

Security and Privacy

E-voting protocols in Switzerland

28.05.2019

Ph. Oechslin



Outline

- Security objectives
- Security levels and trust models
- Example
- Current situation in Switzerland

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

Main Security Objectives

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

Across all channels (booth, mail, Internet)

Typical Risks for e-voting

■ Accuracy:

- ▶ Double votes (e.g. over two channels)
- ▶ Manipulation of votes (e.g. on the voters machine while voting, during transmission over Internet, by hacking servers)
- ▶ Fake votes, given without authorization (voting card)

■ Secrecry

- ▶ Interception of votes (e.g. on the voters machine while voting, during transmission over Internet, by hacking servers)

■ No provisional results:

- ▶ Interception of votes (e.g. on the voters machine while voting, during transmission over Internet, by hacking servers)

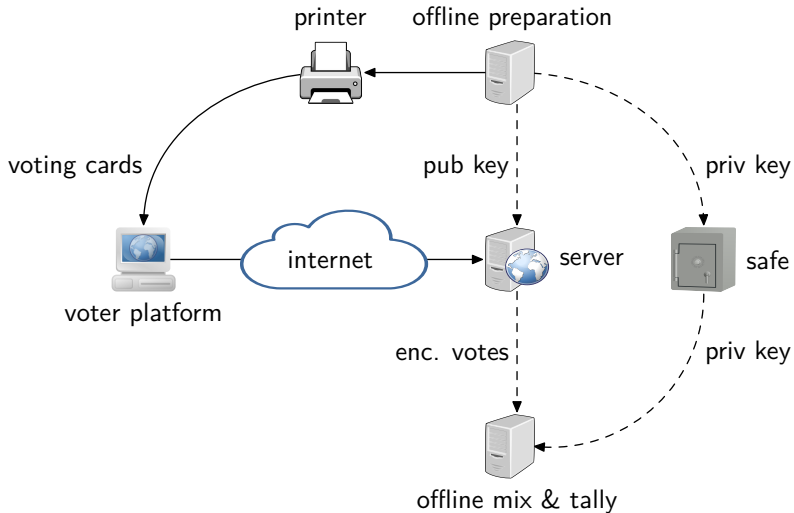
Verifiable e-voting protocols

- To limit the risks, we can use verifiable e-voting protocols.
 - ▶ they allow to verify if the results have 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

Security levels

- Switzerland has defined three security levels
 - ▶ The higher the level, the more people may be allowed to use it
- Up to 30% of the electorate:
 - ▶ no verifiability is required
 - ▶ ad hoc testing must be done
- Up to 50% if the electorate:
 - ▶ individual verifiability is required
 - ▶ system must be certified by an accredited company
- Up to 100% of the electorate:
 - ▶ complete verifiability (individual & universal) is required
 - ▶ system must be certified by an accredited company
- Both the provider of the e-voting system and the cantons using it must be certified

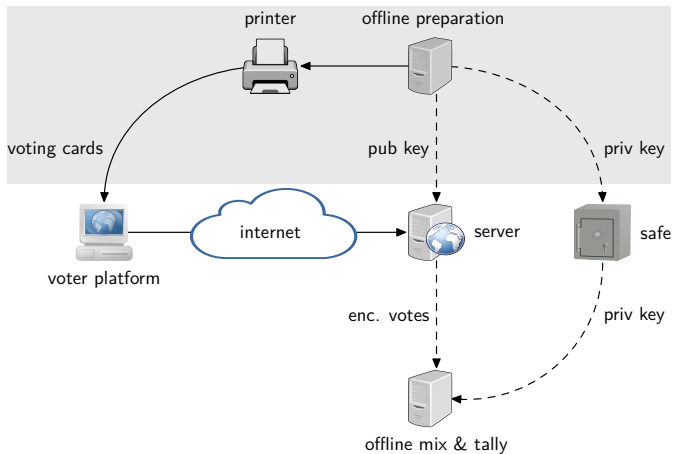
Elements of the e-voting systems



3 Phases

Preparation

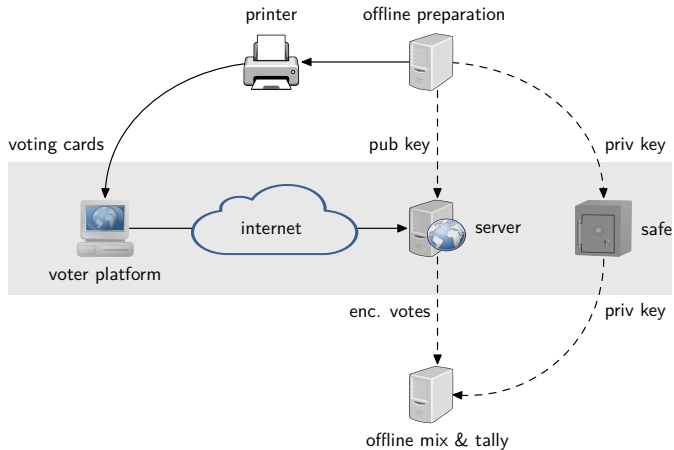
- Key pairs are generated
- Printer gets data to print on voting card
- Cards are sent to voters
- Server gets public key
 - ▶ with USB stick
- Private key is stored in police safe



3 Phases

Voting

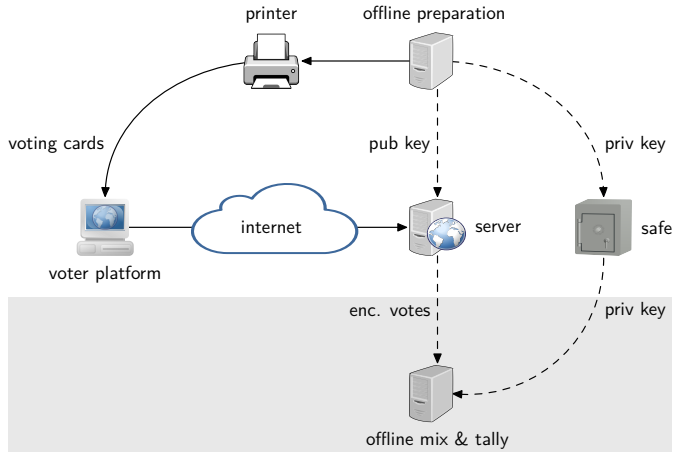
- Voter use voting card to cast vote
- Server encrypts vote



3 Phases

Tallying

- Encrypted votes are transferred to offline server
 - ▶ with USB stick
- Private key is taken from police safe
- Votes are mixed
 - ▶ to guarantee anonymity
- Votes are decrypted and tallied



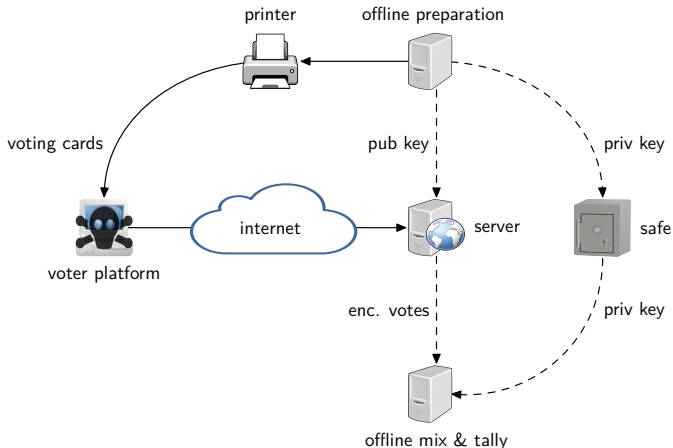
Trust model

- For up to 30% of the electorate
- All elements are trusted ($>$) If they are hacked, they could change the outcome
- We need very good security controls
 - ▶ machine hardening
 - ▶ physical, network and user access control
 - ▶ segregated teams for different jobs (e.g. $\text{dev} \neq \text{ops} \neq \text{monitor}$)
 - ▶ four-eyes principle for critical operations
 - e.g. two people are needed retrieve the priv. key from safe
 - ▶ everything is monitored and logged
 - ▶ test votes are given before and during the voting phase
 - results of tests are verified
 - ▶ e-vote results are compared statistically to votes from other channels

Trust model

For up to 50%

- The platform is not trusted
- The protocol must guarantee vote correctness even if the platform is hacked
 - ▶ voting card contain **verification codes**
 - ▶ when vote is received, server sends back verification codes
 - ▶ voter compares codes on screen, with codes on voting card
- the platform is trusted for keeping the vote secret !



Example: FR (Post)

- Receive voting card by postal mail
- Log in e-voting portal with **Initialization code**
- Make your selection and transmit the vote
- Receive the **verification codes**
- If codes are correct, confirm vote with **confirmation code**
- Receive **finalization code** as confirmation.

Voting card

■ Voting card:

Vote électronique / E-Voting

Adresse / Web-Adresse : <https://evoting.fr.post.ch/>

Empreinte numérique / Fingerprint: 01:33:50:A9:1B:81:9B:43:28:99:DF:60:CA:89:91:80:CD:79:76

A saisir à la fin de la sélection des votes / Muss nach der Stimmabgabe erfasst werden.

**Code d'initialisation /
Stimmrechtsausweisschlüssel :**
**hcq6 - yppx -
wbg7 - c5yi - 8au6**

A saisir après le contrôle des codes de vérification / Muss nach der Kontrolle der Prüfcodes erfasst werden.

**Code de confirmation /
Stimmabgabeschlüssel :**
517 - 980 - 031

A contrôler après la génération de l'accusé de réception / Muss nach der Generierung der Empfangsbestätigung kontrolliert werden.


**Code de finalisation /
Stimmabgabenummer :**
8871 - 2923

Votation du 02.05.2016 - codes de vérification / Wahl vom 02.05.2016 - Wahlentscheidungscode

Vous trouverez tous vos codes de vérification ci-dessous / Sie finden alle Ihre Wahlentscheidungscode auf den beiliegenden Seiten.

N°	Objets fédéraux / Abstimmungsgegenstand	Codes de vérification / Wahlentscheidungscode				
		Oui / Ja	Non / Nein	Blanc / Leer	Initiative / Initiative	Contre-projet / Gegenentwurf
1a	Initiative populaire: Acceptez-vous l'initiative populaire «pour le versement au fonds AVS des réserves d'or excédentaires de la Banque nationale suisse (Initiative sur l'or)? Volksinitiative: Wollen Sie die Volksinitiative «Überschüssige Goldreserven in den AHV-Fonds (Goldinitiative)» annehmen?	3725	2856	4189		
1b	Contre-projet: Acceptez-vous le contre-projet de l'Assemblée fédérale «l'or à l'AVS, aux cantons et à la Fondation»?	4955	3076	3560		

Verifying the codes

 ÉTAT DE FRIBOURG
STANT FRIBOURG

[Aide](#) [FR](#) [Quitter le processus](#)

Sélection

Vérifier et sceller

Vérifier et enregistrer

Vote enregistré


✓

✓

3

4

Examinez les codes de vérification générés ci-dessous. Pour enregistrer votre bulletin, veuillez vérifier qu'ils correspondent à ceux inscrits sur votre carte d'électeur.



Codes de vérification [De quoi s'agit-il?](#)

1. Votation populaire du 22 septembre 2002

Vos codes de vérification

Initiative populaire: Acceptez-vous l'initiative populaire «pour le versement au fonds AVS des réserves d'or excédentaires de la Banque nationale suisse (Initiative sur l'or)»?

3725

Oui

Contre-projet: Acceptez-vous le contre-projet de l'Assemblée fédérale «l'or à l'AVS, aux cantons et à la Fondation»?

4955

Oui

Question subsidiaire: Si le peuple et les cantons acceptaient à la fois l'initiative populaire «pour le versement au fonds AVS des réserves d'or excédentaires de la Banque nationale suisse (Initiative sur l'or)» et le contre-projet «L'or à l'AVS, aux cantons et à la Fondation»: Est-ce

5561

Trust model

For up to 100%

- The servers are not trusted either

- Instead, 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

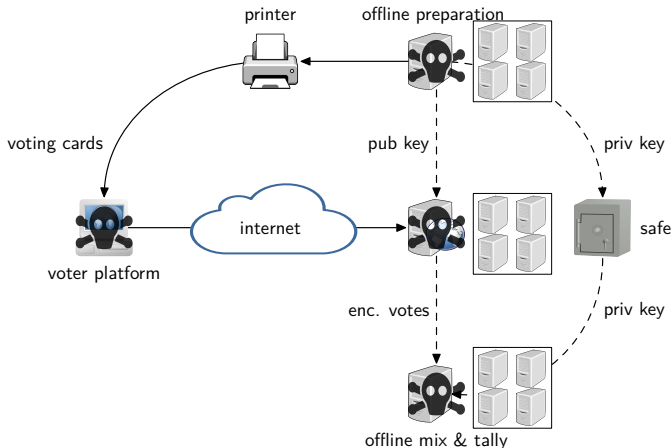
- A group of (4 or more) auditors verify all the proofs in the end

- If at least one CC and one auditor are honest, no manipulation is possible!
 - ▶ vote correctness and vote secrecy are guaranteed

Trust model

For up to 100%

- The platform is not trusted
- The servers are not trusted
- Only 1 in 4 CCs is trusted
- The protocol must still guarantee vote correctness and no preliminary results
 - ▶ keys are generated by the CCs
 - ▶ return codes are calculated by CCs
 - ▶ mixing and decryption is done by CCs
- the platform is still trusted for keeping the vote secret !



Current situation in Switzerland

- Two providers: Canton of Geneva (**GE**) and Swiss Post (**Post**)
 - ▶ GE: open source development with help of BFH (Bern University of Applied Sciences)
 - ▶ Post: commercial solution from Spanish company ScytI
- The systems are mainly used for Swiss citizens abroad
 - ▶ efficient alternative to mail voting
- Some cantons also use it for their citizens in Switzerland (GE, NE, SG)

GE system

- Used by BE, LU, SG, AG, VD, GE
- old system: individual verifiability, simple, no end-to-end encryption
 - ▶ partially open-source
 - ▶ tested and in use
- new system: complete verifiability, end-to-end encryption
 - ▶ fully open-source
 - ▶ not yet certified
 - ▶ development stopped in fall 2018 (budget and time issues)

Post system

- Used by NE, FR, TG, BS
- old system: individual verifiability, end-to-end encryption, protocol allows complete verifiability
 - ▶ certified for 50% (but cantons not yet)
 - ▶ off-line since February, because flaw in implementation of indiv. verif.
- new system: complete verifiability, same protocol but with distributed trust
 - ▶ was certified in January
 - ▶ source code publication in February
 - flaw discovered in indiv. verif.
 - ▶ not in service yet