Uncovering the veil on Geneva’s internet voting solution

The Swiss democratic “semi-direct” system enables citizens to vote on any law adopted by any authority (communal, cantonal or federal) and to propose new laws, provided that they collect the requisite number of signatures. As a result, the Swiss are called to the polls four to six times per year to confirm or reject the decisions of their elected representatives. Consequently, accessibility of the ballots, and good electoral organisation, are essential for democratic rights to be exercised as intended in Switzerland.

In this context, the postal vote has developed up to the point where it is used, according to the cantons, by two thirds to 95% of voters. Further: by facilitating access to voting, the postal vote has for example enabled Geneva to increase average participation by 20 percentage points. This success, together with the acknowledgement that the postal vote does not solve the accessibility problem for voters abroad and for persons with reduced mobility or the visually impaired, paved the way for internet voting. Today in Geneva there are three fully integrated voting channels: polling stations, the postal vote and internet voting.

The first electronic vote in Switzerland took place in January 2003 in the canton of Geneva. To date, 19 votes and three administrative elections involving electronic voting have taken place in this canton. No other public authority in the world has such extensive experience of online voting.

Internet voting involves additional challenges compared with postal voting, due to the virtualisation of the vote. How does a voting operation take place? What security measures are put in place? How is voting secrecy guaranteed? The aim of this article is to offer a basic response to these questions. It is aimed at a technical audience having a basic knowledge of cryptography. In the pages which follow, we will use the expressions “electronic voting”, “on-line voting”, “eVoting” and “internet voting” interchangeably to describe the use of internet voting in Geneva.

The matters dealt with in this article are organised in accordance with the four principal stages in the life cycle of a ballot involving electronic voting:

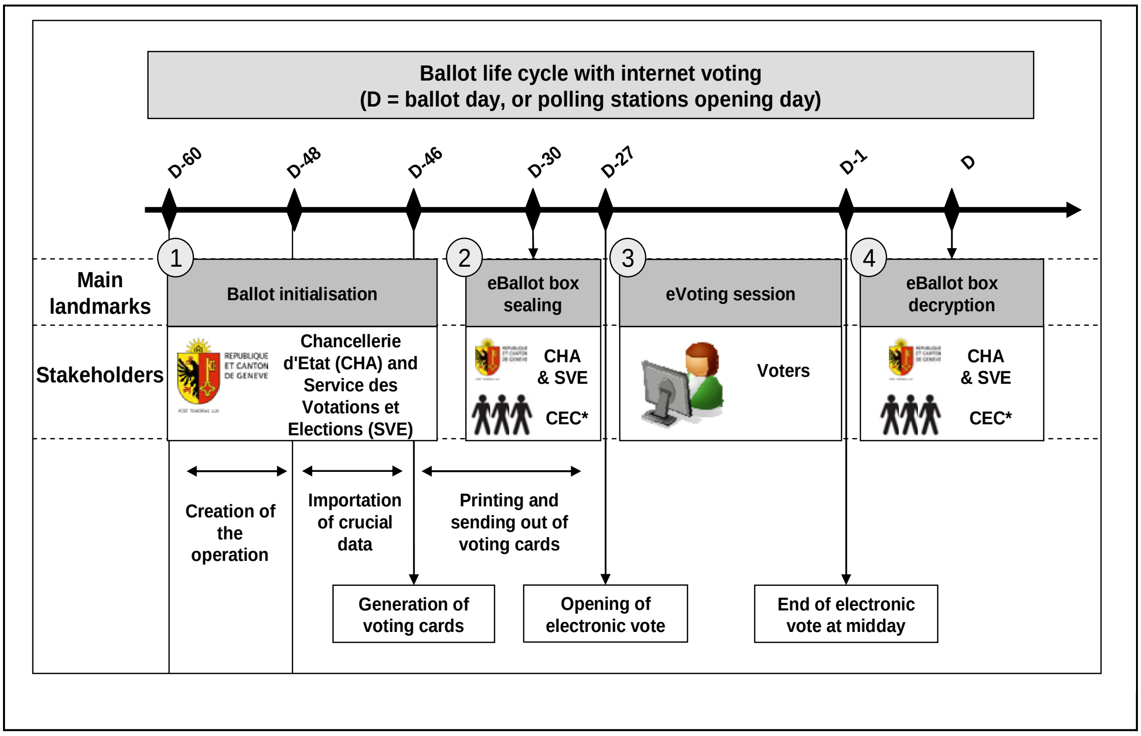

Ballot life cycle with internet voting
(D = ballot day, or polling stations opening day)
D-60
D-48
D-46
D-30
D-27
D-1
D
Main landmarks
Stakeholders
1
Ballot initialisation
Chancellerie d'Etat (CHA) and Service des Votations et Elections (SVE)
2
eBallot box sealing
CHA & SVE
CEC*
3
eVoting session
Voters
4
eBallot box decryption
CHA & SVE
CEC*
Creation of the operation
Importation of crucial data
Printing and sending out of voting cards
Generation of voting cards
Opening of electronic vote
End of electronic vote at midday

Figure 1: Life cycle of a ballot involving electronic voting

*** What is the CEC?**

The Central Electoral Commission (CEC) was formed on 1st January 2010, at the same time that electronic voting was introduced in the cantonal constitution of Geneva. According to the law, the CEC "has access to all operations in the electoral process" and may "undertake checks, at any time, independently of an electoral operation" (Article 75B of the Act on the exercise of political rights).

The CEC locks the electronic ballot box by generating its encryption keys, so that nobody is able to access electronic votes before they are counted. The CEC may access any document relating to the electronic voting system, it may appoint experts of its choice for audits, tests or studies.

The CEC and any specialists it decides to appoint have access to the source code at all times, as well as persons who can demonstrate an academic interest.
This commission has set up an internal technical group which has commenced an audit process of the electronic voting system and procedures. The law also requires the internet voting system to be audited every three years and the results of such audit to be published. The first audit of this cycle will take place in 2012.

Initialisation of an operation

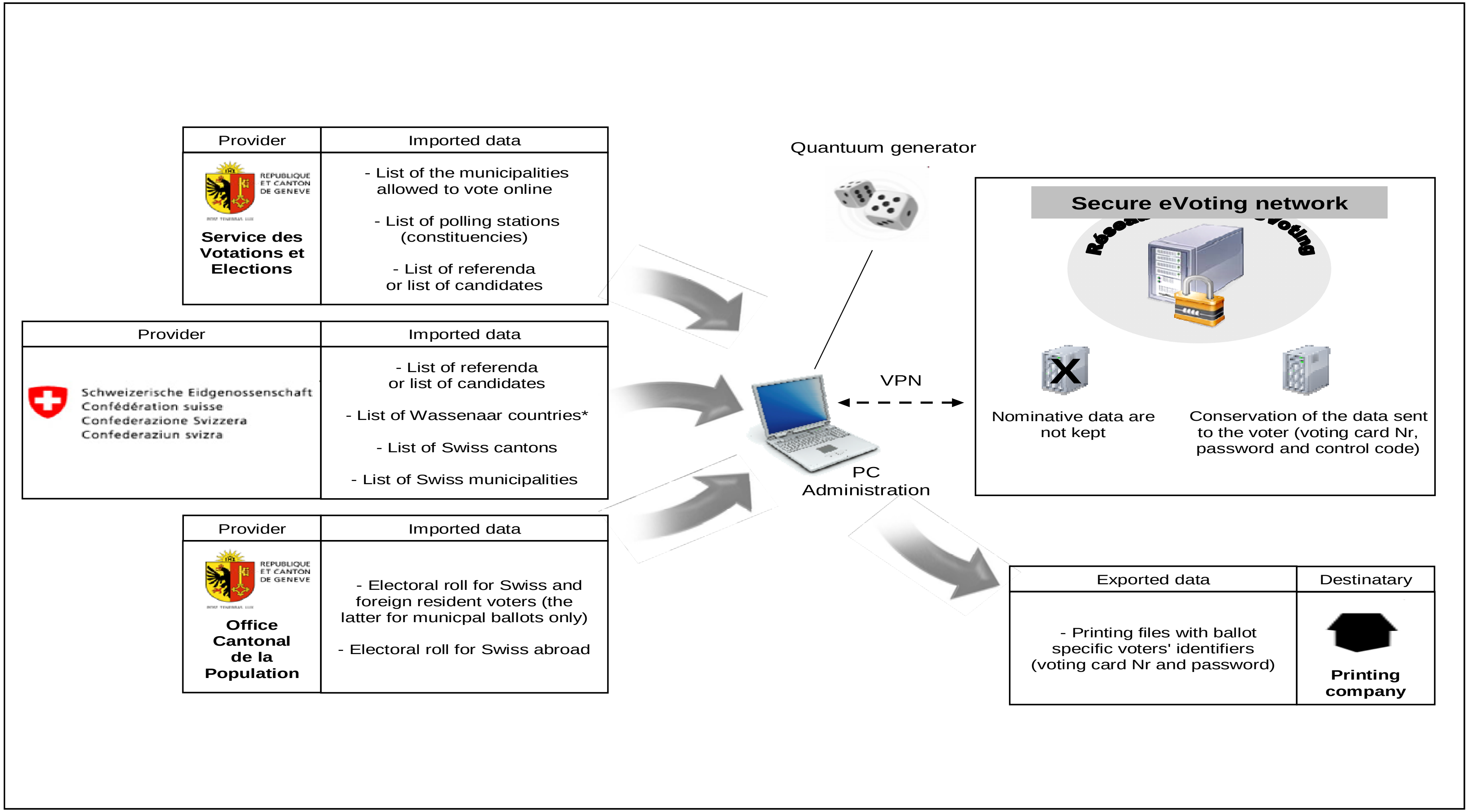
During the initialisation phase, the data necessary for the electoral operation are imported into the eVoting system. These data come from various sources and are of varying types. The following can be distinguished in particular:

- Data concerning electoral organisation: communes and polling stations, in particular communes authorised to vote by internet in a given ballot when the ceiling stipulated by the federal ordinance on political rights applies.
- Data relating to the purpose of the vote: proposals in a referendum, or lists of candidates in elections.
- Data concerning geographical connection: list of countries (for the Swiss abroad in particular*), list of cantons, etc.
- The data necessary for the production of the voting material: in particular electoral register containing, surname, forename, address.
- The data necessary for the voter authentication in the electronic voting system: date of birth, commune of origin and password.

The personal data taken from the register of inhabitants of the Cantonal Population Office enabling files to be produced for the printers are not retained in the database. This, therefore, contains no voter's name.

Print files also contain voting data (voting card number, password and control code) generated with the aid of a true random number generator (quantuum generator). These data are specific to each voter and to each operation.

The flow of data during the initialisation phase may be represented as follows:



Provider	Imported data
Service des Votations et Elections	- List of the municipalities allowed to vote online - List of polling stations (constituencies) - List of referenda or list of candidates

Provider	Imported data
Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra	- List of referenda or list of candidates - List of Wassenaar countries* - List of Swiss cantons - List of Swiss municipalities

Provider	Imported data
Office Cantonal de la Population	- Electoral roll for Swiss and foreign resident voters (the latter for municpal ballots only) - Electoral roll for Swiss abroad

Exported data	Destinatary
- Printing files with ballot specific voters' identifiers (voting card Nr and password)	Printing company

Figure 2: Data flow during a ballot initialisation phase

***Wassenaar countries: why are some Swiss citizens abroad not allowed to vote online?**

We aim here to dispel a frequent misconception regarding access by the Swiss abroad to electronic voting. Only expatriates living in the European Union or in one of the signatory states to the Wassenaar arrangement receive voting materials enabling them to vote online. This has nothing to do with the nature of the internet voting applications used in Switzerland (open source or not); it relates to a decision of the Confederation adhering to a legal principle.

By ratifying the Wassenaar arrangement, states undertake not to punish the trading and using of “dual use” (civil and military) goods and technologies. Cryptographic applications form part of these goods and technologies. By restricting access to online voting to Swiss persons living in a country agreeing not to take legal action against the users of such goods and technologies – as this is the point concerned – the Confederation wished to protect its citizens living abroad from any legal proceedings in their country of residence.

Sealing of the electronic ballot box

The sealing of the electronic ballot box takes place during an official meeting that prepares the electoral session and generates the votes’ encryption keys. This stage is carried out after the information reproduced on the voting cards has been imported into the system and the cards have been printed and are being sent out.

During this stage, cryptographic mechanisms are put in place in order to guarantee the impregnability of the ballot box. A ballot box is impregnable if votes cannot be entered or read in it without the system noticing it.

- The ballot box is illegible during the voting session by virtue of the use of an asymmetric key where only the public encryption key is available and the private decryption key is put in a secure place and protected by passwords.
- The ballot box is unalterable without the system knowing this has happened by virtue of the use of the public voting encryption key and an integrity meter recognised only by the voting system.

  The public encryption key is known only by the system and is the only one capable of entering valid votes in the ballot box. A valid vote is a vote which can be accurately decrypted by the private key.

  The integrity meter indicates the number of votes cast in the ballot box. In order to remain unalterable and capable of robustly resisting a system restart this meter is stored encrypted using a symmetric key in the database.

a. Preparation of the stage

The various parties involved and the material necessary to seal the electronic ballot box are gathered. The stage proceeds in accordance with a protocol drawn up by the Chancellery.

The parties involved in this stage are:

- the Chancellor of State,
- the Chairman of the CEC,
- the Chairman of the Meeting,
- two groups of at least two members of the CEC,
- the representative of the Voting and Elections Department (VED),
- a notary,
- the Police IT department security officer (“security officer”),
- the eVoting administrator.

The eVoting administrator connects himself to the electronic voting system, in a nominative way, with the dedicated administration PC, through a VPN secured with a unique secret, on a dedicated network connection.

The eVoting administrator launches the administration console. This application provides a graphic interface that displays the progress of each stage.

b. Generation of the keys

The eVoting administrator launches the generation of:

- the pair of asymmetric keys for encryption of the votes, which is composed of
  - a public vote encryption key,
  - a private vote decryption key,
- the symmetric key of the integrity meter.

Keys	Use
Public key for encrypting the votes	This key enables the votes in the ballot box to be encrypted but is note able to decrypt them.
Private key for decrypting the votes	This key enables the votes in the ballot box to be decrypted in order to obtain the result of the ballot.
Symmetric key of the integrity meter	This key enables to encrypt and decrypt the integrity meter in the database and, as such, to ensure that the ballot box is unalterable.

Table 1: System keys produced during the ballot box sealing stage

In order to protect the access to the private vote decryption key, this key is stored in a key collection protected by 2 passwords.

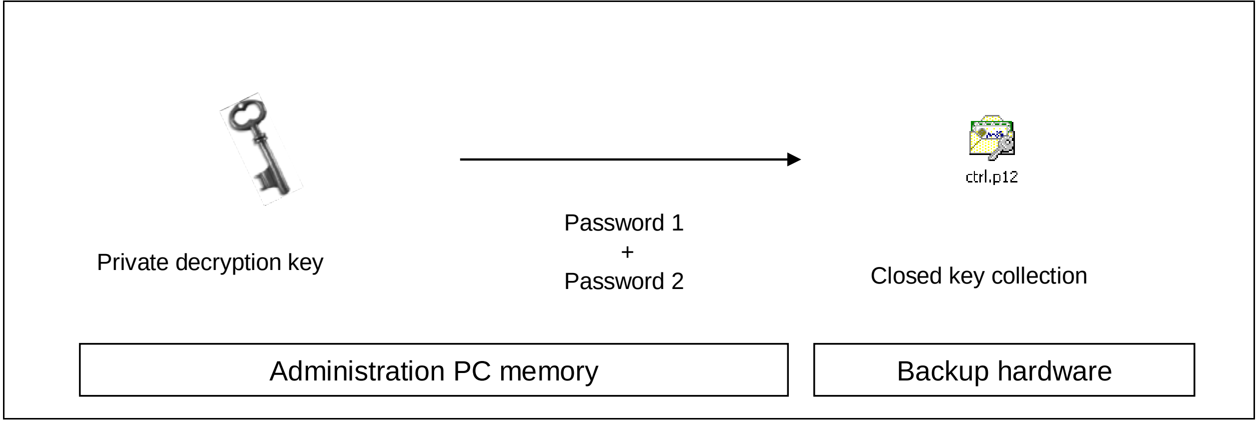


Figure 3: Collection of keys protected by 2 passwords

Each of the two groups of CEC members chooses a password and inputs it into an ad hoc form. The first person in the first group inputs the password chosen by his group. The second person inputs the same password in order to confirm the entry. The same procedure is carried out by the second group for the second password.

c. Storage

Three collections of data are directly generated on 2 removable storage media (a USB key and a CD) so that they are not saved on the Administration PC. These collections are:

- The collection of keys protected by passwords,
- The public key for vote encryption,
- The symmetric key of the integrity meter.

The eVoting administrator transfers a copy of the symmetric key of the integrity meter onto the system. These data media are placed in sealed envelopes and handed over to the security officer. The forms recording the password are placed in two separate envelopes, sealed and given to the notary.

Lastly, the eVoting administrator launches the final initialisation of the eVoting database by setting the integrity meter to 0 with the symmetric key.

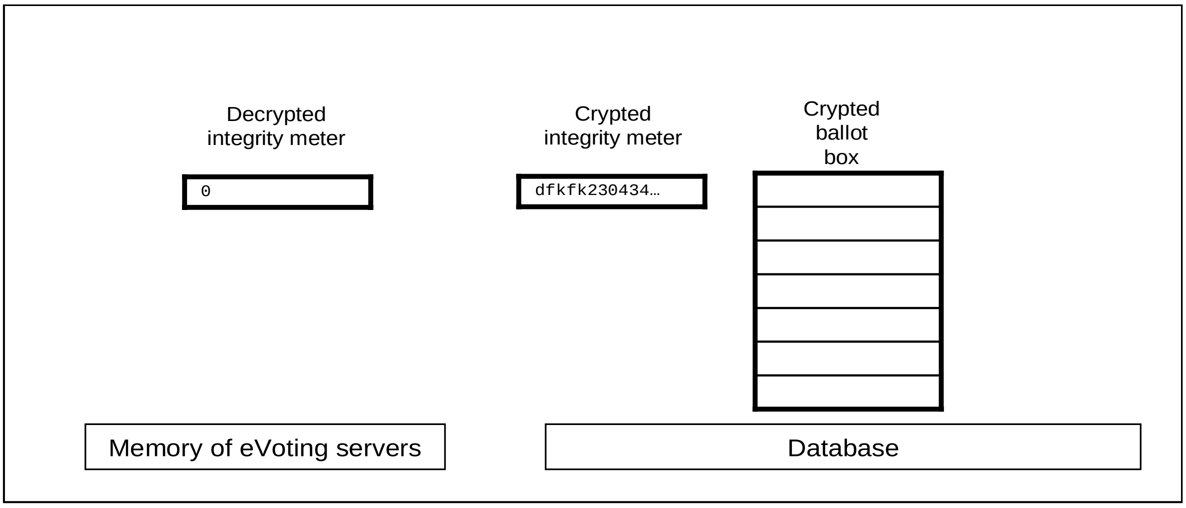


Figure 4: Empty ballot box

Secret	Creator	Back up
Password 1	First group of CEC members	Input form 1
Password 2	Second group of CEC members	Input form 2
Collection of keys protected by password	Administration PC	CD and USB key
Public vote encryption key		CD and USB key
		Evoting system hard discs
Symmetric key of the integrity meter		CD and USB key
		Evoting system hard discs

Table 2: List of secret information

Note that no secret information remains on the Administration PC. A test vote is then carried out on the system by each of the CEC groups. The expected results are noted.

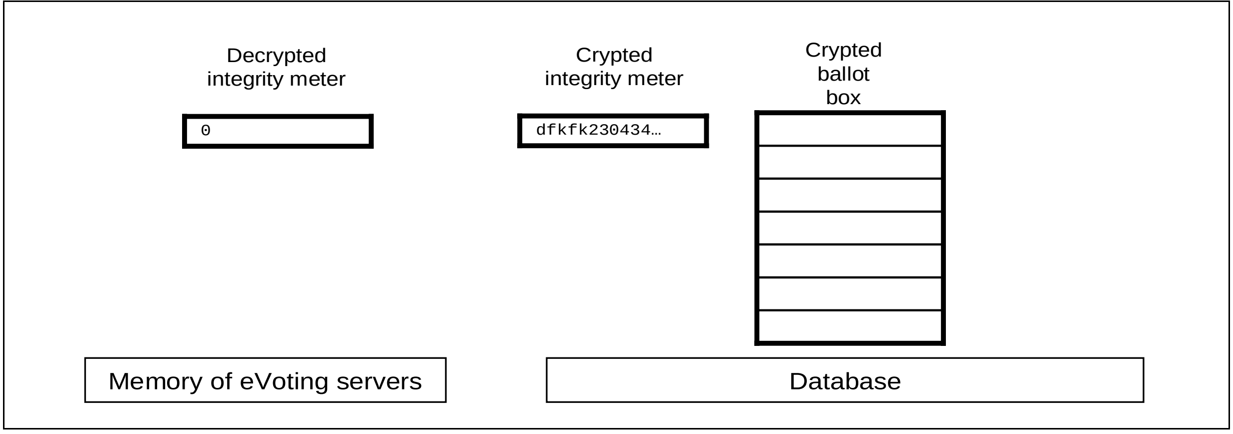


Figure 5: First test vote in the ballot box

The votes in the ballot box are counted (see explanations below) and the results obtained are validated.

The administration PC is placed in a bag which is sealed using numbered seals, the numbers of which are recorded. The bag is delivered to the representative of the Voting and Elections Department who will retain it for the duration of the ballot.

Back up	Integrity medium	Custodian during the voting session
Administration PC	Sealed bag	Representative of the VED
Input form 1	Sealed envelope 1	Notary
Input form 2	Sealed envelope 2	
CD and USB key	Sealed envelope 3	Security officer

Table 3: List of back-up media

The flow of data during the sealing of the ballot box may be represented as follows:

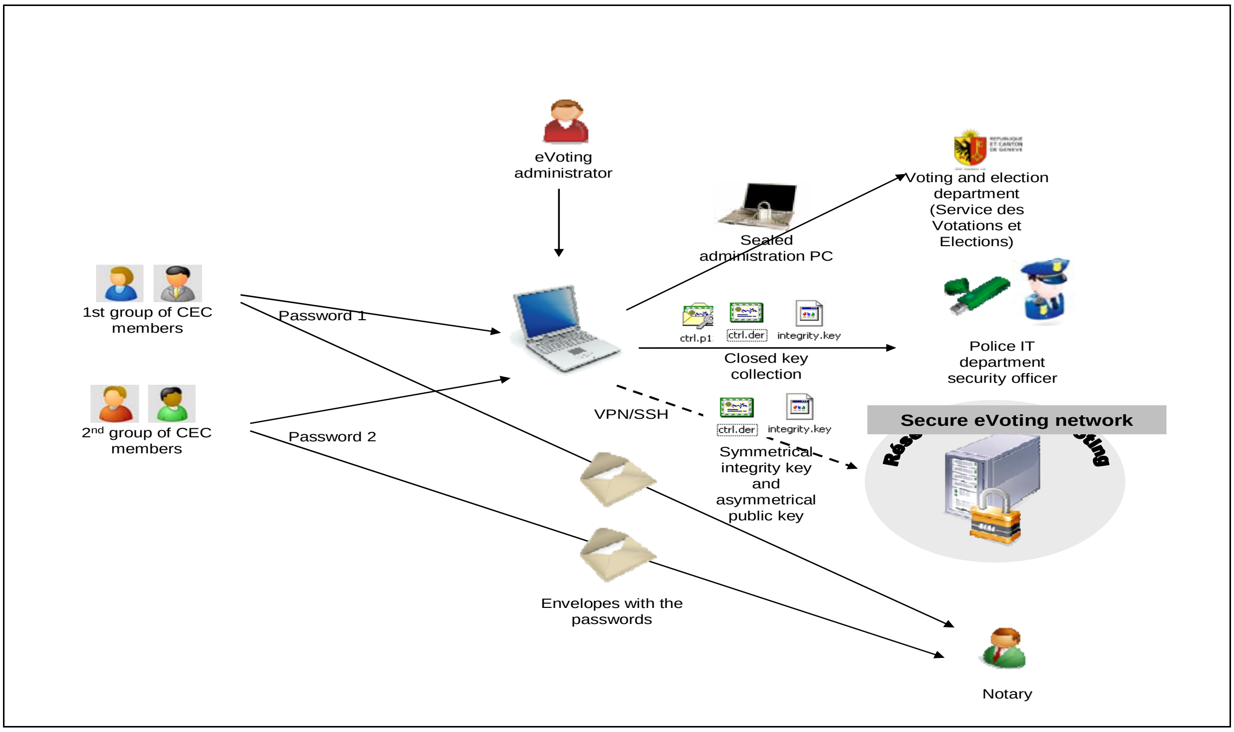


Figure 6: Exchange of secret information and back up media

Before opening the ballot box, the secrets shared between the various parties must be reassembled on protected media. Each party holds no more than one piece of secret information. In order to enter this secret information into the system and unlock the ballot box, it is necessary to connect to a secure infrastructure. No party in possession of secret information has access to this infrastructure.

Each item of secret information is available on two media:

Secret information relating to the ballot	Back up media
Password 1	1. Envelopes containing the passwords held by the notary 2. Memory of members of 1st group of CEC members

Password 2	1. Envelopes containing the passwords held by the notary 2. Memory of members of 2nd group of CEC members
Collection of keys protected by passwords	1. CD with the security officer 2. USB key with the security officer
Public key for vote encryption	1. CD and USB key with the Security Officer 2. eVoting system hard discs
Symmetric key of the integrity meter	1. CD and USB key with the Security Officer 2. eVoting system hard discs

Progress of the voting session

Once the electronic ballot box is sealed, the internet voting website may be opened to the public. When a voter connects to https://www.evote-ch.ch using his web browser, he opens a voting session.

In order to complete a voting session, the voter firstly types in his voting card number on the identification page, then accepts the legal notices, fills in his ballot paper, checks his vote and provides his personal information (password, date of birth and commune of origin) on the identification page, before being transported to the confirmation page that provides a confirmation that his vote has been recorded.

Shared secrets used for the vote	Source	Back up media
Date of birth	Voter's personal data	Population register Database Voter's memory
Commune of origin		Population register Database Voter's memory
Password	Electronic voting system	Database (hashed) Voting card
Voting card number		Database Voting card
Control code		Database Voting card

Table 4: Secret information relating to the vote

A voting session requires a dialogue to be established between the voter's browser and the eVoting system servers. Several questions may be asked regarding the security of these exchanges:

- How can we be certain that the voter is accessing the official eVoting servers?
- How is the voter identified?
- How can we avoid a malicious third party intercepting or manipulating the data exchanged?

d. Authentication of the eVoting website

When the voter's browser makes contact with the eVoting website, the use of the https protocol generates a SSL communication. When a link is established, the browser asks the eVoting website to present its electronic certificate. This is a digital identity card issued by a certification authority, the role of which is to ensure the link between a physical identity and a digital identity.

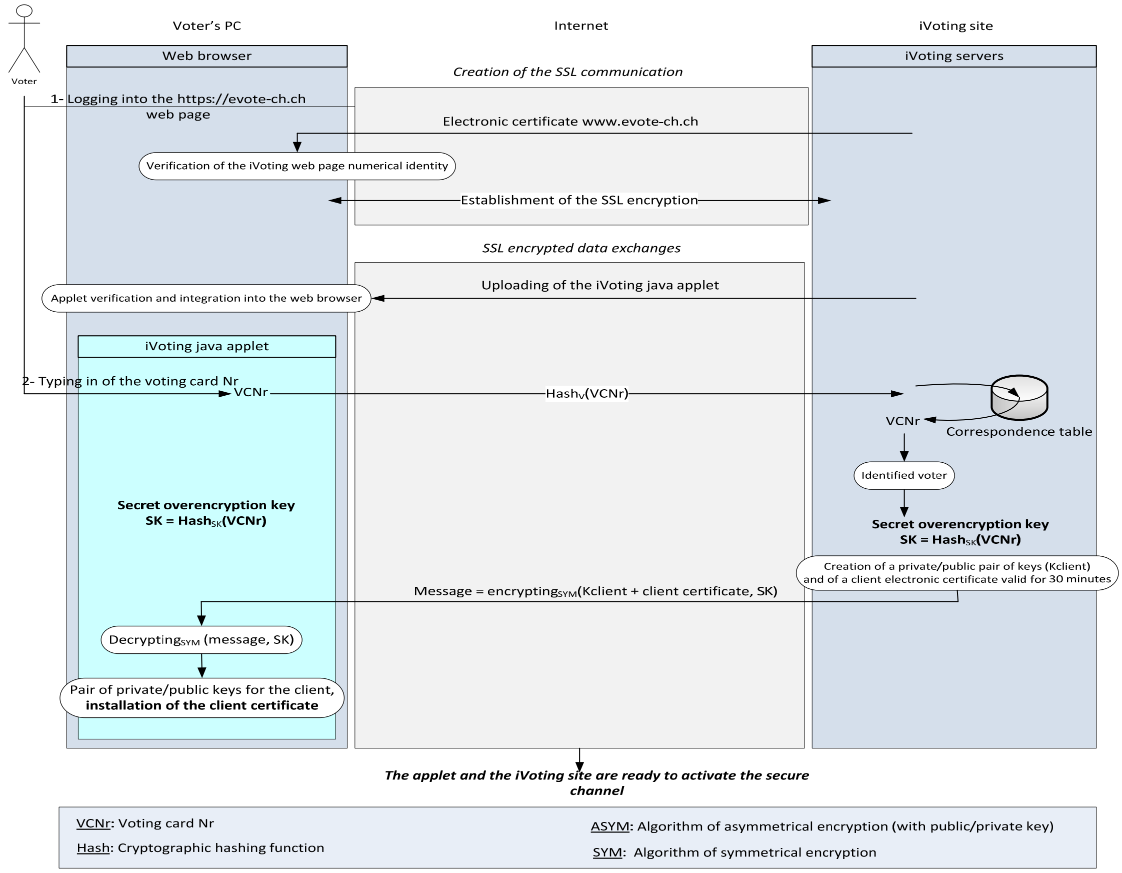
By verifying the certificate received, the browser validates the identity of the eVoting website. Once the SSL communication is in place, there is a guarantee that the voter will access the genuine eVoting website, firstly, and, secondly, that all exchanges between the browser and the eVoting servers are encrypted.

e. Identification of the voter

For each voting operation, the voter receives by post a single use voting card. Additionally, for each voter there is a unique voting card number (UVN), enabling him to be identified in the voting management system, irrespective of the voting channel (electronic, postal or polling station) he chooses.

So that this crucial information is not compromised, it is never exchanged. Instead, an imprint of the voting card number is sent out. This imprint is obtained by applying a cryptographic hash function ($Hash_E$) to the voting card number, which makes it very difficult, or impossible within the time frame of the voting operating, to locate the original number.

The eVoting system uses a correspondence table, drawn up at the stage of the generating of the print files, to determine the voting card number of the voter on the basis of the imprint received. From then on, the voting card number constitutes a “shared” secret between the voter and the eVoting system.



Voter
Voter's PC
Internet
iVoting site
Web browser
iVoting servers
Creation of the SSL communication
1- Logging into the https://evote-ch.ch web page
Electronic certificate www.evote-ch.ch
Verification of the iVoting web page numerical identity
Establishment of the SSL encryption
SSL encrypted data exchanges
Uploading of the iVoting java applet
Applet verification and integration into the web browser
iVoting java applet
2- Typing in of the voting card Nr
VCNr
Hash$_V$(VCNr)
VCNr
Correspondence table
Identified voter
Secret overencryption key SK = Hash$_{SK}$(VCNr)
Secret overencryption key SK = Hash$_{SK}$(VCNr)
Creation of a private/public pair of keys (Kclient) and of a client electronic certificate valid for 30 minutes
Message = encrypting$_{SYM}$(Kclient + client certificate, SK)
Decrypting$_{SYM}$ (message, SK)
Pair of private/public keys for the client, installation of the client certificate
The applet and the iVoting site are ready to activate the secure channel
VCNr: Voting card Nr
Hash: Cryptographic hashing function
ASYM: Algorithm of asymmetrical encryption (with public/private key)
SYM: Algorithm of symmetrical encryption

Figure 7: Stage of authentication of the eVoting website and identification of the voter

f. Secure channel

Up to this point, we have considered the measures put in place to ensure that the voter accesses the genuine eVoting website and how the eVoting system identifies the voter. We will now consider the way in which exchanges are made secure against interception and manipulation.

In effect, although the SSL protocol ensures encryption of the exchanges and authentication of the server, it has been proven that this protocol is susceptible to “man in the middle” attacks. Such an attack, whilst being very complex to implement, consists of the attacker inserting himself between the browser and the eVoting website. The perpetrator consequently passes himself off to the voter as the eVoting server and, conversely, passes himself off as the voter to the eVoting server.

In order to make these attacks more difficult, the eVoting system implements the concept of a *secure channel* between the browser and the server. The secure channel is based on a combination of several security techniques: mutual SSL protocol, surencryption of the data and authentication of messages.

As referred to above, the “simple” SSL requires the server to present an electronic certificate to the client so that the client may authenticate it. The mutual SSL is an extension of the “simple” SSL which adds a stage of authentication of the client by the server. Similarly, the client must present his electronic certificate to the server, which validates it via a certification authority.

Once mutual authentication has taken place, the client is certain that he is accessing the genuine eVoting website and the server is certain that it is accessing the voter. Once it is in place, the mutual SSL guarantees a first level of encryption of all the data exchanged.

Surencryption consists of encrypting the data at the level of the application, even before sending it via the mutual SSL link. The encryption is based on a symmetrical key encryption algorithm ($_{\text{SYM}}$), whose secret key is derived from the voting card number (UVN), both by the server and by the client, via the use of a cryptographic hash function (Hash_{CS}). The data are encrypted twice, in a different way, in the course of being transmitted, which reinforces the security of the encryption.

Authentication of the messages consists in adding an encrypted imprint to each message. In concrete terms, for the client this consists in calculating the imprint of the message (E_{MSG}), then encrypting this imprint with the private key associated with its electronic certificate (EC_{MSG}). The encryption used here is therefore based on an asymmetric key encryption algorithm.

Upon receipt of the encrypted message and its encrypted imprint, the eVoting system uses the public key of the client certificate to decrypt the signature and obtain the imprint of the message (E_{MSG} received). Then, the eVoting system calculates the imprint of the message (E_{MSG} calculated). If the two imprints differ, either the original message has been altered, or the message has not been signed by the private key associated with the public key of the client certificate, therefore not by the expected client!

If the imprints match, the eVoting system deciphers the message with the aid of the secret key and proceeds to process the message.

Current web browsers do not offer the functions required to implement a secure channel such as the one we have described here. For this reason, the eVoting system requires the use of Java technology, which will be incorporated into the voter's web browser thus improving its function.

In practice, from the start of the voting session, a Java applet is downloaded from the eVoting website and run within the web browser on the voter's computer. Once the voting card number has been typed on the identification page, the applet sets up the secure channel. The applet and the web browser integrate in an extended way so that all exchanges of sensitive data travel via the applet rather than via the browser.

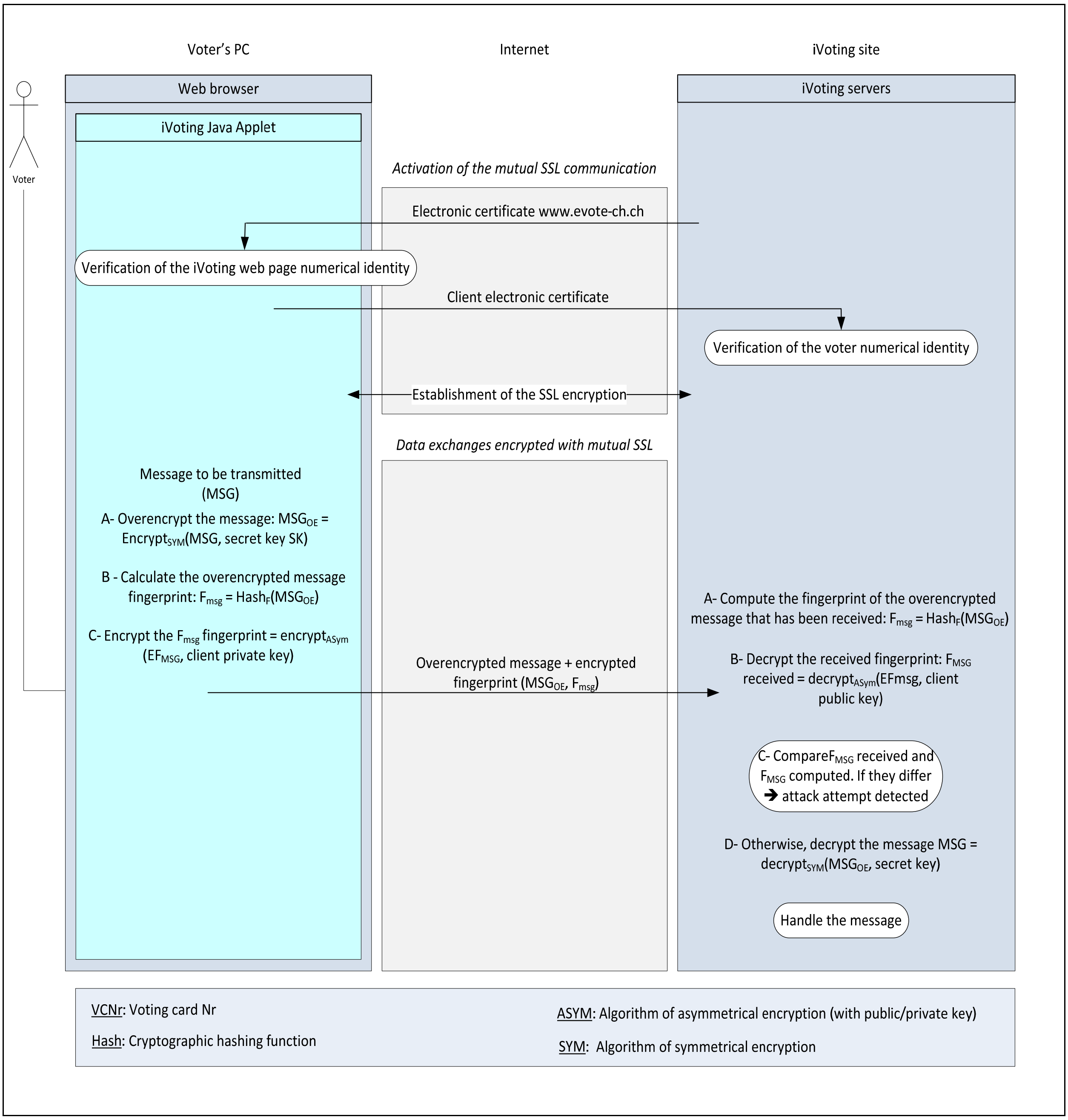

Voter's PC
Internet
iVoting site
Web browser
iVoting servers
Voter
iVoting Java Applet
Activation of the mutual SSL communication
Electronic certificate www.evote-ch.ch
Verification of the iVoting web page numerical identity
Client electronic certificate
Verification of the voter numerical identity
Establishment of the SSL encryption
Data exchanges encrypted with mutual SSL
Message to be transmitted (MSG)
A- Overencrypt the message: MSG_{OE} = $Encrypt_{SYM}$(MSG, secret key SK)
B - Calculate the overencrypted message fingerprint: F_{msg} = $Hash_{F}$(MSG_{OE})
C- Encrypt the F_{msg} fingerprint = $encrypt_{ASym}$ (EF_{MSG}, client private key)
Overencrypted message + encrypted fingerprint (MSG_{OE}, F_{msg})
A- Compute the fingerprint of the overencrypted message that has been received: F_{msg} = $Hash_{F}$(MSG_{OE})
B- Decrypt the received fingerprint: F_{MSG} received = $decrypt_{ASym}$(EFmsg, client public key)
C- CompareF_{MSG} received and F_{MSG} computed. If they differ ➔ attack attempt detected
D- Otherwise, decrypt the message MSG = $decrypt_{SYM}$(MSG_{OE}, secret key)
Handle the message
VCNr: Voting card Nr
Hash: Cryptographic hashing function
ASYM: Algorithm of asymmetrical encryption (with public/private key)
SYM: Algorithm of symmetrical encryption

Figure 8: Establishment and use of the secure channel

g. *Recording of a vote in the ballot box*

The recording of a vote starts with the indication by the voter of his choices on his browser. The completed ballot paper is sent, via the secure channel, to the voting server.

The server decrypts the voter's ballot paper, undertakes a syntax check (to ensure that the vote cast will be valid in order to avoid ballot papers being declared void) then sends the voter confirmation of his choices with a control code. This random code is printed on the voter's voting card and is only known to him and the eVoting servers: it is additional proof for the voter that he has connected to the genuine eVoting server.

The voter is then invited to confirm his identity by inputting his date of birth and the password registered on his voting card and selecting his commune of origin from a list of 50. As with all sensitive data, these are sent by secure channel to the voting server.

The server checks the voter's personal data, checks that the voter is entitled to vote (no previous vote or vote via another method), then records his vote.

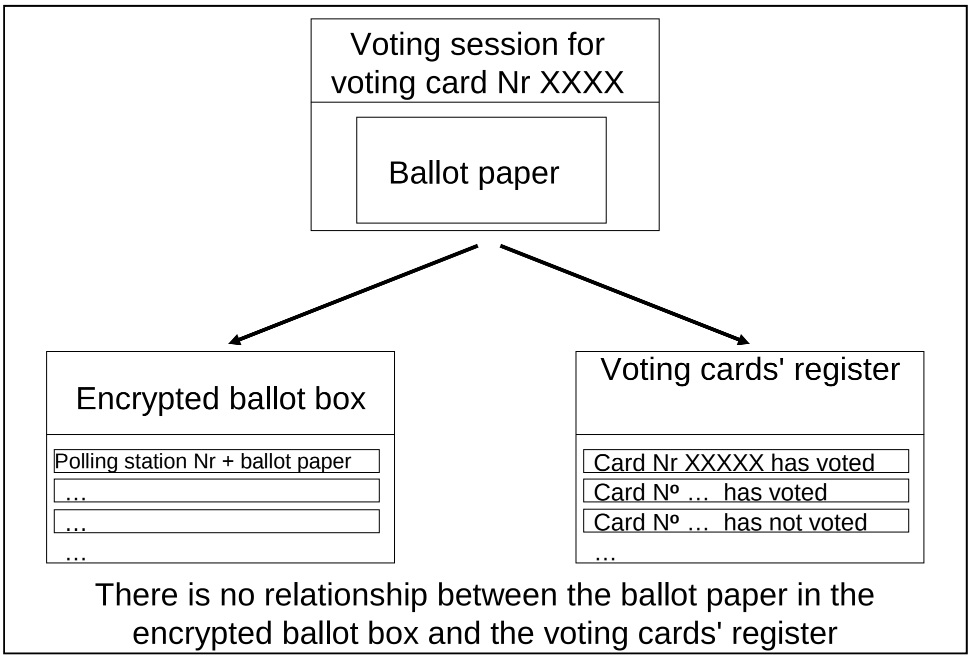

Voting session for voting card Nr XXXX
Ballot paper
Encrypted ballot box
Polling station Nr + ballot paper
…
…
…
Voting cards' register
Card Nr XXXXX has voted
Card Nº … has voted
Card Nº … has not voted
…
There is no relationship between the ballot paper in the encrypted ballot box and the voting cards' register

Figure 9: Separation of data at the time of the vote recording

- The ballot paper and voter's voting location are encrypted with salt, using the public encryption key for the ballot, and then recorded in the ballot box.
- When a citizen votes, the voting cards' register is modified to record the fact that the voting card number associated with this citizen has voted.
- The integrity meter in the database is decrypted by the system using the symmetric integrity key. The application increments this meter, encrypts it again and saves it in the database.
- These three operations are carried out in a single database transaction in order to ensure that the filing of the vote meets the ACID requirements (Atomicity, Consistency, Isolation and Durability).

Lastly the server sends to the voter confirmation of his vote including the date and time of his vote, and the control code which confirms that the message comes from the voting system.

Counting the votes in the electronic ballot

The counting of the votes in the electronic ballot takes place during an official meeting. The objective of this stage is to extract the results of the vote from the electronic ballot box.

h. Progress of the stage

The various parties involved and the material necessary to decrypt the electronic ballot are gathered. The stage proceeds in accordance with a protocol drawn up by the Chancellery.

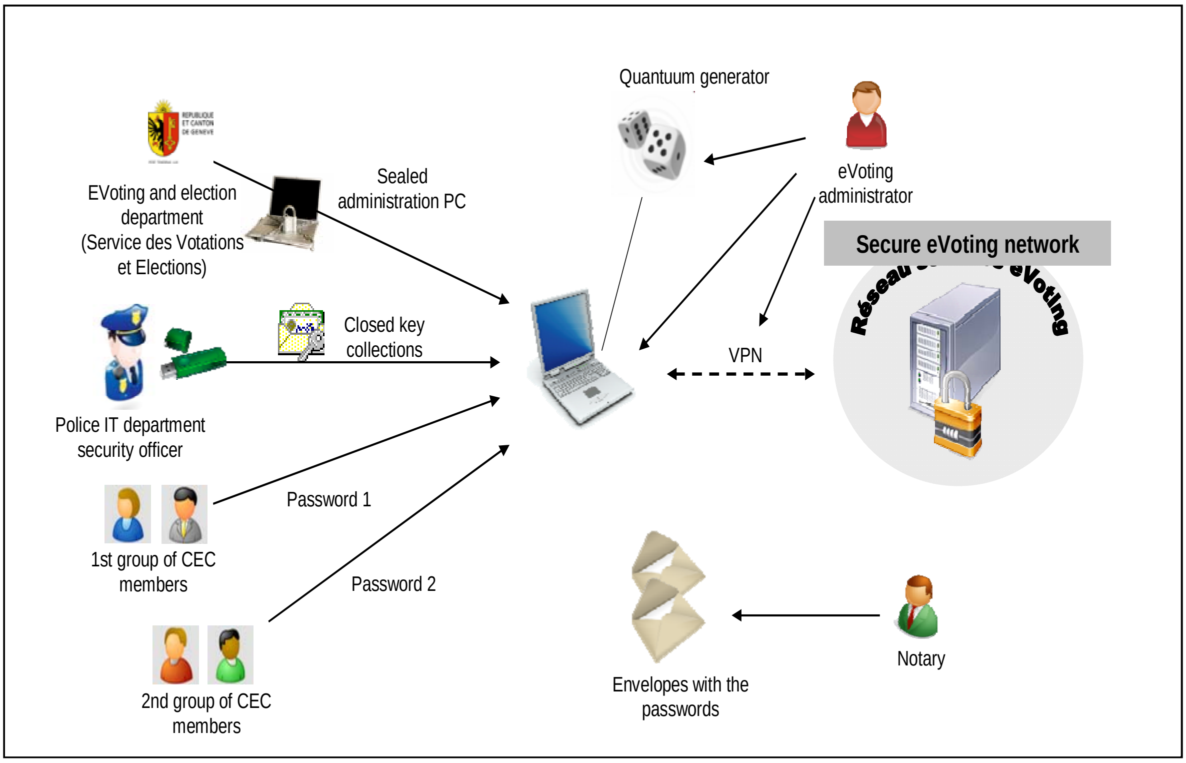


Figure 10: Parties involved and hardware necessary for counting of the votes in the electronic ballot box

- The head of the VED produces the sealed Administration PC. The seals are checked and broken under the supervision of a member of the CEC.

- The eVoting administrator connects the Administration PC to the secure eVoting network. The room where this stage takes place is fitted with a specific connector, and only the administrator has the necessary rights to set up a VPN. At this stage, the random number generator, provided by the administrator, is connected to the Administration PC.

- The security officer provides the locked collection of electronic keys containing the private vote decryption key (USB key and CD-ROM media).

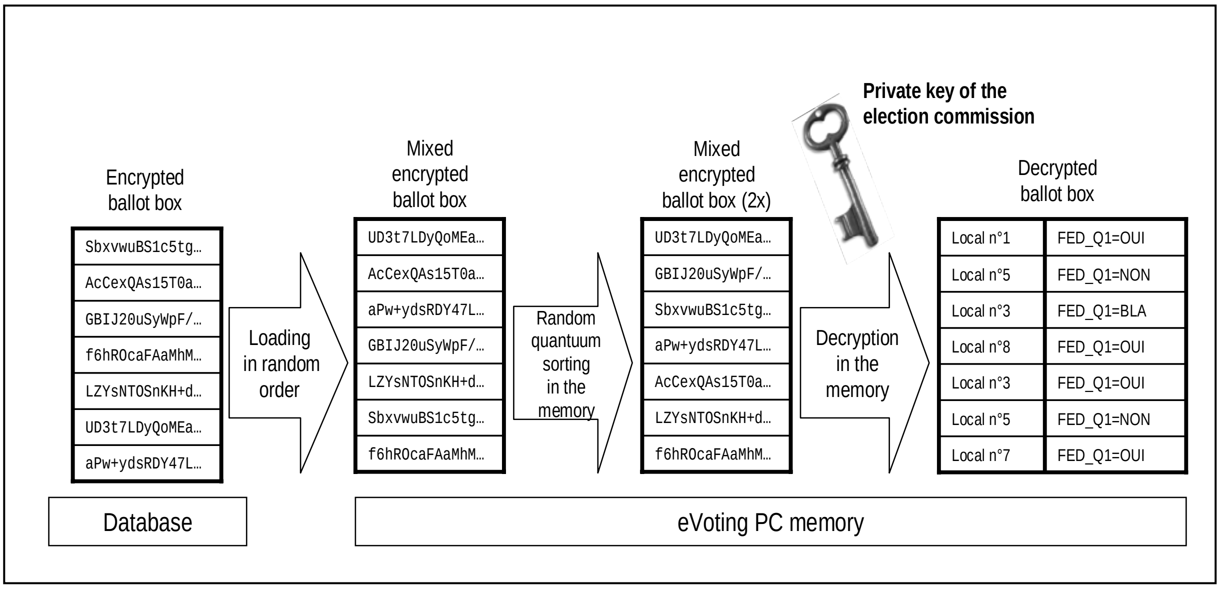
- Each of the two groups of controllers provides its password enabling the collection of keys to be opened. In the event that either of the groups does not recall the password which was set, it can be recovered by opening the corresponding envelope provided by the notary.

- This stage is managed and supervised by the Chancellery.

Once the three items of secret information – collection of keys, password 1 and password 2 – are entered into the administration application, this opens the bunch to recover the private vote decryption key and then decrypts the electronic ballot box and generates the results. The technical arrangements for this stage are set out in the following section.

i. *Techniques for churning the electronic ballot box and decryption techniques*

Although the system was designed so that there would be no relationship in the database between the voters' register and the electronic ballot box, it could nevertheless be possible to establish a temporal link between a voter, for whom the vote casting time is recorded, and the encrypted vote, which is stored in the order of arrival. Various technical and organisational measures prevent this from occurring. One of these consists of churning the ballot box: just as in the case of a real ballot box, decryption of the electronic ballot box is preceded by churning, the principles of which are shown in the diagram below.



Local n°1	FED_Q1=OUI
Local n°5	FED_Q1=NON
Local n°3	FED_Q1=BLA
Local n°8	FED_Q1=OUI
Local n°3	FED_Q1=OUI
Local n°5	FED_Q1=NON
Local n°7	FED_Q1=OUI

Figure 11: Churning and decryption of the electronic ballot box

- Originally, the encrypted votes are recorded in a database in their order of arrival.
- All votes are uploaded into a memory structure. Such uploading uses a specific function of the database enabling reading to take place in a random order.
- This first structure is mixed in turn using the quantuum random number generator. The following diagram demonstrates the principle of this mixing:

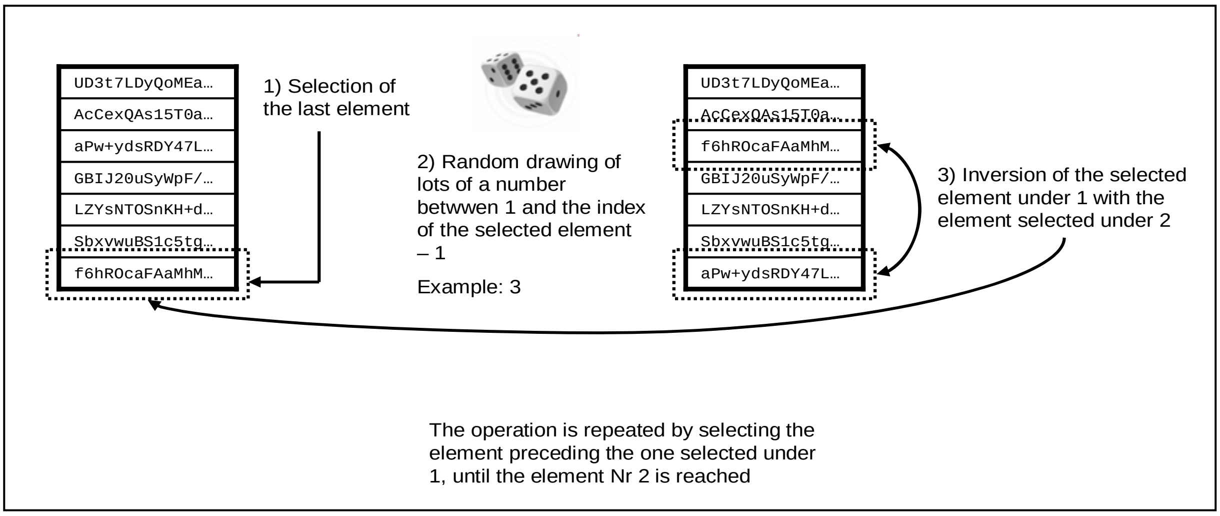
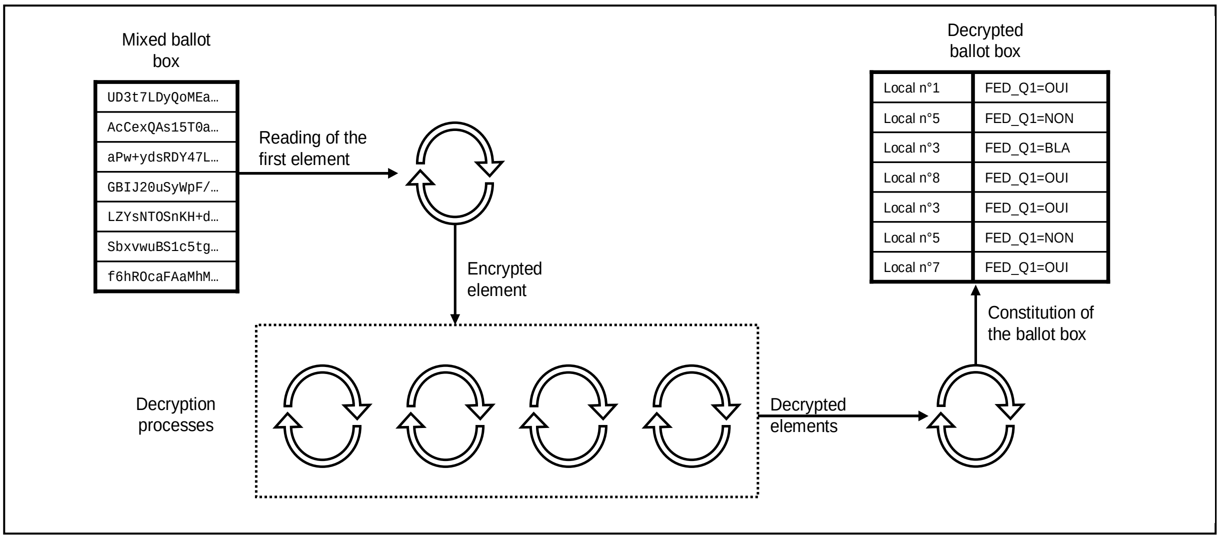

UD3t7LDyQoMEa…
AcCexQAs15T0a…
aPw+ydsRDY47L…
GBIJ20uSyWpF/…
LZYsNTOSnKH+d…
SbxvwuBS1c5tg…
f6hROcaFAaMhM…
1) Selection of the last element
2) Random drawing of lots of a number betwwen 1 and the index of the selected element – 1
Example: 3
UD3t7LDyQoMEa…
AcCexQAs15T0a…
f6hROcaFAaMhM…
GBIJ20uSyWpF/…
LZYsNTOSnKH+d…
SbxvwuBS1c5tg…
aPw+ydsRDY47L…
3) Inversion of the selected element under 1 with the element selected under 2
The operation is repeated by selecting the element preceding the one selected under 1, until the element Nr 2 is reached

Figure 12: Algorithm for the quantum churning of the ballot box

- ➤ Once the ballot box has been mixed twice, the application opens the collection of keys using as a password the concatenation of the password of group 1 following by the password of group 2 of the CEC members. The private key recovered in this way enables each vote to be decrypted and the decrypted ballot box to be created.

As the time required for decrypting a single vote is relevant, the decision has been taken to execute the decryption procedures in parallel in order to optimise the processing time for this stage. The following diagram explains this principle:



Local n°1	FED_Q1=OUI
Local n°5	FED_Q1=NON
Local n°3	FED_Q1=BLA
Local n°8	FED_Q1=OUI
Local n°3	FED_Q1=OUI
Local n°5	FED_Q1=NON
Local n°7	FED_Q1=OUI

Figure 13: Parallel decryption procedure

- ➤ The structure representing the decrypted ballot box is used by the process which produces statements and generates the results of the vote.

How can we be sure that the application counts and records the votes accurately?

The CEC has its own constituency in which it issues votes, which are also recorded on a paper form. As we know the results for this constituency thanks of the paper record, when decrypting the electronic ballot box we check whether the electronic results match the paper ones. This enables us to ensure that the application does not produce biased results.

How can we be sure that all votes are counted?

An integrity meter is incremented in the same operation in which each vote is recorded in the encrypted ballot box. When the votes in the ballot box are counted, the administration application permits the various parties involved to check that the number of votes recorded by this meter equates the number of votes in the ballot box and the numer of voters having voted by internet on the basis of the register.

How can we be sure that a temporal link cannot be made between the voter and his vote?

The following 3 points respond to this question:
- Quantum churning completely prevents the original order of the votes being reconstituted by means of, for example, inverse churning.
- Counting of the votes is carried out in the memory without being logged.

- The same responses do not have the same value once encrypted by virtue of the addition of a different cryptography salt for each vote: the encrypted ballot box cannot be reconstituted on the basis of the decrypted ballot box by analysing the results.

Conclusion

In Geneva, eVoting is not a fixed project but instead forms part of a cycle of continuing improvements. The proposed long-term developments are varied and innovative: new ISO certification, securing the voter's computer, accessibility, etc.

In order to remain in the forefront of internet voting systems and to prepare for the standards being debated by the OSCE and the Council of Europe, we are also working on the issue of verifiability, in order to enable voters to check themseleves that their vote has been correctly taken into account ("counted as cast") mirroring the option provided to citizens to attend the counting of the votes in polling stations.

In the course of this article, we have not been able to consider all the measures taken to ensure in the implementation of the electronic vote compliance with all principles governing the conduct of a democratic ballot as defined by the relevant international legislation. We believe it is important to underline in conclusion that the online voting system used in Geneva is fully integrated with the general system for ballot management, in order to prevent multiple votes by a citizen, among other reasons.

Further, the State of Geneva owns the intellectual property of its system, and is responsible for its operation and for developments. We consider that these ownership rights are an essential aspect of the legitimacy of the use of electronic voting. Consequently, all solutions discussed in this article belong to the State of Geneva. These solutions have in many cases been developed specifically to be implemented in the Geneva application and have no equivalent elsewhere.

Geneva State Chancellery
Geneva Information Technology Centre