Improvements to CHvote

Towards an end-to-end verifiable voting system

REPUBLIQUE ET CANTON DE GENEVE

POST TENEBRAS LUX

Département de la sécurité et de l'économie
Direction générale des systèmes d'information

Short Bio

Thomas Hofer / @thhofer / thomas.hofer@etat.ge.ch

- EPFL MSc in IT
- IT / Java consultant

- Now
  - → Internet voting cryptography @ State of Geneva
  - → Java DEV & AppSec

- Outside from work
  - → OWASP-Geneva co-chapter leader
  - → Married, 2 kids

Outline

- Security properties & challenges
- CHvote: a brief history
- Federal requirements
- The future: protocol overview
- Questions

Outline

- Security properties & challenges
- CHvote: a brief history
- Federal requirements
- The future: protocol overview
- Questions

Security properties

Target security properties

Vote secrecy

Result integrity

Enfranchisement

Availability

Voter authentication

No early tally

Security challenges

Partially contradicting requirements and other challenges

- Vote secrecy vs. result integrity
  - → Cryptographically challenging (but feasible)

- Enfranchisement vs. authentication
  - → Typically opposed
  - → But: in CH, voting legitimation cards are sent to voters (Swiss Post is trusted)
  - → For mail-in ballots / polling station voting:
    - – Voting card + signature + DOB
  - → For internet voting:
    - – Secrets printed on voting card + DOB

Security challenges

Partially contradicting requirements and other challenges (ctd.)

- Availability
  - → OK, but… DDOS??
  - → Standard technical counter-measures
  - → Internet voting closes 24 hours before polling stations

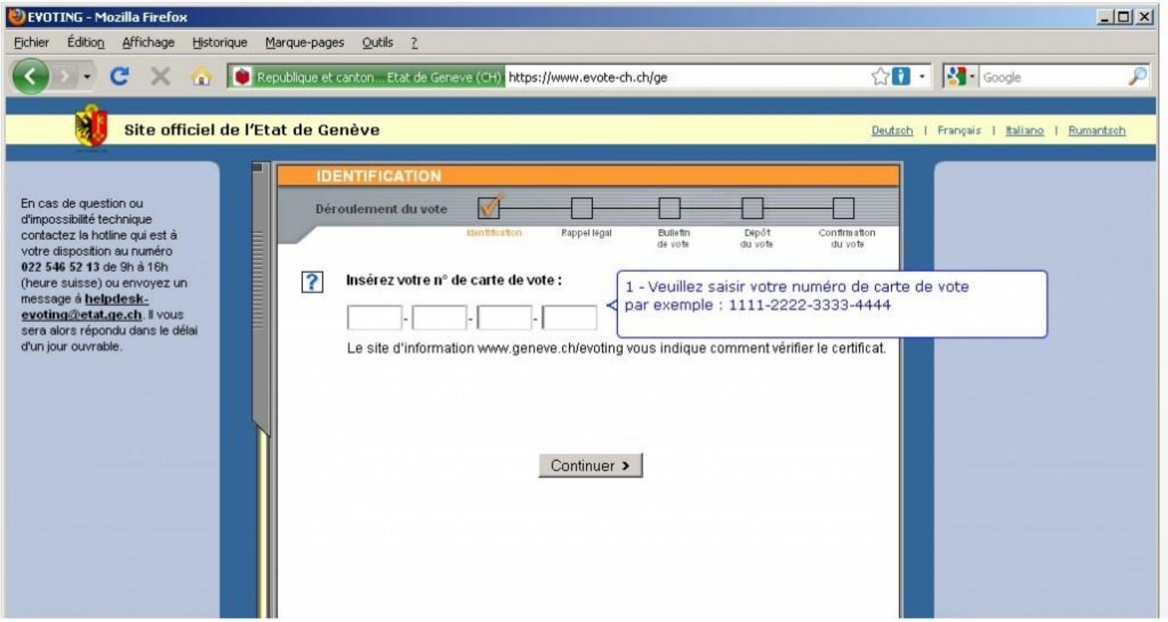
Outline

- Security properties & challenges
- CHvote: a brief history
- Federal requirements
- The future: protocol overview
- Questions

The past of CHvote

First generation E-Voting system

- 2001: start of project
- 2003: first use


EVOTING - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
Republique et canton... Etat de Geneve (CH) https://www.evote-ch.ch/ge
Google
Site officiel de l'Etat de Genève
Deutsch | Français | Italiano | Rumantsch
IDENTIFICATION
Déroulement du vote
Identification
Rappel légal
Bulletin de vote
Dépôt du vote
Confirmation du vote
Continuer ›

En cas de question ou d'impossibilité technique contactez la hotline qui est à votre disposition au numéro **022 546 52 13** de 9h à 16h (heure suisse) ou envoyez un message à **helpdesk-evoting@etat.ge.ch**. Il vous sera alors répondu dans le délai d'un jour ouvrable.

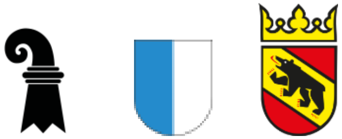
Insérez votre n° de carte de vote :

□ - □ - □ - □

1 - Veuillez saisir votre numéro de carte de vote
par exemple : 1111-2222-3333-4444

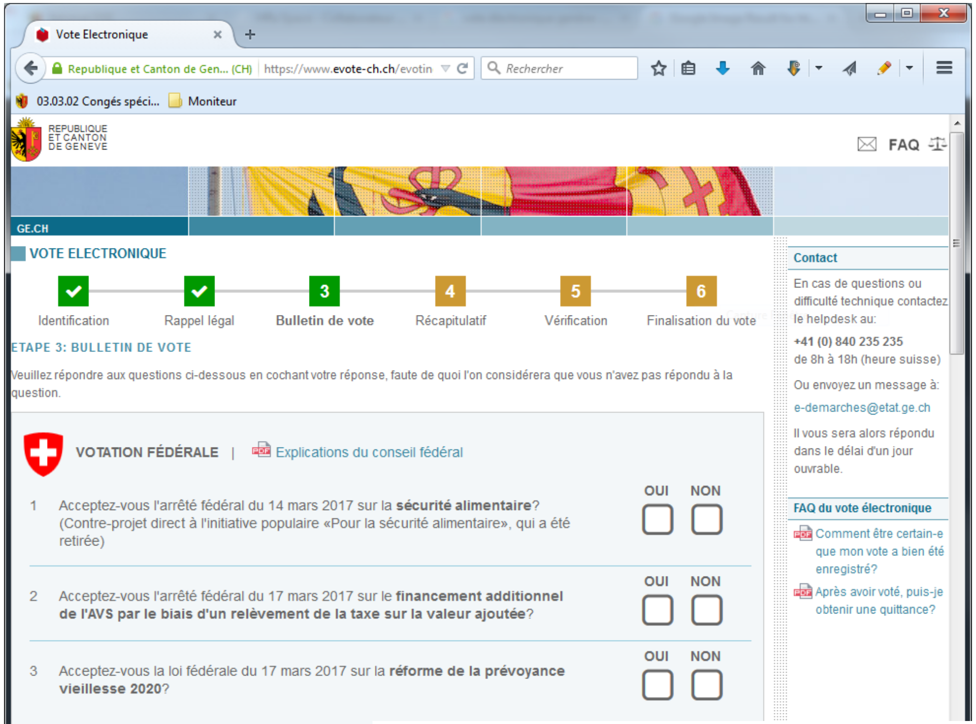
Le site d'information www.geneve.ch/evoting vous indique comment vérifier le certificat.

- Partners



The present of CHvote

Individual verifiability & major appearance overhaul



Vote Electronique
Republique et Canton de Gen... (CH) | https://www.evote-ch.ch/evotin
Rechercher
03.03.02 Congés spéci...
Moniteur
REPUBLIQUE ET CANTON DE GENEVE
FAQ
GE.CH

VOTE ELECTRONIQUE

✓ Identification — ✓ Rappel légal — 3 Bulletin de vote — 4 Récapitulatif — 5 Vérification — 6 Finalisation du vote

ETAPE 3: BULLETIN DE VOTE

Veuillez répondre aux questions ci-dessous en cochant votre réponse, faute de quoi l'on considérera que vous n'avez pas répondu à la question.

VOTATION FÉDÉRALE | Explications du conseil fédéral

		OUI	NON
1	Acceptez-vous l'arrêté fédéral du 14 mars 2017 sur la **sécurité alimentaire**? (Contre-projet direct à l'initiative populaire «Pour la sécurité alimentaire», qui a été retirée)	□	□
2	Acceptez-vous l'arrêté fédéral du 17 mars 2017 sur le **financement additionnel de l'AVS par le biais d'un relèvement de la taxe sur la valeur ajoutée**?	□	□
3	Acceptez-vous la loi fédérale du 17 mars 2017 sur la **réforme de la prévoyance vieillesse 2020**?	□	□

Contact

En cas de questions ou difficulté technique contactez le helpdesk au:

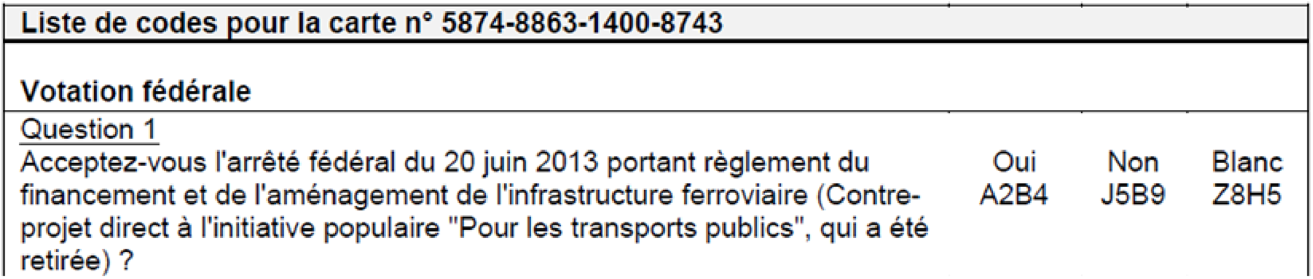
+41 (0) 840 235 235
de 8h à 18h (heure suisse)

Ou envoyez un message à:
e-demarches@etat.ge.ch

Il vous sera alors répondu dans le délai d'un jour ouvrable.

FAQ du vote électronique

- Comment être certain-e que mon vote a bien été enregistré?
- Après avoir voté, puis-je obtenir une quittance?



Liste de codes pour la carte n° 5874-8863-1400-8743

Votation fédérale

Question 1

Acceptez-vous l'arrêté fédéral du 20 juin 2013 portant règlement du financement et de l'aménagement de l'infrastructure ferroviaire (Contre-projet direct à l'initiative populaire "Pour les transports publics", qui a été retirée) ?	Oui A2B4	Non J5B9	Blanc Z8H5

The future of CHvote

End-to-end verifiable internet voting protocol

- New academic partnerships
  - → Berner Fachhochschule
  - → INRIA / Bristol
  - → ITU Copenhagen
  - → EPFL

- New cryptographic protocol
  - → End-to-end encryption
  - → Universal Verifiability
  - → Control Components

- Currently in development, ETA: 2019

Outline

- Security properties & challenges
- CHvote: a brief history
- **Federal requirements**
- The future: protocol overview
- Questions

Federal requirements

New Ordinance on Electronic Voting

- Published in 2013, enacted 2014
  - → Collaborative work between lawmakers, academia and operating staff

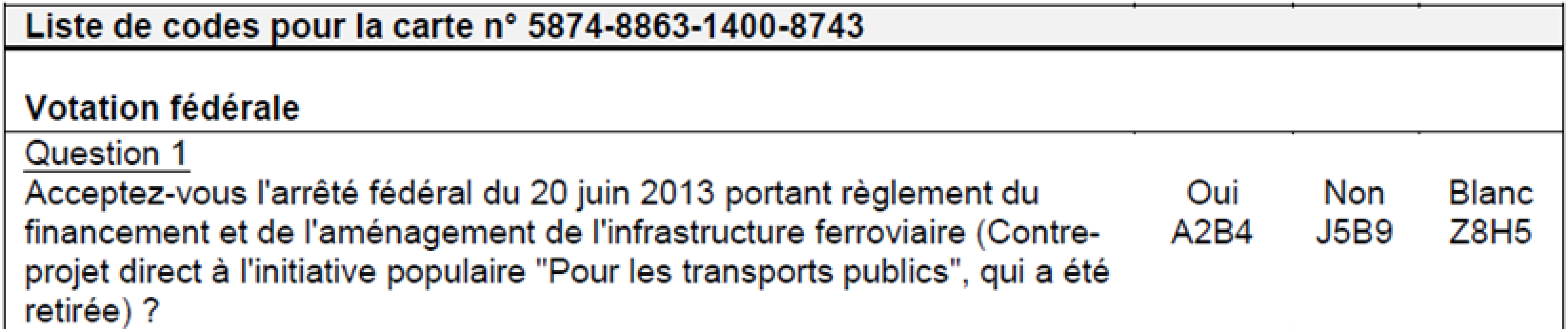
- Compliance levels
  - → The higher the compliance, the more voters allowed

- Reference
  - → https://www.bk.admin.ch/themen/pore/evoting/07979/index.html

Federal requirements

Individual Verifiability

Voters must receive proof that the server system has registered the vote as it was entered by the voter on the user platform – *VEleS, art. 4*



Liste de codes pour la carte n° 5874-8863-1400-8743			
Votation fédérale			
Question 1 Acceptez-vous l'arrêté fédéral du 20 juin 2013 portant règlement du financement et de l'aménagement de l'infrastructure ferroviaire (Contre-projet direct à l'initiative populaire "Pour les transports publics", qui a été retirée) ?	Oui A2B4	Non J5B9	Blanc Z8H5

Federal requirements

End-to-End Encryption

Votes must not be stored or transmitted in unencrypted form at any time from being entered to tallying. – *Technical and administrative requirements, section 3.3.4*

Federal requirements

Universal Verifiability

> For universal verification, the auditors receive proof that the result has been ascertained correctly. They must evaluate the proof in a observable procedure.
> – *VEleS, art. 5 paragraph 4*

Federal requirements

Control Components

The trustworthy part of the system includes either one or a small number of groups of independent components secured by special measures (control components). Their use must also make any abuse recognisable if per group only one of the control components works correctly and in particular is not manipulated unnoticed. – *VEleS, art. 5, par. 6*

Federal requirements

Compliance levels

- First level
  - → Individual verifiability
  - → Internet voting for up to 30% of voters
- Second level
  - → Add certifying audit
  - → Internet voting for up to 50% of voters
- Third level
  - → Add universal verifiability, control components and end-to-end encryption
  - → New certifying audit
  - → Internet voting for up to 100% of voters

Outline

- Security properties & challenges
- CHvote: a brief history
- Federal requirements
- The future: protocol overview
- Questions

Protocol actors

Stakeholders from the perspective of the cryptographic protocol

Election officer

Control components

Bulletin Board

Printing Authorities

Voting client

Voter

Key cryptographic primitives

A brief overview

- El Gamal homomorphic encryption
- Oblivious Transfer for individual verifiability
  → Cast-as-Intended Verification in Electronic Elections Based on Oblivious Transfer
- Pedersen Commitments
- Non-interactive Zero-Knowledge Proofs (ZKP)
- Wikström’s Proof of a Shuffle

Homomorphic encryption

What is it?

- Principles
  - → Operations performed on cipher texts
  - → Result visible on recovered plain texts

  - → Example:
    - – Encrypt 2
    - – Multiply cipher text by 3
    - – Decrypt
    - – Result is 6

- For this project: El Gamal encryption

Homomorphic encryption

How and why?

- Used for voter credentials
  → **Voter authentication**

- Used for encrypting the ballots
  → **Vote secrecy**
- Allows re-encryptions
  → Useful for anonymizing when shuffling
  → **Vote secrecy**

- Allows for key sharing
  → Control components each hold a key share
  → **Vote secrecy & result integrity**

Oblivious Transfer

What does it mean and why is it useful?

- In short
  - → Server knows n secret messages
  - → Client allowed to retrieve k secret messages
  - → Server cannot know which messages the client asked for
  - → *Perfect match for the verification codes issue!*
  - → ***Vote secrecy & Result integrity***

- In detail
  - → Cast-as-Intended Verification in Electronic Elections Based on Oblivious Transfer

Commitments and ZKPs

How and why?

- “public” commitments for the secrets
  - → Share a value computed from secret, without leaking info

- ZKPs relative to those commitments
  - → Prove that
    - − Secret value used in computation =

      secret value used for commitment
  - → Chain of truth from key generation to ballot decryption

- Combination yields Universal verifiability
  - → **Result integrity**

Wikström’s Proof of a Shuffle

Why?

- Re-encrypting mix-net
  - → Each component re-encrypts each ballot and shuffles them

- Since shuffled, simple pre-image proofs would not work
- Since re-encrypted, ciphertexts are not equal
  - → **Vote secrecy**

- Need for a specific proof that the cryptographic shuffle is valid
  - → **Result integrity**

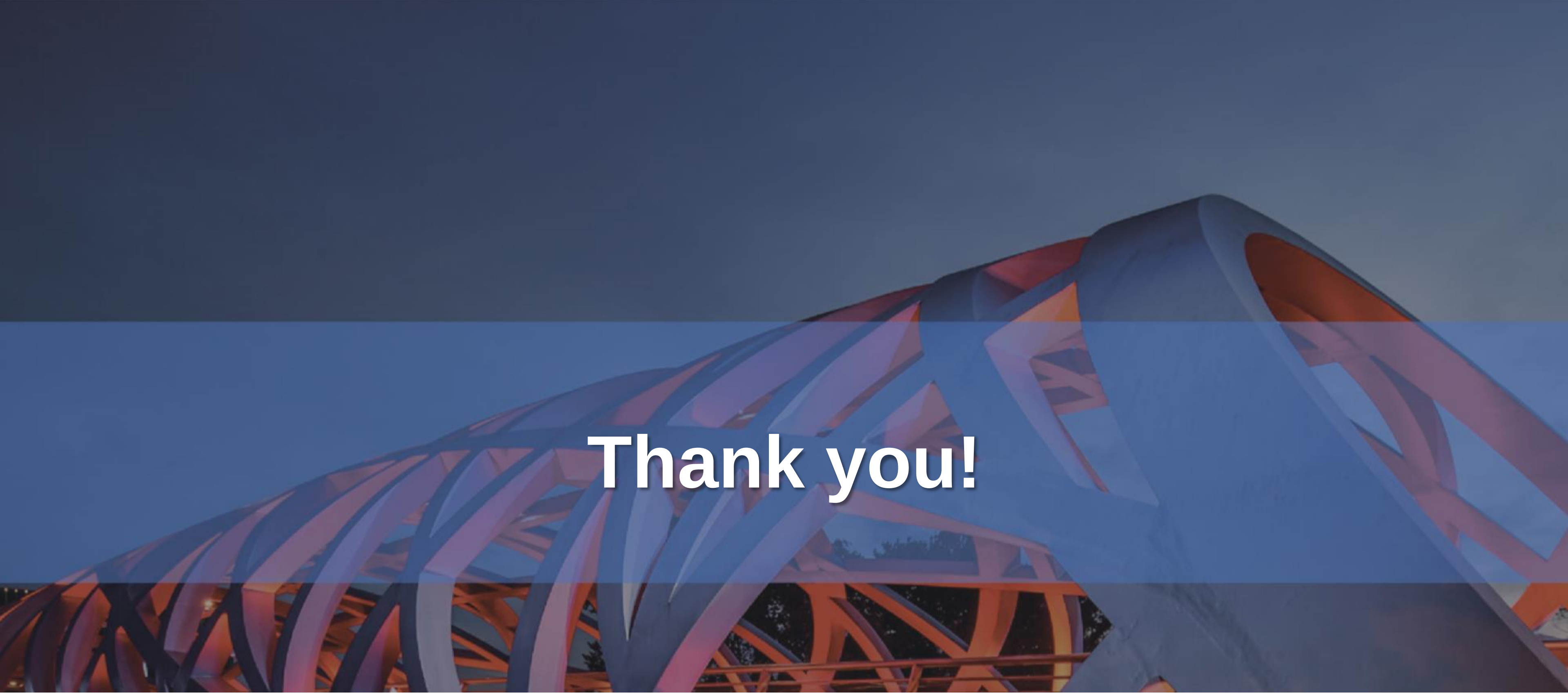
Outline

- Security properties & challenges
- CHvote: a brief history
- Federal requirements
- The future: protocol overview
- Questions

Further reading

And references

- Published protocol specification
  - → https://eprint.iacr.org/2017/325
- Published PoC code
  - → https://github.com/republique-et-canton-de-geneve/chvote-protocol-poc
- Federal requirements
  - → https://www.bk.admin.ch/themen/pore/evoting/07979/index.html



Thank you!

Thomas Hofer

thomas.hofer@etat.ge.ch

@thhofer