CHVote

Vote by internet

The Geneva system

REPUBLIQUE
ET CANTON
DE GENEVE

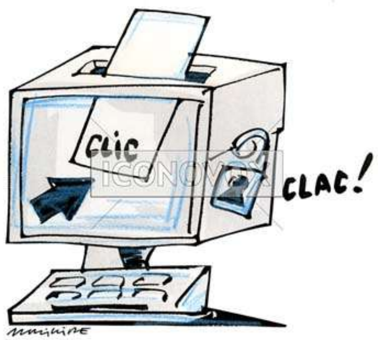
POST TENEBRAS LUX

Service d'audit interne

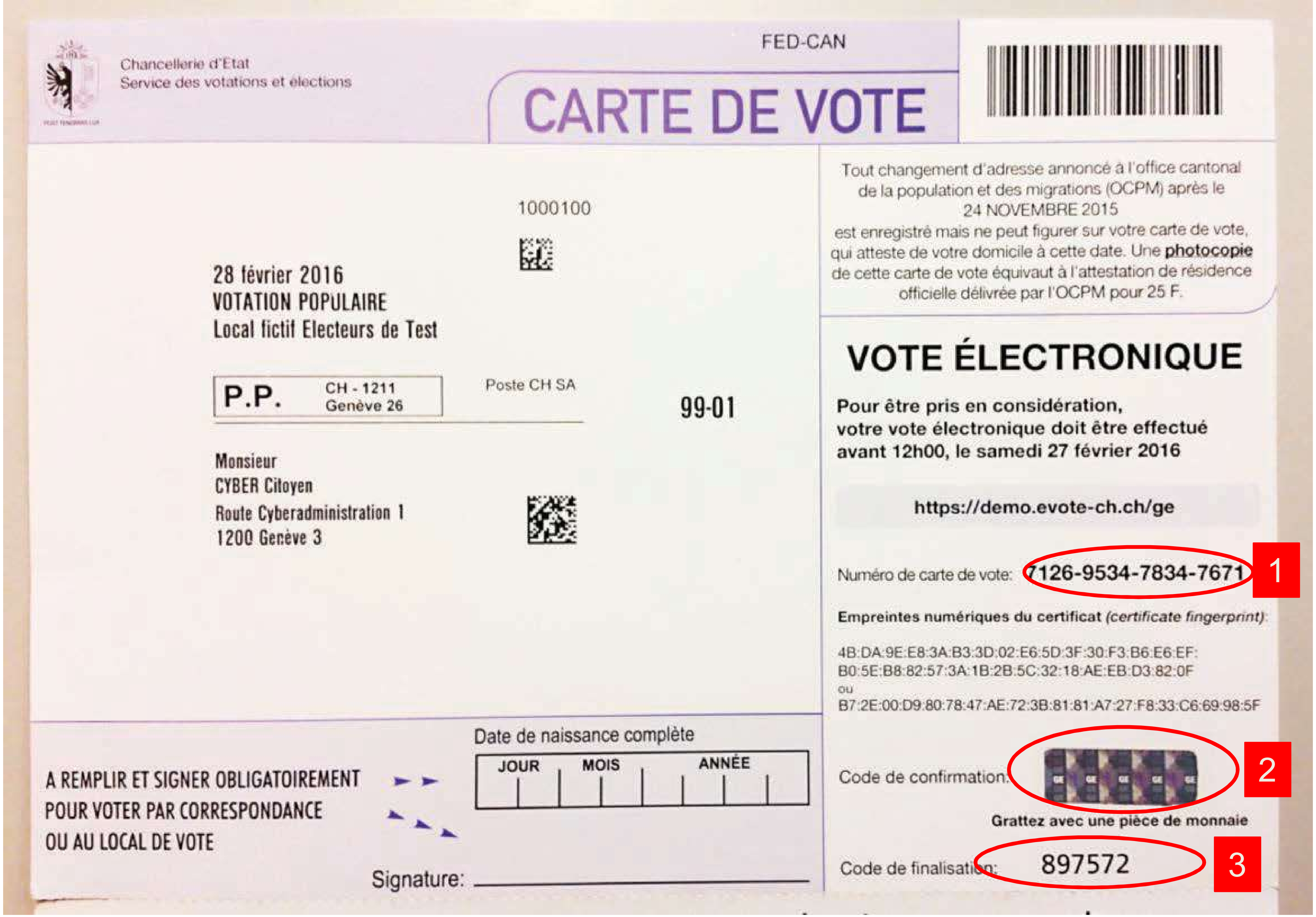
The vote in Switzerland

- 4 votes per year on federal, cantonal and communal subjects (initiatives, referendums).
- Regular elections of political representatives at these 3 levels.
- 3 possibilities: at the ballot box, by correspondence, by internet
- Voting material is sent to every citizen who has the right to vote.
- Internet voting requires prior registration.
- The voting card gives the necessary codes to access the vote by internet : verification codes, confirmation code, finalization code.

The voting procedure



- The citizen connects to the system using the authentication data.
- The citizen enters his vote and sends it to the electronic ballot box using the authentication data.
- The citizen receives confirmation that the vote has been recorded in the electronic ballot box and has not been changed.



Chancellerie d'Etat
Service des votations et élections

FED-CAN

CARTE DE VOTE

1000100

28 février 2016
VOTATION POPULAIRE
Local fictif Electeurs de Test

P.P. CH - 1211 Genève 26 — Poste CH SA

99-01

Monsieur
CYBER Citoyen
Route Cyberadministration 1
1200 Genève 3

Tout changement d'adresse annoncé à l'office cantonal de la population et des migrations (OCPM) après le 24 NOVEMBRE 2015 est enregistré mais ne peut figurer sur votre carte de vote, qui atteste de votre domicile à cette date. Une **photocopie** de cette carte de vote équivaut à l'attestation de résidence officielle délivrée par l'OCPM pour 25 F.

VOTE ÉLECTRONIQUE

Pour être pris en considération, votre vote électronique doit être effectué avant 12h00, le samedi 27 février 2016

https://demo.evote-ch.ch/ge

Numéro de carte de vote: **7126-9534-7834-7671**

Empreintes numériques du certificat *(certificate fingerprint)*:

4B:DA:9E:E8:3A:B3:3D:02:E6:5D:3F:30:F3:B6:E6:EF:
B0:5E:B8:82:57:3A:1B:2B:5C:32:18:AE:EB:D3:82:0F
ou
B7:2E:00:D9:80:78:47:AE:72:3B:81:81:A7:27:F8:33:C6:69:98:5F

Code de confirmation:

Grattez avec une pièce de monnaie

Code de finalisation: 897572

A REMPLIR ET SIGNER OBLIGATOIREMENT
POUR VOTER PAR CORRESPONDANCE
OU AU LOCAL DE VOTE

Date de naissance complète

JOUR	MOIS	ANNÉE

Signature: ______________________

The technical process

- Preparation of client authentication data, cryptographic keys and other system parameters.
- Information and support for electors and auditors.
- Preparation and printing of voting materials.
- Opening and closing of the electronic voting channel.
- Control of compliance and registration of final votes.
- Counting of the electronic ballot box.

The legal bases

- **Federal orders set the conditions for authorizing an administration to use electronic voting :**
  - The system guarantees the safety and reliability of the vote.
  - The system is easy to use for voters.
  - All technical and organizational operations that are relevant from the point of view of security must be documented in an understandable way.

- **A legal base in Geneva sets the requirements :**
  - Make the source code of e-voting applications public, thereby enhancing transparency and democratic control.
  - Frequently test system security.
  - Audit the system at least once every 3 years. The results of the audit are made public. The scope of the audit is not specified.

Security objectives

- Guarantee the accuracy of the result.
- Protect the secrecy of the vote and prohibit the establishment of partial results in advance.
- Ensure availability of features.
- Protect personal information about voters.
- Protect information intended for voters against manipulation.
- Prohibit establishing evidence of voting behavior.

Many threats (risks)

- An attacker reads, hijacks, modifies, creates, destroys votes.
- An administrator manipulates the votes.
- An administrator consults early votes.
- A DOS attack makes the system unavailable.
- An attacker enters the system to falsify the result.
- Malware modifies the vote on the user's platform.

Verification is therefore essential

- Individual verification
  - Every voter must have the means to control that :
    - His vote was sent to the system containing the official ballot box.
    - His vote has not been changed.
- Full verification
  - Auditors must receive evidence that results have been established correctly :
    - All votes registered in the electronic ballot box have been taken into account.
    - And only these votes.

Audit objectives

- Vulnerability Analysis and Intrusion Testing.
- Code analysis.
- Analysis of the measures implemented to guarantee the security of the system.
- Analysis of the ergonomics of the system.

Vulnerability analysis and intrusion testing

- To be done by specialists because :
  - Need to know all the existing attack techniques.
  - Need to know the vulnerabilities of the software infrastructure used.
  - Need to know how to exploit the vulnerabilities found.

Result of the analysis

- No exploitable vulnerabilities
  - Best practices in maintenance and operation of infrastructure are respected.
- No successful intrusion.

Code analysis

Result of the analysis

- The source code is available on the internet.
- Open Source License by Free Software Foundation.
- The State of Geneva encourages communities of computer scientists to contribute to the improvement of the source code.
- The audit of the code thus becomes useless.

Analysis of the measures implemented to guarantee the system security

- Operational organization
  - Identification and risk assessment
  - Organizational measures reducing these risks
    - Segregation of duties
    - Access security (physical, logical)

- IT management
  - IT General controls (COBIT)
    - Incident detection and management
    - Performance and availability management
    - Emergency plans

Analysis of the measures implemented to guarantee the system security

Result of the analysis

- Improve segregation of duties
  - Control of the application logs to be made by an external to the development team to detect possible anomalies or abuses.
  - Formalize a list of roles that have access to the file server.
  - Server administrators should not check the server security configuration.
- Improve process documentation
  - People who monitor processes do not have sufficient knowledge of the usefulness of the actions and controls they perform.
- Improve servers security
  - Better secure access control to systems that manage e-voting.
  - Limit privileged access to servers managing e-voting.

Analysis of the system ergonomics

- The system must be efficient and easy to use
  - Despite authentication, validation and verification steps that require code entry and verification
  - System logic = user logic.
- The system must engender trust among voters.
  - Security and secrecy of the vote.
- The system must not influence the voter's opinion.
- The user must be able to modify his vote until validation.

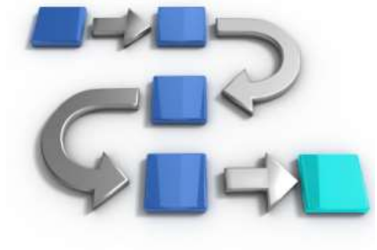
PAPA ! C'EST QUOI L'ERGONOMIE ?
C'EST FAIRE DES ENFANTS ASSEZ GRANDS POUR QUE LES PAPAS N'AIENT PAS À SE COURBER AUTANT !
PL 2003

Analysis of the ergonomics of the system

Result of the analysis

- Clearer explanation of the usefulness of different codes to enter or verify (codes 1, 2, 3, *see slide 4*)
  - Strengthens the perception of the vote security, thus the adoption of the system by the voter.
- Improve the visibility of the steps of the voting procedure in progress.
- Improve the visibility of the documentation pdf of the objects of the vote.
- Improve the identification of the verification codes on the voting card for each step of the voting procedure.

Conclusion



- Good quality and security of the Geneva system.
- Independent audits must be conducted regularly so that the citizen has confidence in this system.
- Technical and complex audits (high visibility, many requirements, numerous risks and significant impacts).