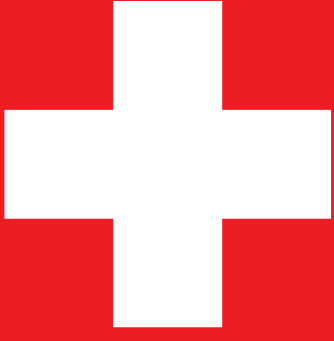
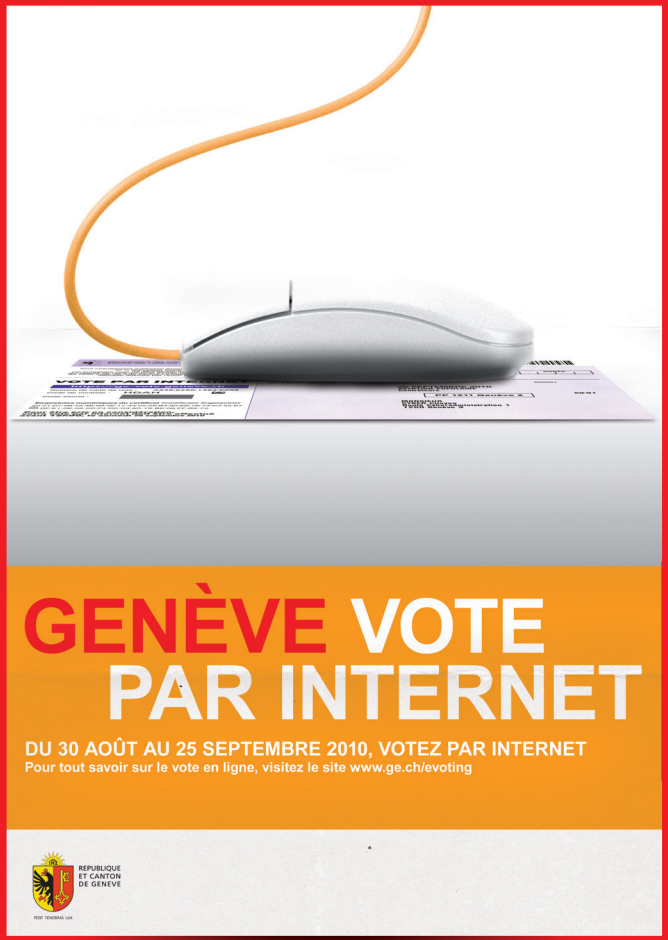


REPUBLIC
AND STATE
OF GENEVA

POST TENEBRAS LUX

POST TENEBRAS LUX

THE GENEVA
INTERNET VOTING SYSTEM



THE GENEVA SYSTEM'S MILESTONES

2001 : Start of the GVA internet voting project.

2002 : Ergonomic and usability tests followed by an eEnabled referendum where 16'000 high school students test the system's robustness.

2003 : 1st binding eEnabled referendum in Europe in Anières. A 2nd binding eEnabled referendum follows in Cologny. GVA internet voting system finalist of the 1st eEurope Awards ever.

2004 : 1st binding eEnabled federal referendum in Switzerland. The Council of Europe organizes a vote on the "Charter for a violence-free school" with the GVA internet voting system. The GVA system is awarded a prize by the Swiss Society for Administrative Science. The GVA system presentation video is distinguished by the Pirelli Awards.

2005 : 1st cantonal eEnabled referendum in GVA. Socio-political study on the profile and motives of internet voting users. 1st implementation of the secure channel, which solves the SSL pipe's vulnerabilities. The GVA internet voting system is finalist of the 2nd eEurope Awards.

2006: 1st eEnabled election in GVA to elect the technical university's council. GVA government report on internet voting. The GVA internet voting system is finalist of the Stockholm Challenge.

2007

2008 : As the GVA parliament debates internet voting, eEnabled ballots are suspended so as not to collide with the debate. The GVA internet voting system is awarded the EU "Good practice" label of the eEurope 2010 initiative. The GVA internet voting system is finalist of the United Nations Public Service Awards.

2009 : Constitutional provision on internet voting is approved in a popular referendum by a 70.2% majority. 1st eEnabled ballot for overseas Swiss citizens. Start of the collaboration between GVA and other cantons on internet voting. The sharing of voters' registers between these and GVA allows them to offer remote electronic voting without purchasing or developing their own system.

2010 : 17th eEnabled ballot by the end of the year.

2011 : 1st eEnabled municipal and national elections.

Access our reports on the web by capturing the Q-codes with your smartphone

THE WORLD NEEDS PIONEERS

Our growing mobility makes us feel increasingly torn between our duties as citizens and the requirements of our careers and social life. Whether for nurses, doctors, lawyers, tourism operators or bankers, a stint of a few years abroad is indeed fast becoming a necessity in one's professional path. We all maintain cross-border friendships, our relationships network spans several countries and, as we travel more and more, we are often not at home on ballot days.

As an elected official, I am convinced that something must and can be done to reconcile our private and public persona. Geneva, a hub for many high tech companies and research centres, decided to offer its citizens internet voting. This voting channel has been a reality since 2003.

For some, internet voting for binding public ballots is an oxymoron: too risky in the current state of the technology, too vulnerable to insider fraud, and not transparent enough - there are unlimited apparent reasons not to touch it. Should we then sit by the roadside and watch the traffic passing by?

In Geneva, we believe that if you do not develop and test innovative solutions, they will never happen. Critics and sceptics are needed, but so are pioneers willing to take risks to achieve technical and social breakthroughs.

The Geneva internet voting system is a mix of detailed procedures, selected and hardened hardware and mostly open source software and, on top of that, a solid dose of common sense, operating in a thorough legal framework.

Reading these pages, you will see that internet voting in Geneva is very much context dependent, as it should indeed be. The institutional framework, legal regulations, political traditions and the extent of citizens' rights vary from country to country. Yet, Geneva has successfully established partnerships with other public entities in implementing its system, showing that it is possible to tailor a common technical base to fit different contexts.

The State of Geneva owns the intellectual property of its system and it is willing to help any interested public entity in implementing it. Discover more abut this application by visiting www.ge.ch/evoting and contact us for any questions. We look forward hearing from you.

Anja WYDEN GUELPA
Geneva State Chancellor

THE SWISS CONTEXT

Swiss institutions are quite unique. In this so-called semi-direct system of democracy, citizens can challenge through the polls any law voted by any level of authority (municipal, cantonal or federal) and propose any new piece of legislation, provided they collect the legally required number of signatures, which they regularly do. As a result, Swiss citizens have to vote four to six times a year to censure or support their MPs decisions.

In such a context, good organization, swift ballot counting, versatility of the system and low accessibility threshold to the voting process are essential. And so is public trust in the system, the authorities and the civil servants.

Because trust exists, remote ballot casting in the form of postal voting was added to polling station voting in the mid-nineties. This led to a trend towards home voting, which today in Geneva represents some 95% of all cast votes. Parallel to the introduction of postal voting, the ballot casting period was extended to three weeks. The impact of these changes was immediate: turnout increased by 20 points and has not diminished since.

To ensure that no-one casts a vote on behalf of a third party, random controls were introduced: for each ballot, the state phones 2% of the citizens who mailed their ballot paper back to ensure they did it themselves, freely and without any supervision or constraint. The records of such controls show that voters behave in a very responsible way.

This, together with the fact that access for overseas voters' was not solved by postal voting, opened the way for internet voting.

Trust is a two-way process. The legitimacy of online does not just rely on an administrative decision alone or on its approval by the parliament, but also on its support by civil society. On February 8th, 2009, Geneva citizens approved with a 70.2% majority an amendment introducing internet voting in the cantonal constitution and creating a permanent electoral commission. Trust does not exclude control, on the contrary: control reinforces trust.

So today in Geneva, there are three fully integrated ballot-casting channels: polling stations, postal voting and internet voting. This is the Geneva way to show citizens that their opinions count and their participation is valued.

THE LEGAL FRAMEWORK

Cantonal and federal lawmakers have developed a set of binding rules specific to internet voting. The main provisions under which the Geneva system operates are as follows:

1. Visually impaired voters should be able to vote online.

2. The electronic voting application must be clearly separated from the state's other IT applications.

3. Systematic fraud, systematic vote hijacking on the internet and systematic identity theft shall be impossible.

4. Voters should be provided a way to ensure that they are voting on the State's official web site and should be informed that their ballot has been properly cast and stored in the electronic ballot box.

5. Stored votes should be totally anonymous and all procedures should be organised in such a way that it will not be possible to identify any voter.

6. Vote counting order must not be the same as vote casting order.

7. Whilst a ballot is ongoing, any intervention on the system must be made by a team of two technicians and duly registered.

8. The independent electoral commission, formed by members of political parties as well as lawyers and IT specialists, can supervise and question any ballot. It locks the electronic ballot box by generating its encryption keys, thus ensuring that nobody can access the electro-

nic votes until ballot counting day. This commission can access any document regarding the electronic voting system. It can mandate any audit, test or study by any expert of its choice.

9. The electoral commission, as well as scholars and academics can access the source code at any time.

10. The internet voting system must be audited on a regular basis; the results of the audits are public.

Requirements 1 to 7, prescribed by the federal law, are to be validated by an independent body nominated by the federal authorities. Requirements 8 to 10 are written into the cantonal law.

PROJECT MANAGEMENT

Internet voting is a sociological project before being a technical one. The issues to be solved are first and foremost social ones: acceptance of a virtual voting channel, creation of trust in the system and definition of procedures that minimize human error and hidden manipulation possibilities. Only then comes the technique. The Geneva internet voting project has been managed accordingly.

The initial decision was to create a widely accessible system; one that does not oblige voters to own or purchase any particular infrastructure beyond a PC and an internet access. Voters wishing to vote online should not be required to pre-register with the state.

The Geneva University was appointed to conduct legal and socio-political studies, IT companies were mandated to develop aspects of the application, audit its security and perform intrusion tests. An ISO 27001 certification process was conducted.

Ergonomic tests helped define the user interface. Mass voting was simulated to challenge the system's robustness and availability. A website (www.ge.ch/evoting) has been set up since the advent of the project to inform citizens and provide a contact platform.

The Geneva parliament has been involved on a regular basis, either through its Commission on political rights or its plenary body.

The development of the internet voting application has relied as much as possible on the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting.

OF PAPER TRAIL, BALLOT RECOUNT AND FORENSIC STATISTICS

It is often asserted that electronic voting makes it impossible to recount votes, whilst paper ballots allow it. This claim deserves attentive cross-examination.

What is being (re)counted when (re)counting paper ballots? The US 2000 presidential election, for instance, showed that paper ballots are no panacea as they offer no guarantee that the voters' will can be read without ambiguity. Furthermore, paper ballots do no prevent counting errors. And two manual counts will always yield two different results. When the gap between two candidates or referendum proposals is wide, this is not a problem. But when the margin is narrow, the limits of paper ballots with or without manual counting become obvious.

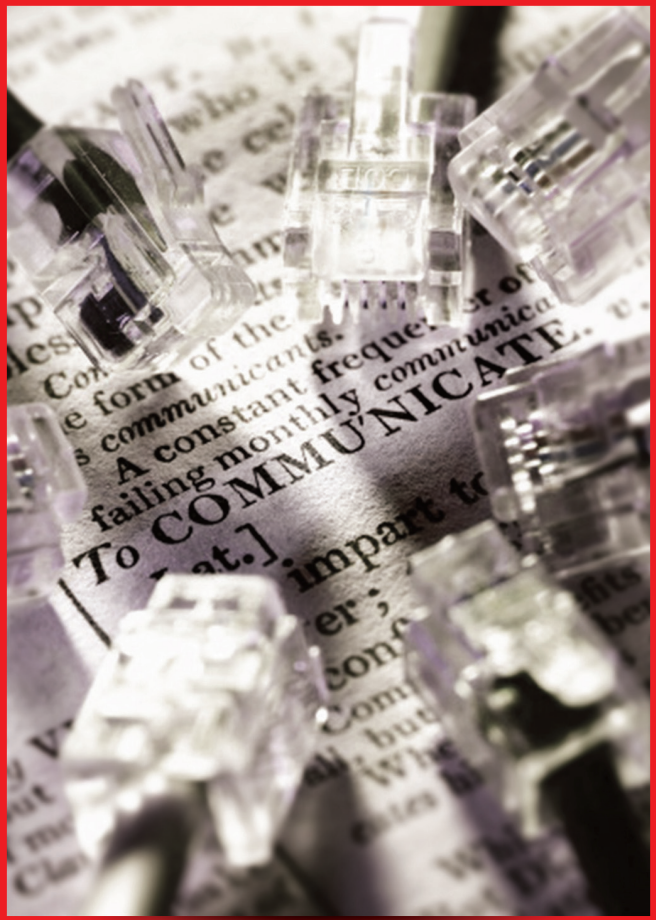
What about electronic voting? In the Geneva system, counting electronic votes does not destroy them. A recount is possible, from the same source or from one of the three mirror ballot boxes built into the application, using the same counting software or another one.

For any ballot, it is possible to display the outcome, either question by question (a typical referendum ballot in Switzerland will carry 3 to 6 different questions) or individual ballot by individual ballot - that is citizen by citizen. It is also possible to produce an image of each single ballot. This enables a comparison of both results to see whether they match.

A virtual municipality has been added to the system, to enable predictive testing. Members of the electoral commission cast votes for this municipality and record them on paper so that this municipality's results are known beforehand. On ballot counting day, this "control municipality" is the first to be counted. Paper records and electronic votes must coincide to show that the system records and stores the votes as cast.

Finally, systematic forensic statistic checks are performed on the electronic votes' results after each ballot. Two tests are used. The first one is based on the Benford law, which tests the probability of distributions and singles out non-random ones. The second one implements the Robust Overdispersed Binomial Model that compares the ballot result in a constituency to the voting history of this same constituency to see whether the last result is in line with the historical record.

The true issue in remote electronic voting lies upstream: it is the quality and the integrity of the data contained in the electronic ballot box. In Geneva, a java applet combined to a servelet compares each single vote with all possible options before it reaches this box. The same control is performed at the server side. Any vote which does not fit into this referential is rejected and the voter is informed to cast his vote in another way. This ensures that all accepted votes are valid and readable.



SOME WORDS ABOUT 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 from A to Z by any computer specialist anywhere. This would promote the IT specialist to the role of guarantor for the system's fairness, even if he may not be connected at all with the community using it.

Is this democracy? Or isn't democracy rather a set of known and accepted rules and procedures whose implementation is verified by an official commission? And doesn't sovereignty also encompass the freedom to choose one's reviewers and auditors?

In Geneva, the opinion has always been that the state must own the intellectual property of its internet voting system. Black boxes are not acceptable. This requirement can be translated in two different ways: either the state uses software whose sources are public (open source software) or it acquires the intellectual property of the sources it uses. Some 80% of the software used in Geneva (firewall, servers' operating system, etc.) is open source; the rest is owned by the state, with the exception of the databases.

The Geneva law opens the code for review by the electoral commission or by any expert it designates. It also foresees access to the code by anyone having a scientific interest

THE SECURITY APPROACH

What must be protected in the context of electronic voting? Voters' ID? Votes anonymity? Votes content? None of these, or all of them. It is the community of citizens and not each single voter which must be protected against the consequences of an inaccurate ballot outcome. The right approach is therefore a holistic one and the key issue is securing data.

Three environments must be taken into account to this end: the voter's PC, the internet and the state's IT system. Instead of considering all three as separate entities to be protected per se, the Geneva team focused on the common factor to all three: the data.

The voter's PC

The voter's PC is the weakest link in the chain of custody. The risks linked to this situation are managed by sending a signed java applet to the voter's PC without installing it there. All through the voting session, the applet is stored on the state's voting server in order to insulate it from the malicious software that could lie in the PC.

This applet has several functions. As the SSL pipe is browser-driven and vulnerable to compromised PC environments, the applet creates an additional layer of encryption inside the SSL. The applet also tests the validity of the votes upon their arrival in the state's system by comparing each single one to the universe of all possible answers in a given ballot. This control is performed again on the server side. Any vote which does not fit into this referential is rejected. This prevents malicious software entering the ballot box and ensures that the ballot box's content is valid and readable.

The internet

On the internet, the data is protected by the secure channel created by the java applet encryption. This channel's encryption key is defined by true random numbers generated by a quantum generator.

The state's IT system

Any off the shelf hardware (server, router…) or software (database, firewall…) used in a complex system such as the internet voting application comes with a high level of customisation options in order to make it suitable for many different uses. Yet, this versatility represents a danger, as it is associated with far more lines of code or entry ports than would be needed for a secure voting transaction.

Securing the system means performing a severe hardening process to deactivate all irrelevant functions. A second level of hardening involves the careful management of the interactions between the various system's components. In a third stage, all requests and commands reaching the system are filtered so that only the ones compatible with a normal voting procedure are processed.

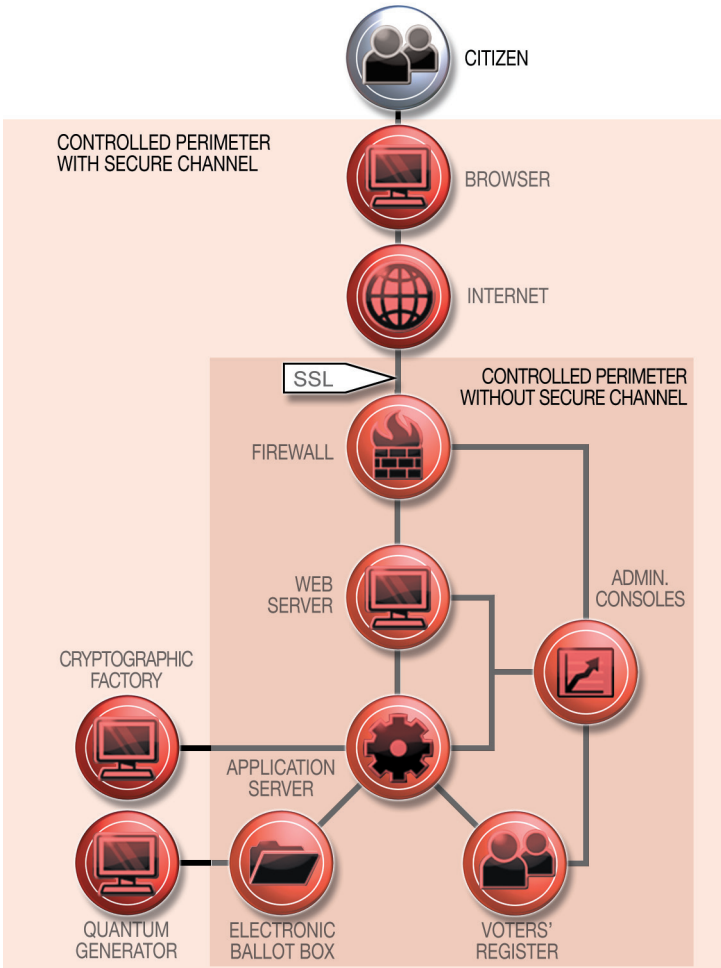
A few other measures

A few other security measures are taken on the Geneva internet voting system, such as:

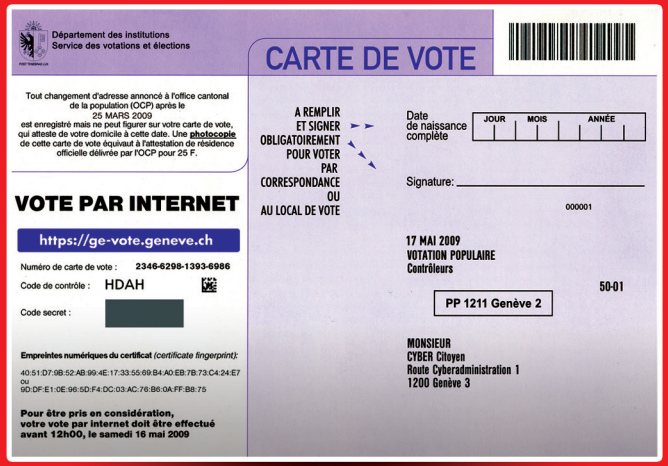
- The absence of any connection between the electronic ballot box and the voters' register.
- The anonymous nature of the voters' register. It only contains single use voting cards numbers, but no name.
- The recording of the number of cast votes by an encrypted counter which is off-limits for the database administrator. No vote can be added or subtracted from the ballot box without the electoral commission noticing.
- The ownership of the ballot box encryption keys by the electoral commission, which makes it impossible to alter the votes.
- The randomisation of the ballot counting order by application of an algorithm to the ballot box before decrypting votes.
- The screening of helpdesk calls for valuable information.

The sum of all these measures brings the Geneva paradigm close to situation of the polling station. The strength of the polling station resides in it being a fully controlled perimeter. The challenge with internet voting is to extend the state control as far as possible in order to recreate as much as possible the situation of the polling station.

This illustration shows how far this has been achieved in Geneva:



THE ID ISSUE


Département des institutions
Service des votations et élections

CARTE DE VOTE

Tout changement d'adresse annoncé à l'office cantonal de la population (OCP) après le 25 MARS 2009 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'OCP pour 25 F.

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

Date de naissance complète JOUR MOIS ANNÉE

Signature: _____

000001

VOTE PAR INTERNET

https://ge-vote.geneve.ch

Numéro de carte de vote : 2346-6298-1393-6986

Code de contrôle : HDAH

Code secret : [redacted]

Empreintes numériques du certificat *(certificate fingerprint):*

40:51:D7:9B:52:AB:99:4E:17:33:55:69:B4:A0:EB:7B:73:C4:24:E7
ou
9D:DF:E1:0E:96:5D:F4:DC:03:AC:76:B6:0A:FF:B8:75

Pour être pris en considération, votre vote par internet doit être effectué avant 12h00, le samedi 16 mai 2009

17 MAI 2009
VOTATION POPULAIRE
Contrôleurs

50-01

PP 1211 Genève 2

MONSIEUR
CYBER Citoyen
Route Cyberadministration 1
1200 Genève 3

Dealing with ID management on the internet raises a fundamental question: how do I know that 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 settle 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 cyberworld, there can be as many "time zeros" as one decides; everyone can assume as many names, genders and ages as they wish. Therefore, the central question becomes: is it acceptable to fully dematerialize the digital ID?

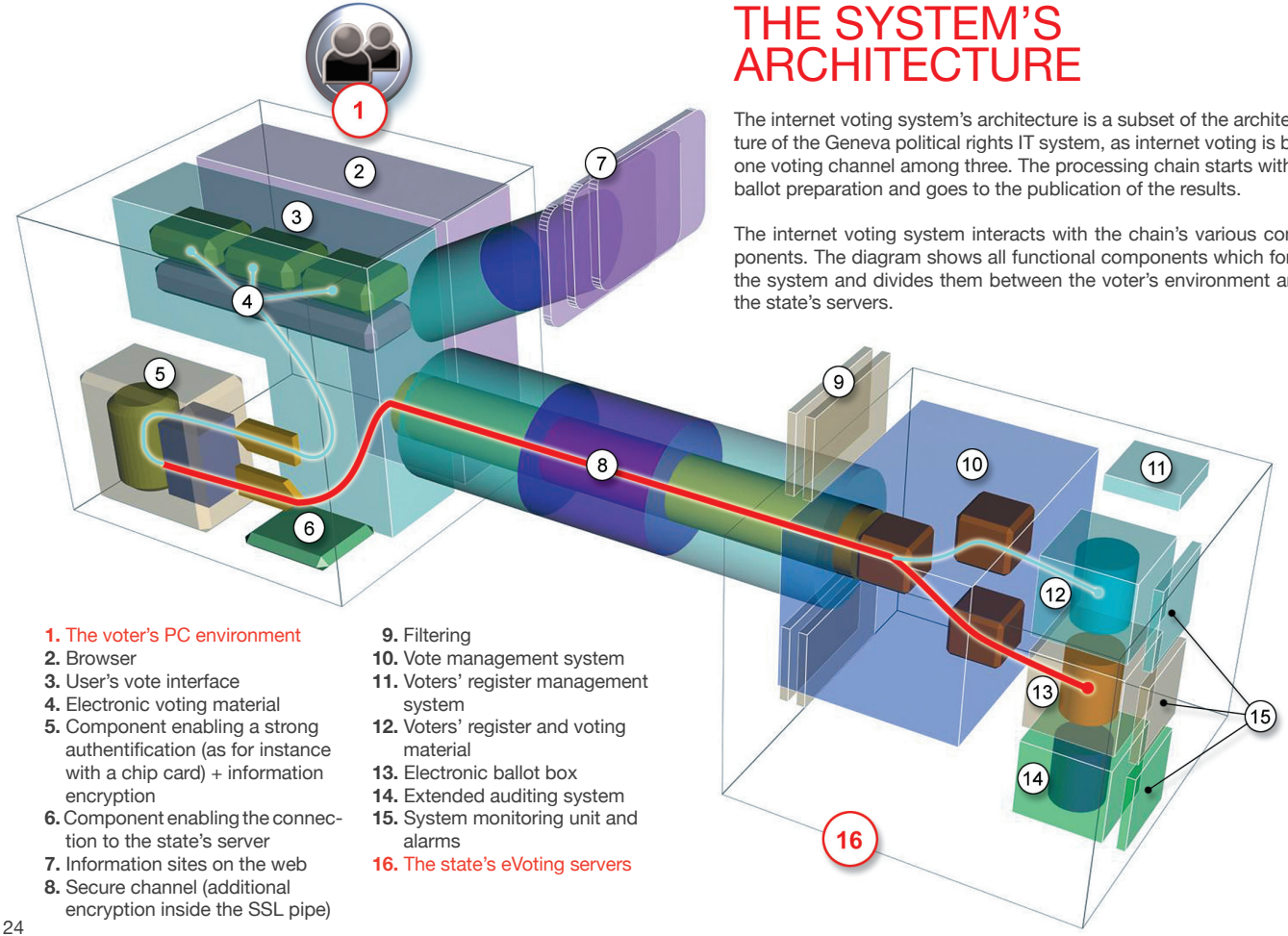
The Geneva answer is no. Digital certificate issuers do not carry out the extensive checks performed in the physical world to ascertain one's identity and too often the certificate's control is delegated to the browser, which can be compromised.

This does not mean that online authentication has to be complex. Before every ballot, Geneva voters receive by post a single use voting card, which is their numerical ID with time-limited validity. This card carries the voter's number and PIN code. To validate their votes, citizens must also give the system two shared secrets: their birth date and municipality of origin. This is a implementation of the strong online authentication rule that relies on the combination of two out of the three following items: something you know (in this case, your birth date and municipality of origin), something you have (your voting card with PIN code) and something you are (which could for instance be your fingerprint).

THE SYSTEM'S ARCHITECTURE

The internet voting system's architecture is a subset of the architecture of the Geneva political rights IT system, as internet voting is but one voting channel among three. The processing chain starts with ballot preparation and goes to the publication of the results.

The internet voting system interacts with the chain's various components. The diagram shows all functional components which form the system and divides them between the voter's environment and the state's servers.



1. The voter's PC environment
2. Browser
3. User's vote interface
4. Electronic voting material
5. Component enabling a strong authentification (as for instance with a chip card) + information encryption
6. Component enabling the connection to the state's server
7. Information sites on the web
8. Secure channel (additional encryption inside the SSL pipe)
9. Filtering
10. Vote management system
11. Voters' register management system
12. Voters' register and voting material
13. Electronic ballot box
14. Extended auditing system
15. System monitoring unit and alarms
16. The state's eVoting servers

GLOSSARY

Auditability (end-to-end): E2E auditable systems allow citizens to verify that their votes were not modified, without revealing the votes' content. These systems use codes to convey this information to the voters, in order to be receipt-free - meaning that they do not give plain access to the votes as stored in the electronic ballot box. In Geneva, the control municipality provides an E2E control over the system, but not over each single vote, as this would offer internet voting users a control that paper-based channels do not offer (see page 15).

Cast as intended: a voting system must allow voters to cast their vote as intended (see also «Family voting»).

Coherence control: a coherence control, also called integrity control, is performed on all votes arriving in the Geneva internet voting system by comparing each one to the universe of all possible answers in a given ballot. Each vote must match one of the possible answers, otherwise it is rejected. This prevents malicious software entering the ballot box (see page 15 and 18).

Coercion-free: a coercion-free voting system makes it impossible to force voters to vote in a given way.

Control code: the control code is a unique image printed on each voting card enabling voters to ensure they are casting their ballot on the Geneva official voting system, as only this system is able to link any voter's ID with the correct image.

Control municipality: the control municipality is a virtual constituency which is used in Geneva to perform a predictive test on the voting system (see page 14).

Counted as recorded: a voting system must count votes the way they were recorded, without any alteration.

Cryptography (end-to-end): E2E cryptography refers to a system where votes are encrypted in the voter's PC, but outside the normal working environment thanks to a token. As it has been decided in Geneva not to impose any equipment besides a PC and an internet connection (see page 13), vote coding takes place in the normal working environment. This is compensated by the coherence check performed on each vote upon its arrival into the state controlled voting system.

Family voting: family voting refers to the pressure voters can be exposed to when voting remotely, as with postal or internet voting. There are ways to fight it online, such as allowing citizens casting more than one vote or asking a private question during the voting process to enable the voter to tell the system in a transparent way whether his vote must be recorded or not. In Geneva, ex-post random phone checks are performed to ascertain the absence of pressure on voters (see "Random phone control" and page 9).

Predictive test: a predictive test is a test whose expected results are known in advance and compared to its effective outcome (see page 15).

Protected perimeter: the protected perimeter is a measure of the state's control on the voting process. The paper-based polling station sets the benchmark with a full state control. Geneva has probably one of the largest controlled perimeters for electronic voting (see page 21).

Quantum generator: the quantum generator uses the property of a physical object (in Geneva, the light) instead of that of numbers to generate in a truly random way a sequence of digits. Cryptographic keys generated this way are much more difficult to break than keys generated by computer algorithms (see page 18).

Random phone control: 2% of the remote voters for any ballot are called by the Geneva administration to ensure they voted freely and without any supervision or constraint (see “Family voting” and page 9).

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

Recorded as cast: a voting system must record votes the way they were cast, without any alteration.

Secure channel: the secure channel is a feature of the Geneva voting system which adds a second layer of encryption to the SSL. The encryption key for this channel is generated by quantum generator (see page 18).

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 (see page 15).

Verifiability (individual): individual verifiability refers to the possibility given to each voter to check his vote as stored in the system.

Verifiability (universal): universal verifiability refers to the possibility given to all voters to check that a ballot outcome is correct. In Geneva, this possibility is given to the electoral commission.

IMPRESSUM

See our video online by photographing this image with your smartphone.

Conception and textes:
Michel Chevallier, Geneva State Chancellery
michel.chevallier@etat.ge.ch

Layout and images:
Clerc&Ventura, Geneva (www.clercventura.com)
and Constantin Sandru (State of Geneva)

Printed by:
Imprimerie genevoise SA (Printed on recycled paper)

Visit www.ge.ch/evoting
The Geneva internet voting system is compliant
with the Council of Europe Recommendation Rec (2004)11

NOTES