Threat models

Basics of threat modelling

- Threat actors
- Adversaries
- Capabilities of adversaries
- Trust vs verifiability
- Clear articulation of all trust points

Case study: Authentication and KYC

Trust model of old-fashioned identity cards

- Presenter trusted?
- Verifier trusted?
- KYC based on identity documents?

Trust model of old-fashioned identity cards

- Presenter trusted?
- Verifier trusted?
- KYC based on identity documents?
    - Possibilities of repurposing?
- Vacuous?

Trust model of smart cards with chips

- Content trustworthy?
    - Under what conditions?
- Presenter?
- Verifier?
- Verifier machine?

Trust model of Aadhaar Based Biometric Authentication

- No trust requirement on presenter?
- What about verifier?

Trust model of Aadhaar Based Biometric Authentication

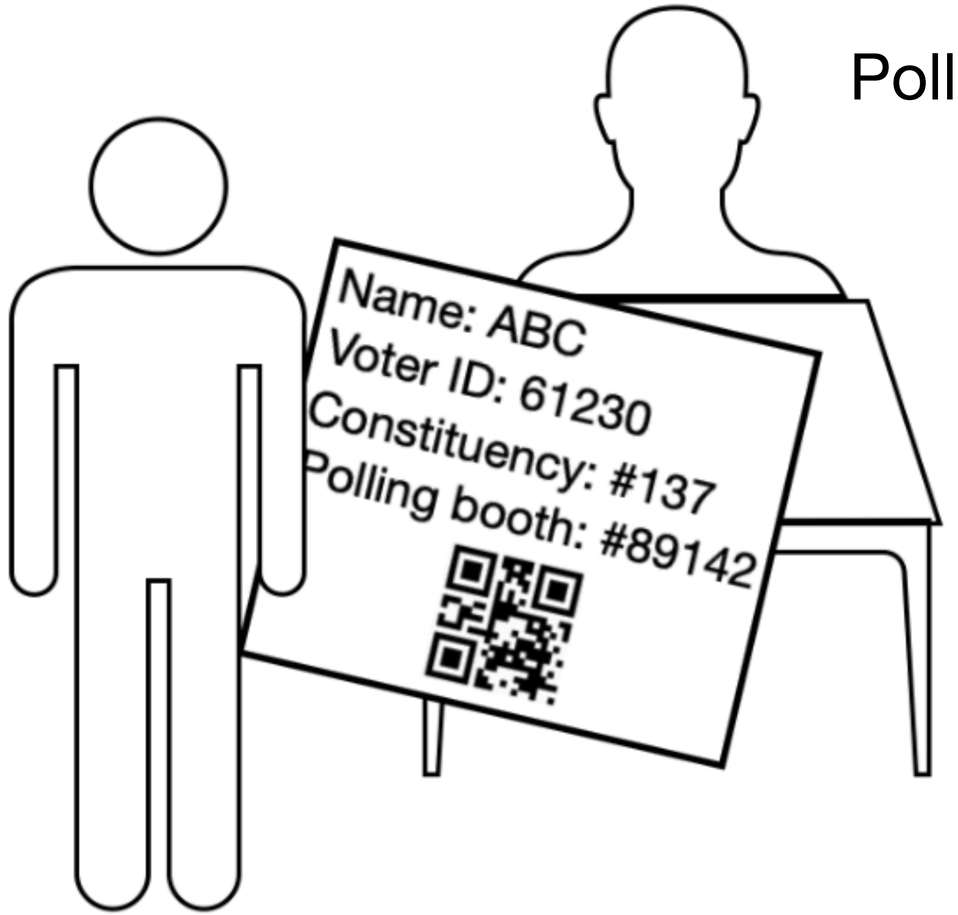
- No trust requirement on presenter?
- What about verifier?
    - Assume cannot control backend
    - False authorisation and/or accounting?
    - Store and replay?
- What if authentication outcome is routed through the verifier?

Trust models of other authentication methods?

- Passwords
- Ssh authentication (Diffie-Helman key exchange)
- Kerberos authentication

Case study: elections

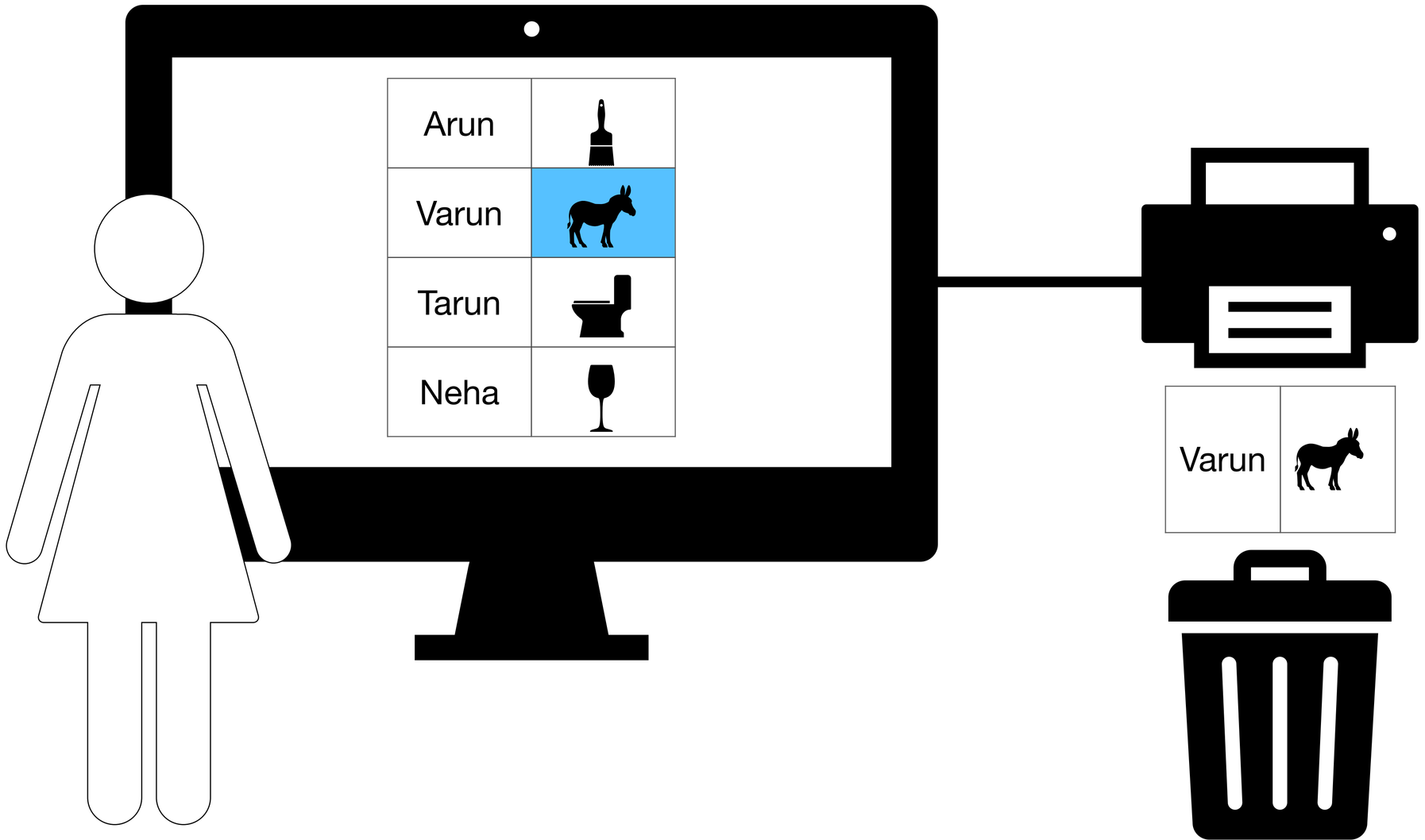
Identity and eligibility verification



Polling officer

Also polling agents

EVM + VVPAT



Security threat analysis

Threat model

- Adversary can corrupt and control
    - An arbitrary set of polling officials
    - An arbitrary set of voters
    - Voting equipment

Voting requirements

- Correctness
    - Cast as intended
    - Recorded as cast
    - Counted as recorded
    - Only eligible voters and only 1 vote per eligible voters
    - Non-repudiation and dispute resolution
- Secrecy
    - Receipt free (voter should not be able to prove who she voted for)