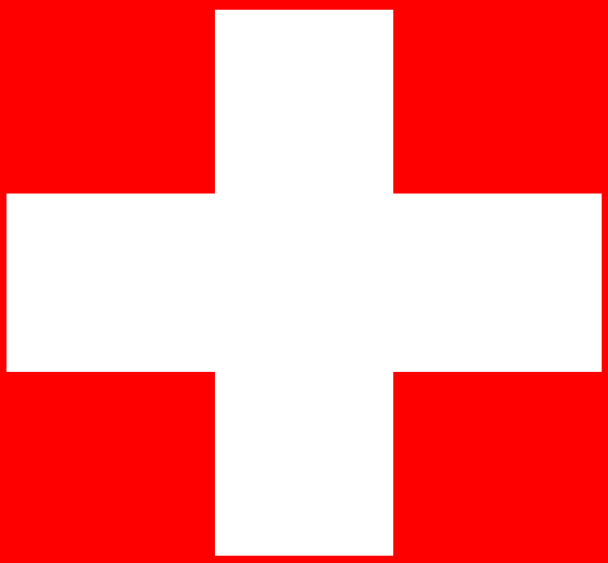


EVOTING BY CHVOTE

CHVote

EVOTING BY CHVote

INTRODUCTION

CHVote is an open source Swiss public online remote voting system (e-voting). It is developed, hosted, operated and owned by the Republic and canton of Geneva.

CHVote is a concrete answer and a real breakthrough in digital technology and e-government. This system is the outcome of a partnership between the State Chancellery and the General Directorate of Information Systems (DGSI) of the Department of Security and Economy (DSE) of the Republic and canton of Geneva.

The State of Geneva is a pioneer in the e-voting domain with 120 polls successfully accomplished (as of June 2017) since 2003.

In 2017, CHVote is offered to nearly 140'000 voters in six cantons (Geneva, Bern, Luzern, Basel-city, Aargau and St. Gallen), for voting on referendums and for electing on the communal, cantonal and federal levels. It also allows people with disabilities to take part in the polls. In 2018, canton of Vaud will do its first evoting test with CHVote.

The noticeable feature of this evoting solution is to be managed by experts in political rights. The Canton of Geneva is both the user and the provider of this system.

THE SWISS POLITICAL CONTEXT

Switzerland is a federal state divided in 26 cantons (subnational level). Political rights are a shared competence between the Federal State and the Cantons, however, most of competences belong to the cantons. Swiss institutions are quite unique. The so-called "semi-direct democracy" enables citizens to challenge any law at any level of authority (municipal, cantonal or federal) or to propose new piece of legislation, provided they collect the legally required number of signatures. As a result, Swiss citizens cast their votes at least four times per year and express their views on a variety of issues and censure or confirm their representatives' decisions. During his/her whole life, a Swiss citizen will vote more than 360 times, that is why in this country we need all the imaginable tools to allow citizens to express their political rights.

In such a context, good organisation, swift ballot counting, a versatile system, a low accessibility threshold to the voting process and a public trust in the system are essential.

Because trust exists, postal voting was introduced in the mid-nineties. Turnout increased by 20 points and has not diminished since. Simultaneously, the voting period has been extended to three weeks. Today in Geneva, home (by post) /remote voting (by internet) represents more than 95% of all votes cast.

This, together with the acknowledgement that postal voting has not solved the accessibility issue for expatriates and disabled voters, has paved the way for internet voting. The validity of this approach has been underlined by 20% increase in the number of Geneva citizens abroad registered to vote in the two years following the introduction of internet voting.

On February 8th, 2009, the Geneva citizens approved by a majority of more than 70% the inscription of internet voting into the cantonal constitution.

Since 2003, there are three ballot-casting channels in Geneva: polling stations, postal voting and remote voting. This is a way to show citizens that their opinion counts and their participation is valued.

EVOTING BY CHVOTE, IT'S…

…TRANSPARENCY AS A PHILOSOPHY AND SECURITY AS A PRIORITY

Since 2010, the Geneva citizens have been granted access to the source code on a written request to the State Council (Government of Geneva). In 2012, two organisations reviewed the source code: Geneva Pirate Party and the University of Applied Sciences of Bern. Recommendations formulated by the reviewers improved the evoting process and/or the system itself.

On January 29th 2016, the Parliament of Geneva, on a proposal from the Government, unanimously adopted a modification of the law, which makes it compulsory to publish the source code of the electronic online voting system on the Internet.

On July 27th 2016, the government chose to uphold the Affero GPL 3.0 free software license for the source code publication. This license is written by the Free Software Foundation, a token of ethical accuracy and international renown.

The State of Geneva thus wishes to increase confidence and trust in a transparent and secure system. The State of Geneva encourages programmer communities to contribute to source code quality and security.

Since March 8th 2015, CHVote is a so-called second generation system with security requirements laid down by the Swiss Confederation (thanks to the third report of Federal Council) by implementing individual verifiability.

… AN HISTORY: CHVOTE MILESTONES

2001	Start of the Geneva internet voting project
2002	16'000 students test the system's ergonomics and usability during a test ballot.
2003	First binding e-Enabled referendum in Europe in the Geneva municipality of Anières.
2004	First binding e-Enabled federal referendum in two cities and several villages around Geneva. The Council of Europe organises a consultation on the "Charter for a violence-free school" among its 47 member states using the Geneva evoting system.
2005	First cantonal e-Enabled referendum in Geneva. Publication of a socio-political study on the profile and motives of internet voting users.
2006	First e-Enabled election in Geneva to designate the University of Applied Sciences' council.
2007 -08	As the Geneva parliament debates electronic voting, the e-Enabled ballots are suspended in order not to collide with the parliamentary debate.
2009	A constitutional amendment allowing internet voting is approved in a popular referendum by a 70.2% majority. First e-Enabled ballot for overseas Swiss citizens. Start of collaboration between the canton of Geneva and the canton of Basel-city.
2010	The cantons of Bern and Luzern begin a collaboration with Geneva to use CHVote.
2011	First eEnabled national elections.
2013	Presentation of public Audits to Parliament.
2014	End of Wassenaar Clause which allows all Swiss living abroad to use remote online voting, if the evoting channel is offered by their canton. Change of Swiss federal Ordinance concerning the political rights and came into force of th Swiss federal chancellery ordinance on Electronic Voting (VEleS).
2015	First e-Enabled referendums with the new evoting platform using the individual verifiability (36^{e} e-Enabled ballot). Municipal eElections in the canton of Geneva (37^{e} and 38^{e} e-Enabled ballot). Government's proposal to change the political rights law by publishing the source code of the evoting system. National eElections (40^{e} and 41^{e} e-Enabled ballot) for the cantons of Geneva, Luzern and Basel-city.
2016	Government's proposal concerning the publication of the source code is adopted with unanimity by Parliament. Partnership with University of Applied Sciences of Bern (BFH) to develop the universal verifiability. Publication on GitHub of the first elements of source code: the offline Console.
2017	Publication on GitHub of the prototype of a next-generation evoting system. e-Elections of the Swiss living abroad association (ASO) representatives from Mexico ar Australia. Aargau and St. Gallen begin collaboration with Geneva to use CHVote.

… A SYSTEM UNDER PUBLIC SCRUTINY

The Geneva internet voting system's operation relies on well-defined procedures based on a strict separation of duties and rights.

For the initialisation and decryption of the electronic ballot box, a representative of the State chancellery, four representatives of the Central Electoral Commission (CEC), a representative of the State election service, a notary, an IT security officer from the police, the internet voting network administrator (NA) and the administrator of the internet voting system (system administrator or SI) come together. Should one of them be missing, it would compromise the system's initialisation or decryption.

The participants meet in a room fitted with a dedicated and secure (4-eyes authenticated and traceable) network connection to the electronic ballot box. The NA connects the PC to the internet voting specific network.

Using a 4-eyes identification process with 2-factor-authentication, the SI starts a connection to the internet voting system on the administration PC. The SI launches the generation of a pair of asymmetric vote encryption keys, which is composed of a public vote encryption key and a private vote decryption key, as well as of a symmetric key to check the integrity of the ballot box.

The CEC members are divided into two groups of two people. Each group generates a password, the combination of the two locking the ballot box encryption key or - for the decryption - enabling this key to be unlocked. For decryption, should either of the groups not recall its password, it can be recovered by opening a sealed envelope provided by the notary. The notary is the person in charge to keep all the sealed documents.

The ballot box is illegible during the voting session by virtue of the use of an asymmetric key. Only the public encryption key is available to the system while the private decryption key is stored in a secure place, protected by passwords. The public encryption key is used by the system to encrypt the votes into the ballot box.. The ballot box cannot be tampered without the system detecting it thanks to a harness of integrity checks relying on a cryptographic integrity chain of the votes that would raise an alert in case of discrepancy.

Thanks to the mandatory access to the system using 4-eyes identification and full tracing of all administrative actions, a single insider attack on the ballot box is impossible without detection, while ballot decryption and counting is impossible without the presence and participation of the CEC acting as representative of the citizenry. The public administration is confined to its role of support of the process whose owner is the CEC.

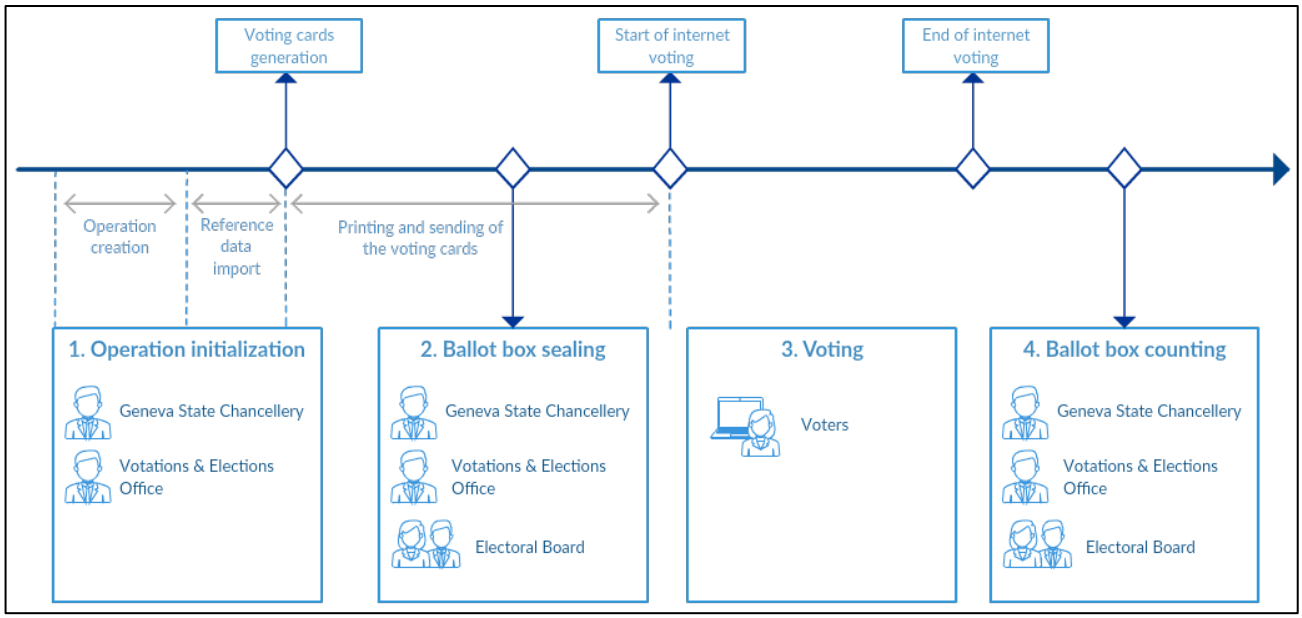


Figure 1: The life cycle of a ballot with CHVote

…THE ID ISSUE

Dealing with ID management for internet applications raises a fundamental question: how do I ensure you really are who you say you are?

In the physical world, this answer is easily provided. A passport, an ID card or a driver's license settles the question. To obtain an ID from the state, one has to come in person and provide a pre-existing document whose origin can be traced back to the official record of one's birth. At that moment, let's call it time zero, our parents created our identity and the state gave it a material existence.

In the digital world, there can be as many "time zeros" as one decides; anyone can assume as many names, gender and ages as she wishes. Therefore, the central question becomes: is it acceptable to fully dematerialise the digital ID?

The Geneva answer is no, because digital certificate issuers do not carry out the extensive checks performed in the physical world to ascertain one's identity and because too often the certificate's control is delegated to the browser, which can be compromised.

This does not mean that online authentication has to be complex. In Geneva, we implemented an authentication procedure relying on personal information we send to the voter and on so-called "shared secrets", that is information that both the voter and the administration have but that is not exchanged in the pre-voting phase.

Before every ballot, Geneva voters receive by post a single use voting card (figure 2). It is their numerical ID. This card carries the randomly-produced one-time voter's ID number and her PIN code. To validate their ballot, the voter must type their birth date.

Other modalities to fight fraud can be thought of, such as:

- Adding a personal question in the voting procedure. Depending on the answer, the vote would be recorded or not.
- Limiting the number of votes cast from a single IP address.

- Performing forensic statistical checks.

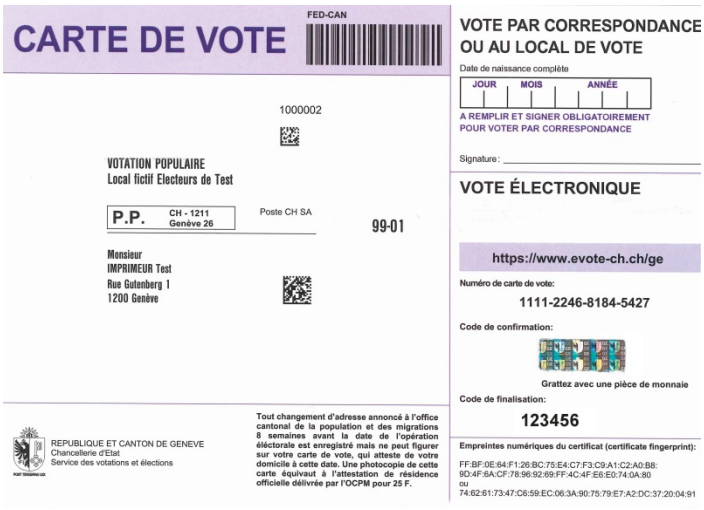
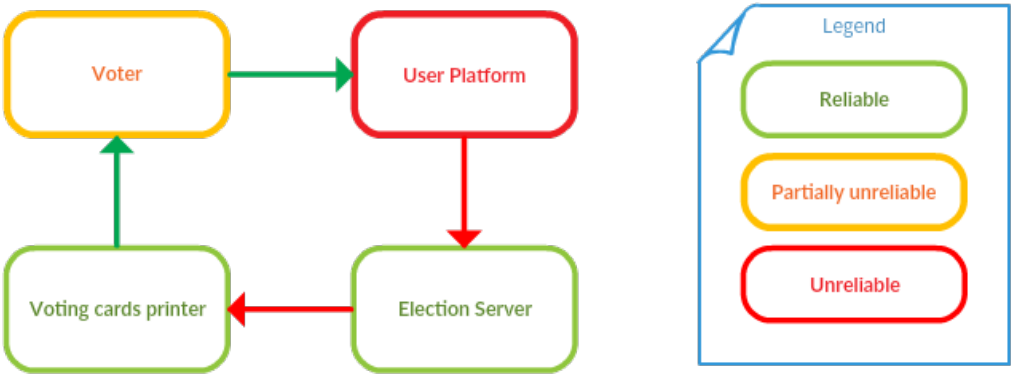


Figure 2: example of a voting card

… THE SECURITY, ALWAYS A PRIORITY

Conforming to the Swiss federal chancellery ordinance on Electronic Voting (VEleS), a system that complies to the following trust model can be offered up to 30% of the resident voters.



The security objectives defined by this ordinance are correctness of the results, protection of voting secrecy, non-disclosure of early provisional results, availability of functionality, protection of voter information and absence of proofs of voting behaviour in the election server.

Many security measures are implemented to address the security requirements and the security risks, the main ones being:

Secure software development lifecycle:

The system development follows a secure software development lifecycle. The following activities are actively held:

- The IT specialists follow security training plans (secure software development, secure infrastructure operations, etc.).
- The business stakeholders follow security awareness programs, in particular concerning data treatment, exchange and storage.

- The security requirements are first class citizens among the no-functional requirements of the evoting system. They are derived from the legal requirements, the best practices and the business functionality. They also include access control matrices.
- The threats to the evoting system are modelled and rated, and include attacker profiles from outside and inside the organization. Furthermore, the abuse cases are built and maintained.
- The software is built using approved third-party and custom developed security components. The team is aware of the secure design patterns and applies them according to the developer guidelines documentation.
- The design of the system is checked against the threat and security models. Any major change to the security design of the system is also reviewed by a third-party security expert.
- A manual code review is performed on all the committed source code. It is based on the OWASP ASVS and checks the use of the project security design patterns. Automated static checks are also performed to find security flaws.
- A third-party code review is conducted by a secure coding expert on every major releases of the application.

Security testing:

- The application's security features are automatically checked with specifically developed integration tests. A third-party penetration test is conducted by security experts on every major releases of the application or of its infrastructure.
- Automatic vulnerability tests are run over the voting services and its infrastructure. The IT specialists (infrastructure as well as software) conduct a security watch for the domains under their responsibilities. Patch assessment and deployment is also part of the process.
- The server infrastructure is hardened according to the CIS security benchmarks. This covers the operating system and the installed middleware.

Logical access control:

- A privileged access management (PAM) system ensures that the system administrators can have access to the evoting infrastructure only through a four eyes connection policy: a user requests a connection, which another user authorizes. It also involves a strong authentication with personal accounts. Once connected, all the actions are then logged by the PAM system, either when using a ssh or a RDP connexion.
- The access to the evoting administration application complies with the same rules. It is the reason why it runs in a virtualized environment, ensuring four eyes connection with strong authentication and traceability through the RDP channel.

Physical access control:

- The evoting infrastructure is placed in secured rooms, whose access are controlled and logged.

File system integrity:

- The integrity of the web server and of the application server file systems is checked from the production deployment to the vote closing. It allows to detect any change in the parameters, in the application or in the cryptographic data. A probe sends an alert in case of integrity inconsistencies.
- An additional preventive measure consists in having an immutable zone in the file system that is activated from the ballot box initialization until the vote is closed. This zone stores all the data than should not change during this period.

Sensitive data protection:

Sensitive data is stored in the evoting database and consists mainly of the voting card identification and authentication data, as well as the return codes. As per the best practices, cryptographic protections are applied. Two kinds of solution are used:

- HMAC-SHA256 using a key known to the voting servers only for data not needing to be retrieved in clear text. No rainbow table can be generated without knowing this key.
- AES256-GCM encryption for data to be retrieved as clear text (return codes, birth date for statistics purpose).

Whitelisting:

Whitelisting is a key security design pattern used throughout the evoting system for validating user input:

- At the reverse proxy level, for each service published by the application:
  - a regular expression pattern defines the URI validity (rewrite rules). It validates the incoming requests URI method, path and parameters.
  - a regular expression pattern defines every expected body request parameters (custom ModSecurity rules).
  - In case of mismatch, a 403 error page is issued.
- At the internet voting application level, every expected request parameters are validated against regular expressions or custom business rules, as well as their completeness. Unexpected parameters are rejected. In case of invalidity, a 403 error page is issued.
- At the regular expression patterns level, whitelisting is also preferred to excluding for example specific characters for validating user input.

Monitoring of the system integrity:

A monitoring application checks regularly the state of the system and raises alerts in case of failures. It runs a collection of probes, the security-wise main ones being:

- A probe that casts votes in a test ballot box through the internet voting application services.
- A probe that checks that there are no more ballots in the ballot box than there are in a log recording the fingerprints of each received ballot.
- A probe that checks that there is the same number of ballots in the ballot box than the number of voting cards that have used the internet voting channel.
- A probe that checks the integrity of the election data stored in the database.

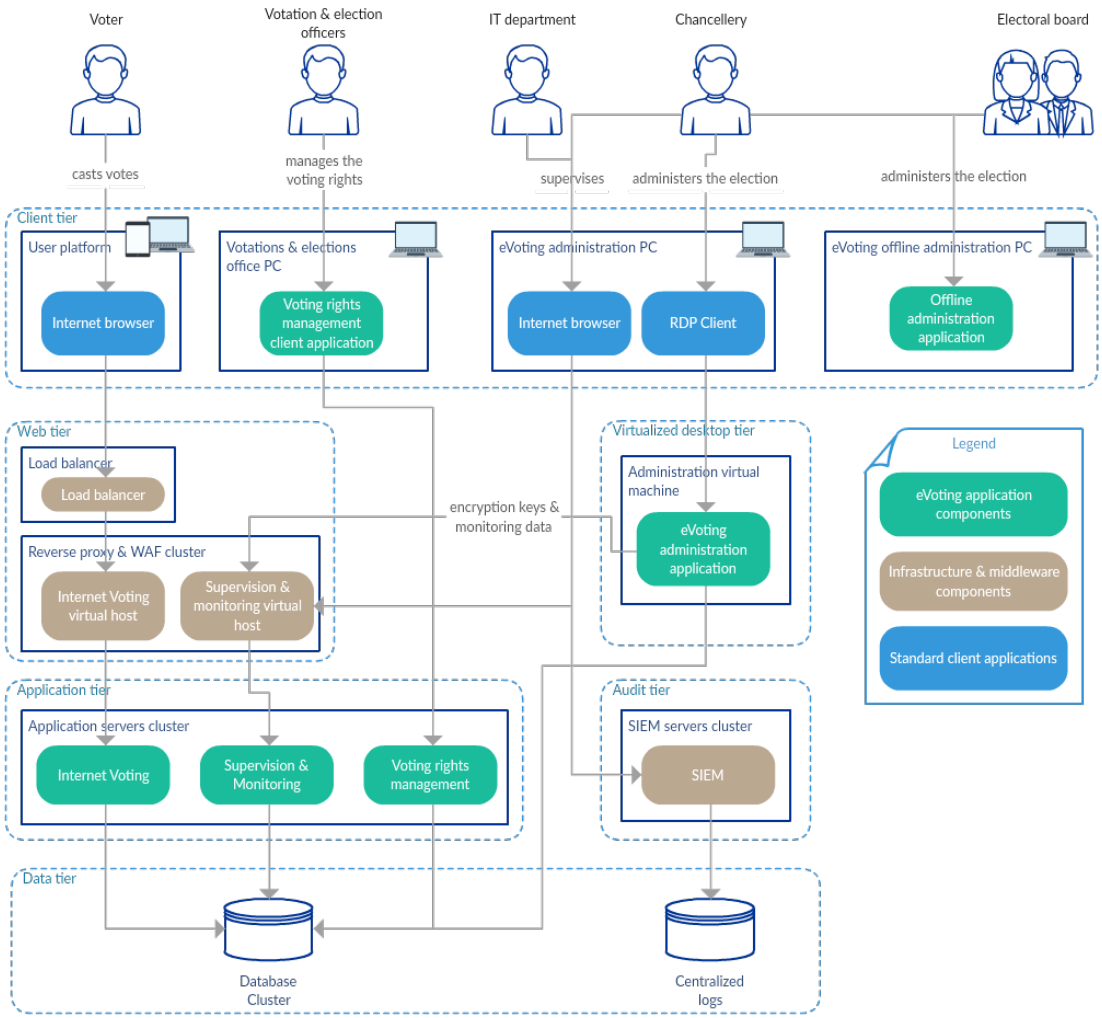
Logging:

Logs are generated by the evoting system applications. They are sent to a central SIEM system for collection and integrity guarantee (the SIEM system uses fingerprints and block chaining):

- At the application servers level, adding to the middleware standard log files (access and error logs, ModSecurity logs, application server logs), custom logs are used by the applications:
  - Security event log: results (OK or KO with reason of failure) of identification, authentication, confirmation, vote record, etc.
  - Vote fingerprints log: index of the vote along with the authentication tag provided by the encryption algorithm.
  - Performance log: the time used to serve each request at the application level.
  - Monitoring probes results log

- At the administration application level, every action of the user is traced into a security event log (database initialization, date of opening and of closing entry, etc.).

Architecture of the system:



… CITIZENS AT THE HEART OF THE PROCESS

The individual verifiability has been used for the first time on March 8th 2015. The individual verifiability gives the voter a way to check that her ballot has been received untampered by the server (*cast as intended*). Concretely, the voter receives with its voting card a list of codes related to the answer (yes; no; no answer) in the case of referendum (figure 3), or related to a candidate in the case of elections. Each code is unique for each voting card.

VOTATION POPULAIRE 14 juin 2015

Liste des codes de vérification pour le vote électronique uniquement

Liste de codes pour la carte n° 9559-6518-5896-3977

Votation fédérale							
Question n° 1	OUI	**Q7S7**	NON	**P5K6**	BLANC	**B2X3**
Question n° 2	OUI	**R8V6**	NON	**M4M2**	BLANC	**K8Q8**
Question n° 3	OUI	**R8Q6**	NON	**V2W9**	BLANC	**M7E5**
Question n° 4	OUI	**U3X3**	NON	**M2T3**	BLANC	**A7P6**

Votation cantonale							
Question n° 1	OUI	**T8G6**	NON	**V3U6**	BLANC	**Y4W5**

Figure 3: example of codes in the case of referendums

…USABILITY AND ACCESSIBILITY

One of the added values of electronic voting compared to paper-based voting lies in its enhanced usability. In the Geneva system, this translates into:

- A large choice of supported OS/browser configurations.
- The possibility to vote in any of the four Swiss national languages.
- Assistance tools integrated into the voter interface, such as direct access to the political parties vote recommendations in the case of referendums.
- Prevents to cast an invalid vote thanks to the user interface.
- Prevention of disenfranchisement, by the existence of multiple voting channels. if the security of the internet voting channel appears compromised, a voter may turn to another voting channel
- In a complex electoral system such as Switzerland's, where you can mix candidates from different parties on your ballot up to the number of seats to be filled, the user interface indicates how many suffrages are used, how many are left and how the suffrages will be awarded to the different parties.
- A recap of choices is displayed to the voter so that she can correct any mistake before authenticating herself.
- Thanks to the individual verifiability (codes of verification), the voter has the possibility to check that its ballot has been received untampered by the server (*cast as intended*).
- Confirmation of the vote successful registration. The voter knows that the vote will be counted.
- Helpdesk is opened during ballots.

Accessibility, the twin sister of usability, has also been taken into account:

- Simple and intuitive user interface, compatible with web surfing devices for visually impaired voters.
- Voting procedure modelled on the paper-based voting procedure.
- No pre-registration required, all you need is the single-use voting card that you receive home.
- No assistance needed to vote for visually and mobility impaired voters.
- Possibility to use any computer, laptop or smartdevices.

60% of Swiss citizens living abroad and almost 100% for Swiss living very far away from Switzerland (USA, Oceania) use e-voting to express their political opinion. This channel of voting is also very important for people with disabilities: they are able to vote with more autonomy.

… A CONCRETE TRANSPARENCY

Transparency is a growing requirement facing electronic online voting systems. While some keep arguing that transparency is inherently impossible with eVoting, examples of the contrary abound.

Geneva has implemented a set of measures aimed at making the system and its operation as transparent as possible. These measures encompass the system's documentation, the system's operation or predictive testing, and the publication of the source on an free software licence.

Documentation:

- Availability of the source code on Github platform (https://republique-et-canton-de-geneve.github.io/chvote-1-0/index-en.html).
- Regular audits whose final reports are made public (every three years).
- Studies by the Geneva University on the impact of electronic voting on the citizens.
- Detailed statistics on the usage of internet voting by age, gender and municipality.
- Ballots results published by voting channel (polling stations, postal vote and internet voting) as well as consolidated.

Operation:

- Strict division of duties and responsibilities

Testing:
Before each ballot, the system is submitted to a set of tests that replicate the conditions of an actual ballot. Only when these have been successful can the system be sealed for the forthcoming electoral operation. These tests are:

- Performance test controlling the level of service and the system's response time.
- Predictive test where more than 200'000 votes are cast and counted. As the votes' content is defined beforehand, we can control that the counted result is in accordance with the input.
- OS/browser compatibility test.
- Breakdown tests: how does the platform react to the breakdown of one of its components? How does the maintenance team react?
- Alarm test: does the monitoring system work? Does it activate alarms when it is expected to?

Besides these, we also conduct the following tests:

- Testing each ballot for integrity and validity code before accepting it into the eBallot box in order to prevent accepting malformed ballots into the eBallot box that could lead to unexpected results.
- Calling a randomly selected sample of 2% of citizens having cast a remote ballot to ensure they have voted themselves and without constraint.
- Use of a "control polling station" where the members of the Central Electoral Commission cast votes using the Internet voting system and keep track of their votes on paper. This virtual polling station is the first to be counted on ballot counting day, in order to compare the ballot box content with the paper records.
- Weekly security log analysis looking for suspicious voting session patterns.

… GOING TO OPEN SOURCE

The open source issue is not a technical question, but a political one. It has more to do with legitimacy than with security. A fully open source solution would be auditable by any computer specialist anywhere. This would promote this specialist to the role of guarantor for the system's fairness, while he may not be connected at all with the community using it. Is this democracy?

What is important for traditional ways of voting (local or postal) is even more essential for evoting.

One thing is clear: in order to ensure the highest level of security and trust, the system has to be developed and operated by the State. It is a deliberate choice not to depend on private companies. In the CHVote philosophy, political rights are a domain which is not profit orientated and cannot be delegated to a private company.

This first publication of the source code concerned an element currently used, it is the software used to decrypt the e-ballots. The second publication happened on 20th April 2017 with the prototype of the cryptographic protocol of the universal verifiability. This early publication is designed to encourage the collaboration of the experts community and to improve the protocol before its realization. The publication of the source code will be made step by step until the whole code is published by the end of 2018.

The use of open source is an active transparency, where the public is able to review, exchange and improve the source code itself. A few years ago, sceptics and opponents to e-voting criticized CHVote system. Today, we are discussing with them. This discussion was the first step of this transparency approach and as a next step, we are eager to work with any willing person interested by this problematic. The aim is to co-create in order to obtain the best system, open and secure.

Today, security is openness: the more is shown how things are done, how they work, the more we learn from expertise outside the group of developers, the more we build trust.

For more information: www.chvote.ch

COMPARISON OF VOTING CHANNELS IN SWITZERLAND

This table highlights the theoretical strengths and weaknesses of different voting channels.

Channels Risks	Paper-based polling station voting	Voting machines in polling station	Postal voting	Internet voting
Existing in Switzerland	Yes	No	Yes	Yes (in some cantons)
Accessibility	Problematic for some voters' groups such as visually or mobility impaired persons	Problematic for some voters' groups such as mobility impaired persons	Problematic for some voters' groups such as visually or mobility impaired persons	Good
Casting an invalid vote	Yes	No	Yes	No
Counting errors	Yes	No	Yes	No
Family voting	Possible	Possible	Possible	Possible
Insider tampering	Can be prevented	Can be prevented	Can be prevented	Can be prevented
Loss of votes	Yes	Yes	Yes	No
Loss of vote anonymity	Possible	Possible	Possible	No
Public control over the process	Yes	Possible	No	Yes through Electoral Commission, publication of source code and open source
Transparent voting and counting process	Yes	No	No	Yes through proxies (Electoral Commission), publication of source code and open source
Usability	Can be problematic	Good	Can be problematic	Good
Vote change without voter's knowledge	Possible	Possible	Possible	Impossible thanks to individual verifiability

GLOSSARY:

Affero 3 GPL: complete information available on https://www.gnu.org/licenses/agpl.txt.

Auditability (end-to-end)**:** E2E auditable systems allow verifying that the votes were not modified at any stage of the process: vote casting, vote storage and vote counting. In Geneva, the control municipality provides an E2E control over the system, but not over each single vote.

Control municipality: the control municipality is a virtual constituency which is used in Geneva to perform a predictive test on the voting system.

Electoral roll: in Geneva, there is one single roll so that, irrespective of your voting channel you can only vote once. The roll is fully anonymous, citizens are only known by their voting card number, which changes for each ballot and is randomly generated.

Electronic ballot box: in Geneva, votes are stored encrypted in the eBallot box. A salt is added to each encrypted vote, so that no two similar votes look the same. Ballots are protected with two layers of authenticated encryption, one using the Electoral Commission's asymmetric key (generated anew for each election / vote), and the other using a symmetric key inaccessible from the database, as a measure to ensure the integrity of the ballot box.

Family voting: family voting refers to the pressure from any third party voters can be exposed to when voting remotely.

Free Software Foundation: is a non-profit organization founded in 1985 to support the free software movement. "Free software developers guarantee everyone equal rights to their programs; any user can study the source code, modify it, and share the program". More information available on http://www.fsf.org/

Hardening: software hardening consists in a careful customisation that only allows requests compatible with a legitimate transaction to be answered. Any other request will not yield any reaction from the system. The same can be applied to hardware, operating system and to the interaction between systems. In Geneva, we have carefully hardened all our components.

Individual verifiability: individual verifiability refers to the possibility given to each voter to check that her vote is received unaltered in the system. CHVote already offers this.

Man in the browser (MITB): this type of attack infects a web browser by taking advantage of vulnerabilities in browser security. It can modify web pages, or modify the data sent to the server in a completely covert fashion. The CHvote system prevents such attacks from having an impact on the integrity of the result by using individual verification.

Man in the middle (MITM): the man in the middle attack consists in intercepting the exchanges between two points to change the content of the communication. The protection against this kind of attack is the use of individual verifiability which gives the voter the possibility to check that the ballot has been received by the system untampered

Mixing process: mixing processes are algorithms applied to the eBallot box before decrypting and counting the votes in order to read them in a random order, breaking any potential vote-voter chronological link. In Geneva, an irreversible mixing process is applied to the votes before decrypting them.

Open source: complete definition available on https://opensource.org/osd-annotated**.**

Predictive test: a predictive test is a test whose expected results are known in advance and compared to its effective outcome.

Random phone control: 2% of the remote voters for any ballot are called by the Geneva administration to inquire about the conditions of their voting.

Receipt-freeness: a receipt-free voting system does not allow voters to show a third party how they voted. The Geneva system is receipt-free.

Statistics (forensic)**:** forensic statistics refer to tests that can be performed ex-post on a ballot result to check its likelihood in a given context.

Universal verifiability: universal verifiability refers to the possibility given to all voters to check that a ballot outcome is correct. Geneva is in the process of developing it.

PRESS REVIEW (IN ENGLISH ONLY)

Media

SocietyByte (27 June 2016) "E-voting: when transparency means more security" https://www.societybyte.swiss/2017/06/26/e-voting-when-transparency-means-more-security/

European Commission – Join up (15 December 2016) "Geneva canton publishes eVoting system source code" https://joinup.ec.europa.eu/community/osor/news/geneva-canton-publishes-evoting-system-source-code

WRS (Swiss radio in English) "Geneva to boost e-voting" https://worldradio.ch/news/2016/09/15/geneva-to-boost-e-voting/

Swissinfo (13 September 2016) "Geneva mounts e-voting charm offensive" https://www.swissinfo.ch/eng/politics/pitching-for-partners_geneva-mounts-e-voting-charm-offensive/42439582

WRS (Swiss radio in English) (24 March 2016) "Geneva plans evoting for all" https://worldradio.ch/news/2016/03/24/geneva-plans-e-voting-for-all/

Academic Papers

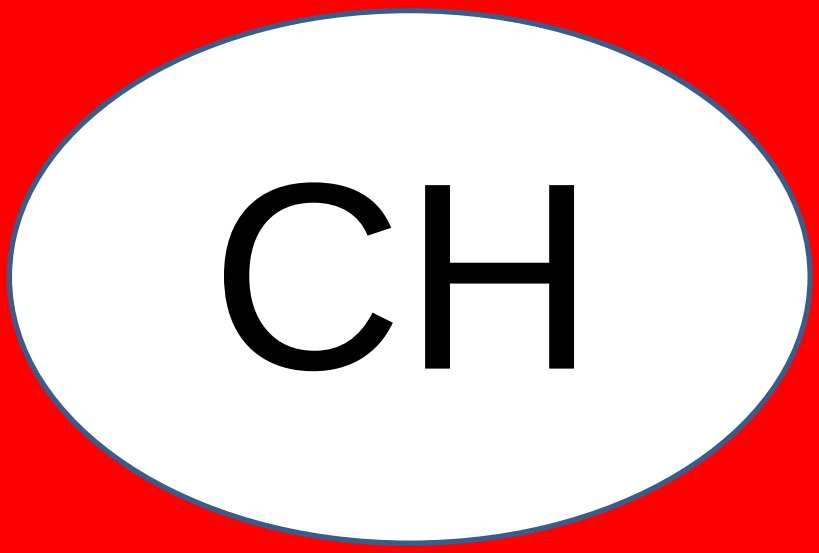
"CHVote System Specification" Rolf Haenni, Reto E. Koenig, Philipp Locher, Eric Dubuis (April 2017) https://eprint.iacr.org/2017/325.pdf

"Cast-as-Intended Verification in Electronic Elections Based on Oblivious Transfer" Rolf Haenni, Reto E. Koenig, and Eric Dubuis (September 2016) https://e-voting.bfh.ch/app/download/6525334361/HKD16.pdf?t=1484052996

Links to source code

Github platform https://republique-et-canton-de-geneve.github.io/chvote-1-0/index-en.html

September 2017


CH