Security and Privacy

risks and trust assumptions

Outline

- Introduction
- Security Objectives

Introduction

Some Swiss background:

- Swiss people vote four times a year at federal level and possibly more at cantonal and municipal level
  - Running federal votes and elections is delegated by the confederation to the cantons
  - The Federal Chancellery defines the rules for federal votes and elections
- Two well established channels:
  - Voting in person at poll booths
  - Voting by mail (over 90% of votes)
- One experimental third channel
  - Voting over Internet (called e-voting, in Switzerland) is possible experimentally since 2014
  - The laws are being adapted to make it an official 3rd channel

Security Objectives

- Accuracy:
  - the result reflects the choice of the voters
- Secrecy:
  - The vote of each voter remains secret
- Absence of provisional results:
  - There is no information about provisional results during the election

Across all channels (booth, mail, Internet)

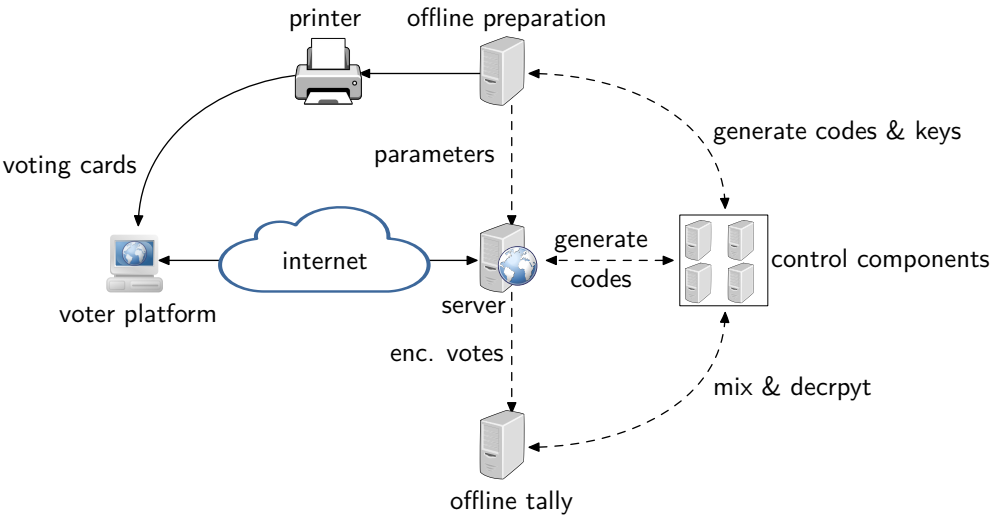
Typical Risks for e-voting

- Accuracy:
  - Manipulation of votes (on the voter's machine while voting, during transmission over Internet, by hacking the servers)
  - Fake votes, given without authorization (voting card)
  - Double votes (possibly. over two channels)
- Secrecry
  - Interception of votes (on the voters machine while voting, during transmission over Internet, by hacking servers)
- Absence of provisional results:
  - Interception of votes (on the voters machine while voting, during transmission over Internet, by hacking servers)

Verifiable e-voting protocols

- Verifiable e-voting protocols reduce the risk
  - they allow to verify that the votes have not been manipulated
- Individual verifiability
  - An individual has proof that their vote has been correctly taken into account
    - protects against a man-in-the-browser that changes outgoing votes and incoming confirmation (you think you voted 'yes' but you voted 'no')
- Universal verifiability
  - We have proof that all votes have been correctly counted
    - protects against attacks on the server, that delete, add or modify some votes

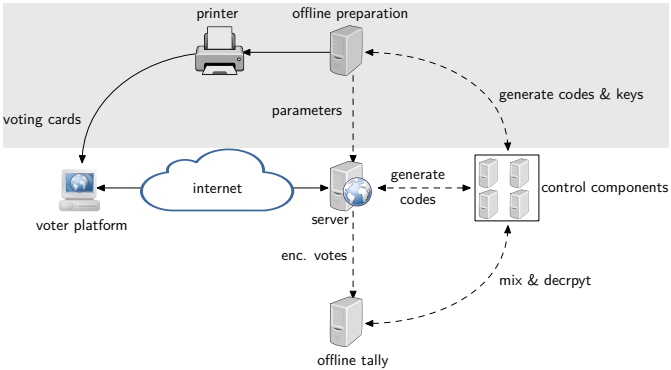
Elements of the e-voting systems



3 Phases

1. Preparation

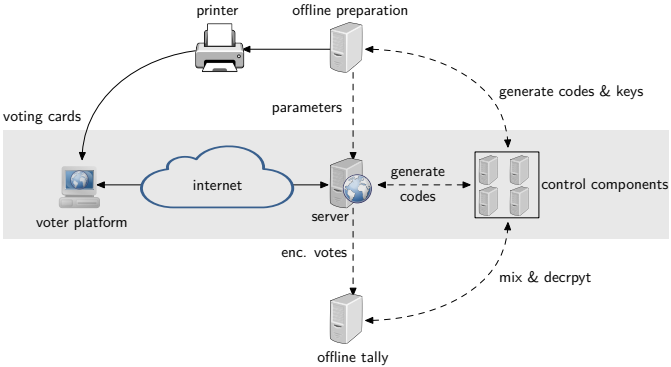
- Key pairs are generated
- Printer gets data to print on voting card
- Cards are sent to voters
- Server gets parameters



3 Phases

2. Voting

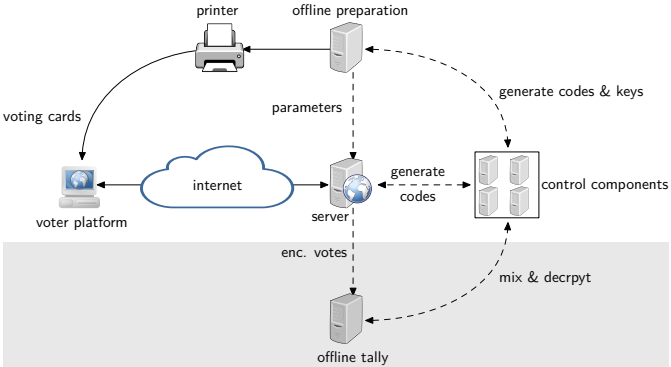
- Voter use voting card to cast vote
- Platform encrypts vote and generate proofs
- Server generates codes and proofs with CCs
- Voter confirms that codes are correct



3 Phases

3. Tallying

- Votes are mixed by CCs
  ➡ anonymity
- Votes are decrypted by CCs and tallied



Trust model

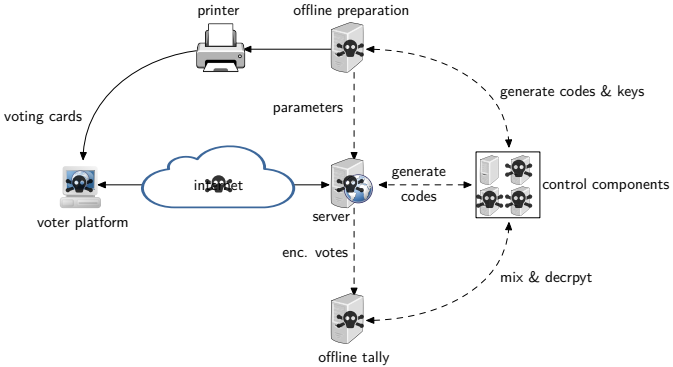
- If we can't trust anybody, we can't have security.
- Explicit trust:
  - the printer
    - because it is off-line and physically secured
  - one in of 4 CCs
    - because they are independent
  - postal mail
    - because it is already trusted
- Implicit trust:
  - cryptography (encryption, proofs)
  - implementation of crypto in CCs

Trust model

- There are four control component (CC)  that carry out all critical operations
  - generation of keys
    - each CC generates a part of the keys
    - nobody know the full private keys
  - mixing
    - each CC mixes and anonymizes the votes
  - decryption
    - each CC participates to the decryption
  - logging of these operation
  - Zero knowledge proofs that all operations where executed correctly
- A group of (4 or more) auditors verify all the proofs in the end
- If at least one CC and one auditor are honest, no manipulation is possible!
  ➡ vote correctness and vote secrecy are guaranteed

Trust model

- The platform is not trusted
- The servers are not trusted
- The internet is not trusted
- 3 out of 4 CCs are not trusted
- The protocol must still guarantee vote correctness, secrecy and no provisional results



- note: the platform is trusted for keeping the vote secret