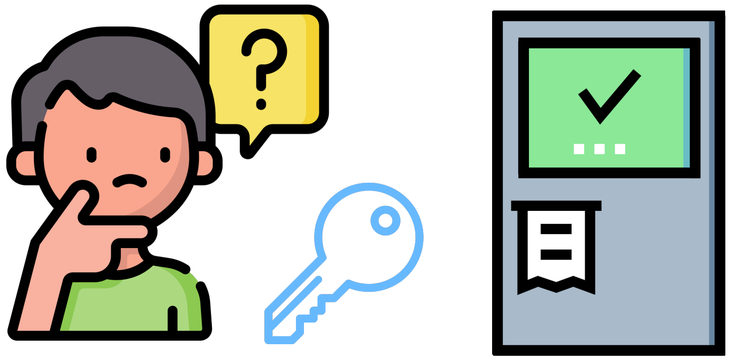
Coerced Vote

Fake credentials cast votes that **do <u>not</u>** count **while** being **indistinguishable** from **real credentials** which cast votes that **do** count.

1. Juels, Ari, et al. "Coercion-Resistant Electronic Elections." *Towards Trustworthy Elections: New Directions in Electronic Voting*, 2010.

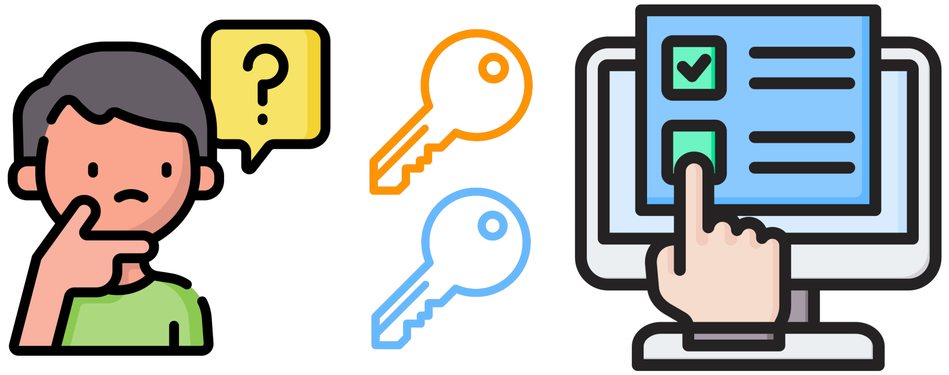
Fake Credential Concerns

Verifiability



Genuinely Real?

Usability

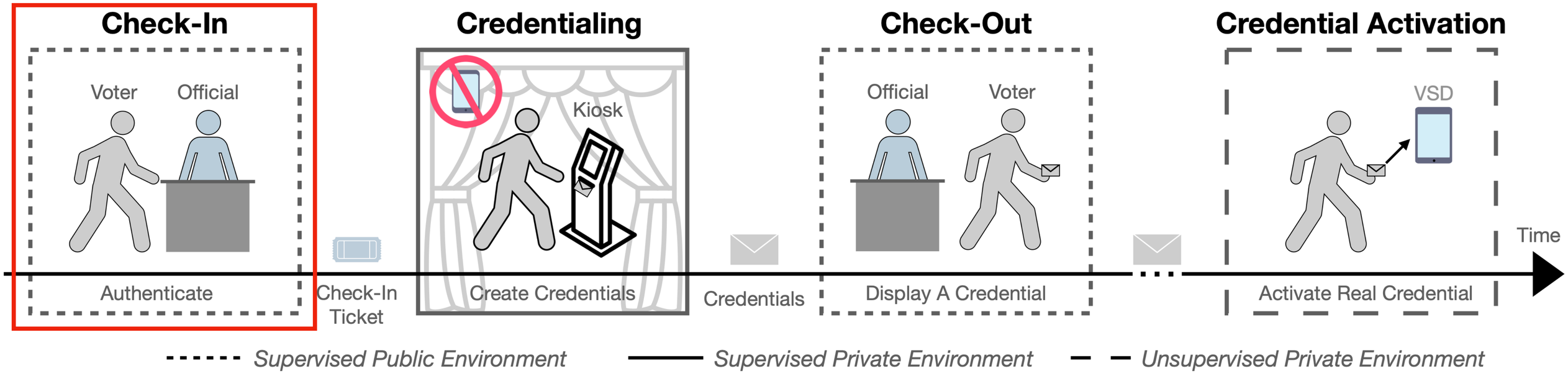


Distinguish Real from Fake?

Roadmap

- Coercion-Resistance
- **TRIP Registration Protocol**
- Limitations and Conclusion

Trust-Limited Coercion-Resistant In-Person Registration

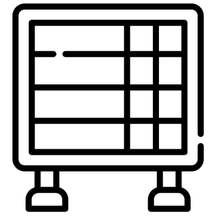


TRIP issues **voter-verifiable real credentials** and **indistinguishable fake credentials**

Registration Log

Credentialing in Booth

Public Ledger



Alice

Real: R_A

Fake: F_{A_1}

Fake: F_{A_2}

...

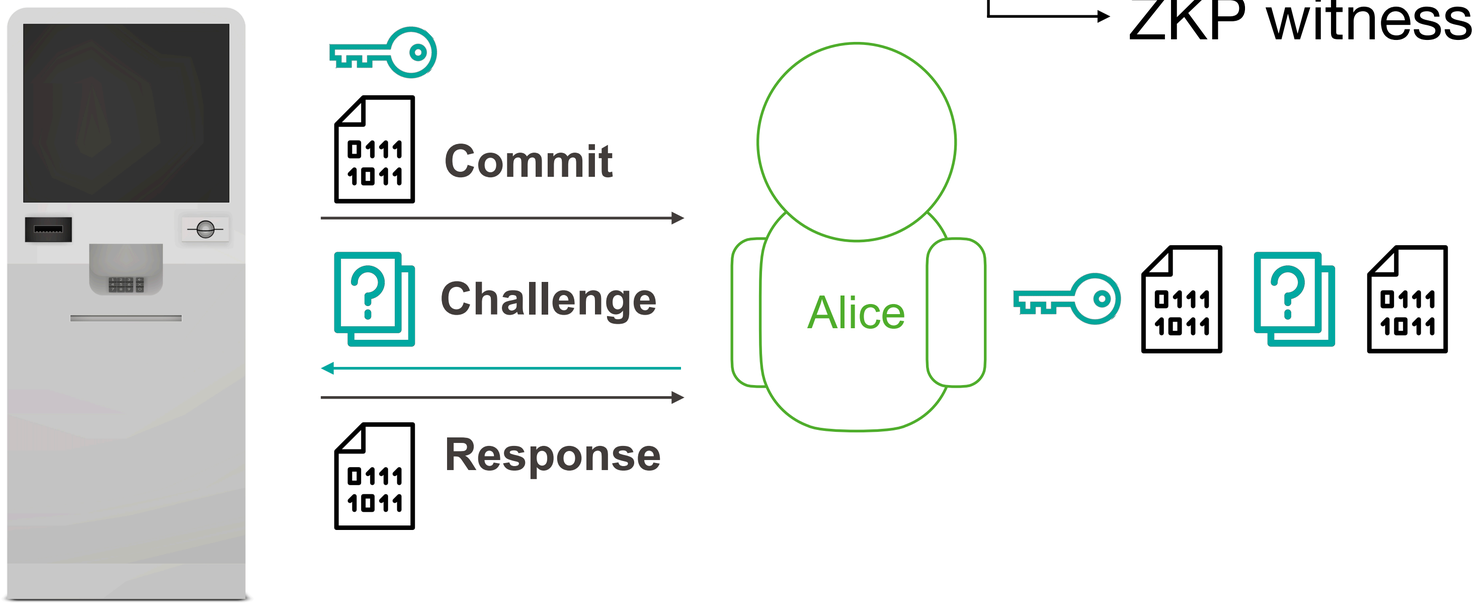
Alice	$T_A = \text{ElGamal}(R_A, x_A \in Z_q)$
Bob	$T_B = \text{ElGamal}(R_B, x_B \in Z_q)$
Carol	$T_A = \text{ElGamal}(R_C, x_C \in Z_q)$

Real Credential Issuance
Schnorr interactive zero-knowledge proof

Convince **Alice** T_A (on public ledger) is an ElGamal encryption of R_A (given to Alice)

$$T_A = \text{ElGamal}(R_A, x_A \in Z_q)$$

ZKP witness



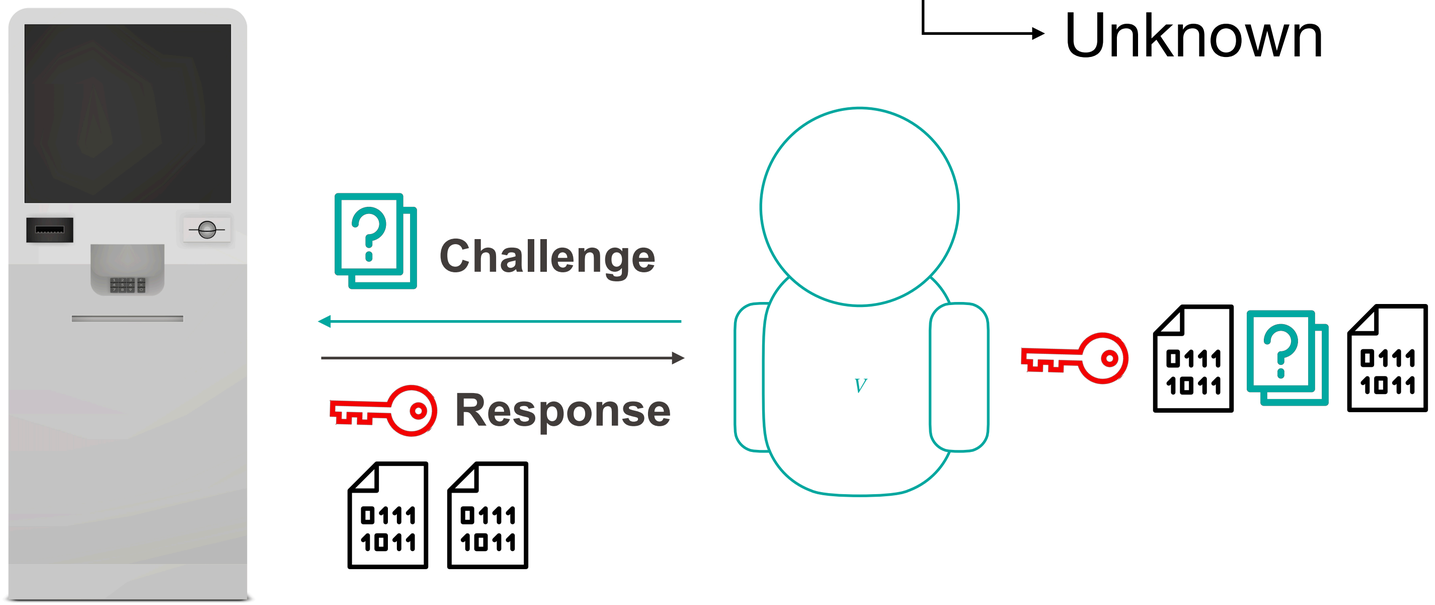
- Kiosk forced to give the voter their real credential
- Cannot create fake credentials using this process

Fake Credential Issuance

Simulated Schnorr interactive zero-knowledge proof

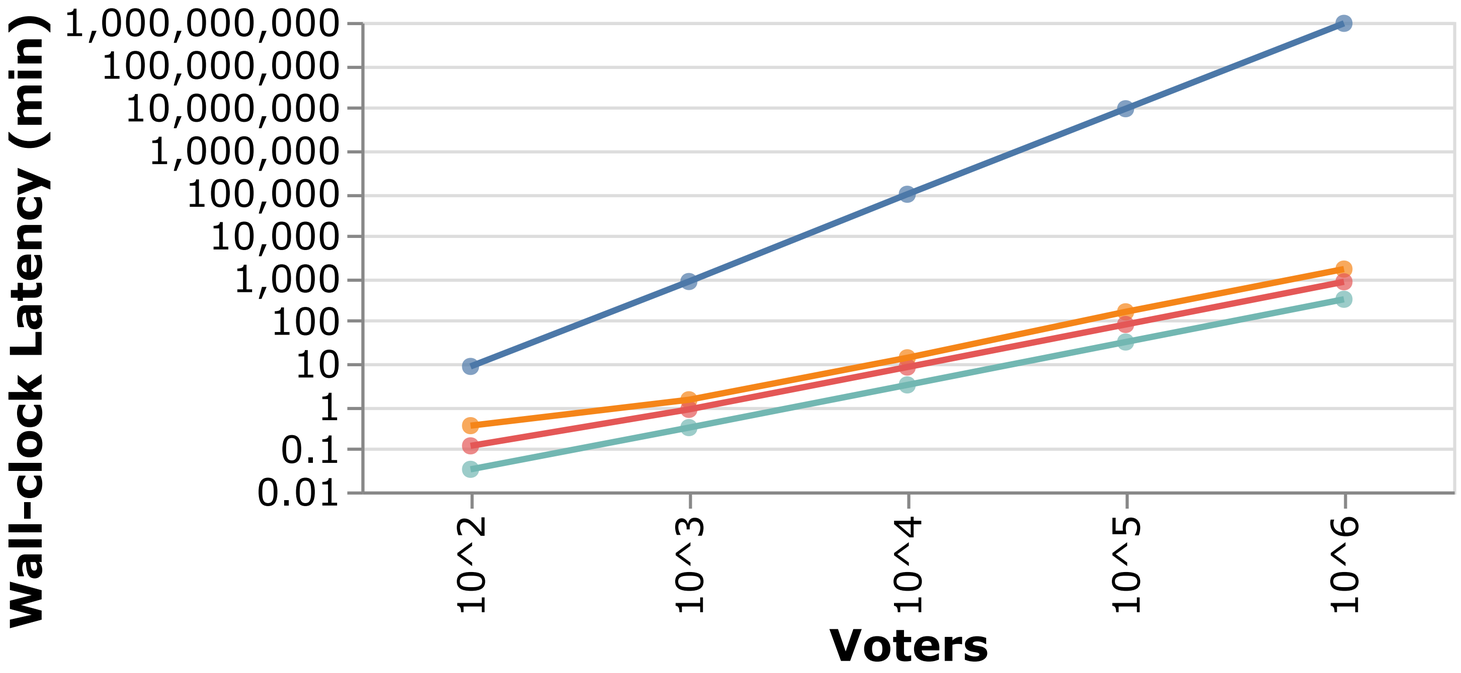
Falsely prove for **Alice's coercers** that T_A is a correct ElGamal encryption of F_A

$$T_A = \text{ElGamal}(F_A, \underbrace{x \in Z_q}_{\text{Unknown}})$$



- Real and fake credentials *indistinguishable* outside privacy booth
- Voters can *procedurally* distinguish real and fake credentials (3 vs 2 steps)

End-to-End Coercion-Resistant Verifiable E-Voting System



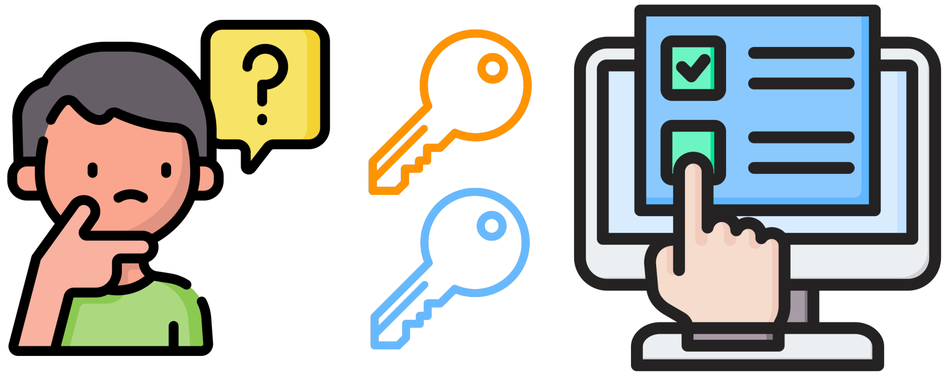
System
- Civitas
- SwissPost
- VSYS-Tally
- VoteAgain

- **1 million voters**
  - Civitas: 1,768 years
  - Swiss Post: 27 hours
  - **Votegral: 14 hours**
  - VoteAgain: 5 hours

- Votegral achieves **comparable latency** to the state-of-the-art voting systems
- Votegral **significantly outperforms Civitas**, the closest comparable system

Usability

Comprehension?



Distinguish Real from Fake?

User Study

- 150 participants
- Suburban Park in Boston, Massachusetts, U.S.A.

Instructional Video → **Registration** → **Vote** → **Survey**

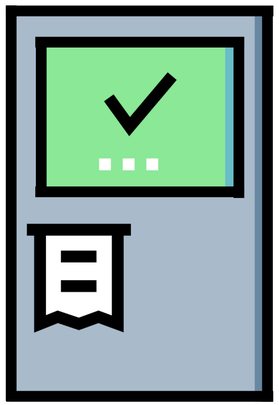
~30 min per participant

User Study Results

Comprehension

96%

Create Credentials



95%

Activate Credential

92%

87%

Vote with Real Credential

90%

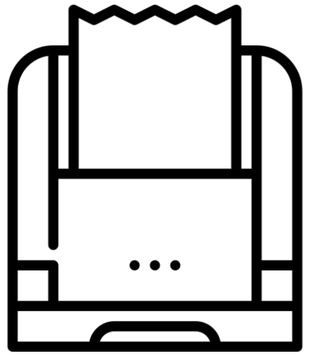
83%

Roadmap

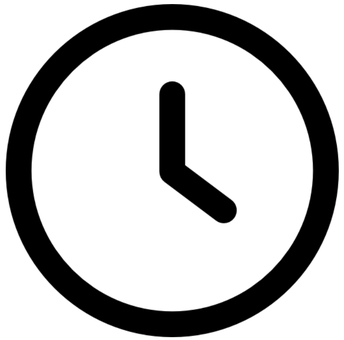
- Coercion-Resistance
- TRIP Registration Protocol
- **Limitations and Conclusion**

TRIP Limitations

- Side Channel Attacks



Printer Noise



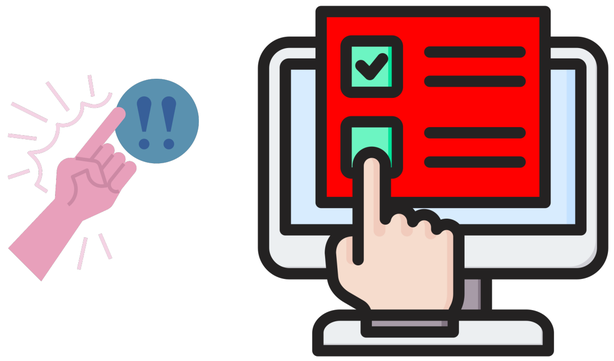
Timing Attacks

Electromagnetism

- Lack of post-quantum security: Scheme based on Discrete Logarithm

Conclusion

Coercion Problem



Interactive ZK Proofs

Real Credential
(Non-Transferable Proof)

Fake Credential
(False Proof for
Coercion-Resistance)

TRIP Usability

STAR-Vote: 93%

Online Voting

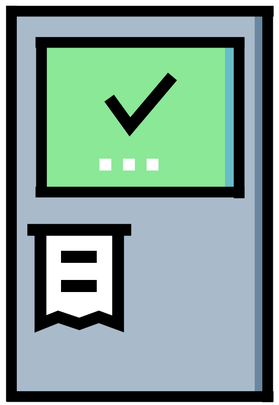
TRIP
83%

Helios: 60%

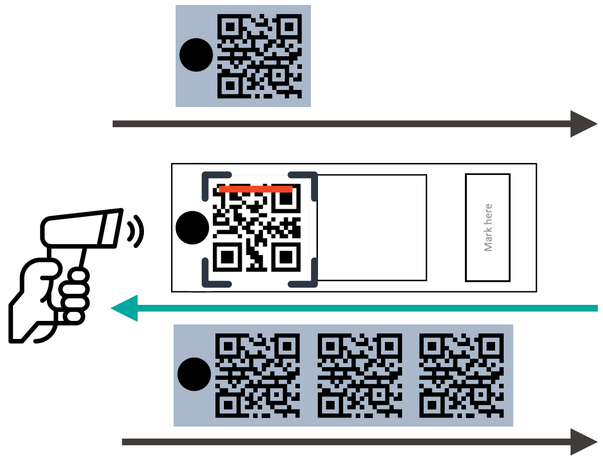
Prêt à Voter: 60%

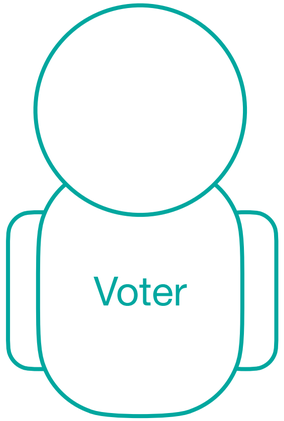
Real Credential Creation Process

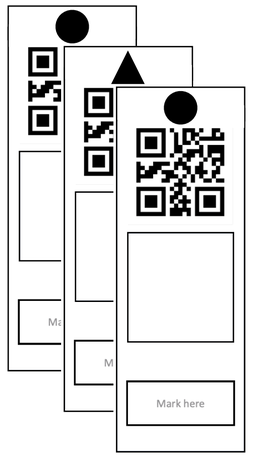
(with an interactive zero-knowledge proof)



Kiosk





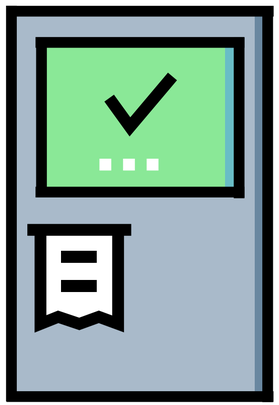


Envelopes

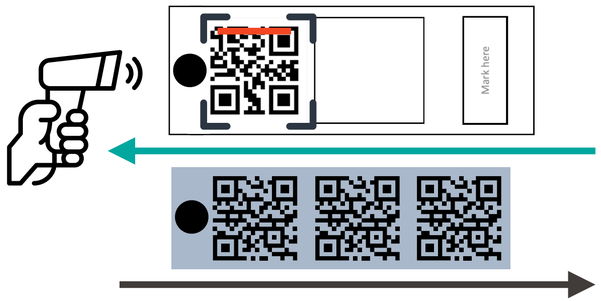
Pen

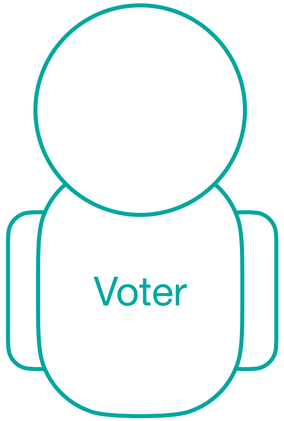
Voter **presents** envelope after kiosk prints **first** QR code

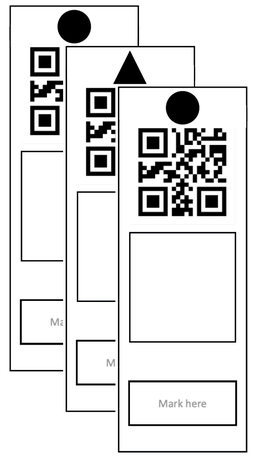
Fake Credential Creation Process



Kiosk







Envelopes

Pen

Voter **presents any** unused envelope