Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

Political Rights Section

Redesign of Internet Voting Trials in Switzerland 2020

Instructions for the questionnaire

- This questionnaire is meant to initiate a constructive dialog among the invited experts, the Confederation, the cantons and their partners.
- Please go through all questions first and consult the material in the next section.
- Extensive answers are more than welcome. If applicable, please summarize the essence of additional material that you might quote.
- If you find a question trivial, please do not settle for a “yes” or a “no”, explain your answer. If you find a question impossible to answer, break down the question and give answers as far as possible.
- Internet voting is interdisciplinary. For example, the concept of verifiability is a vehicle for both security and its (public) perception. Therefore, experts from technical and social sciences should participate in the dialog. Unless agreed with the Federal Chancellery, we expect that you share your view on every subject to the full extent that your expertise, experience or personal reflections allow. If you really think you should not be answering a question, please contact the Federal Chancellery (FCh).
- Feel free to formulate further questions that could be raised for debate based on your statements.
- Please indicate how you wish your statements to be perceived (do you have special in-depth expertise and are you explaining a fact with a scientific foundation? Or are you rather sharing your opinion on a matter you feel deserves to be debated?).
- We would like to publish your answers at some point. Beforehand, you will get the chance to modify your answers, e.g. with respect to the case where your views might change in the course of the dialog.
- You are free to use this questionnaire for any purpose and to publish it. If you make modifications, you must highlight the fact that you did.
- You are allowed to share and publish your personal views on the dialog, its conduct and the issues discussed. The following rules apply:
  - With regard to statements made in the workshops, the Chatham House Rule[1] applies. We impose this requirement in order to allow participants to express their views freely, i.e. without adapting their statements in the possible prospect of being quoted.
  - In case the publication of the final report is yet to be expected, you are asked to inform the Federal Chancellery before publishing statements.

[1] https://en.wikipedia.org/wiki/Chatham_House_Rule

Material

Federal legislation:

[1] Ordinance on Political Rights (see articles 27*a* to 27*q*): German / French / Italian

[2] Federal Chancellery Ordinance on Electronic Voting VEleS

[3] Annex of the Federal Chancellery Ordinance on Electronic Voting VEleS

Information of the Federal Chancellery:

[4] Full information on internet voting (German, French or Italian); navigate using the menu on the left

[5] Information in English; navigate using the menu on the left

[6] Report of the Federal Council on electronic voting - Evaluation of the introduction of electronic voting (2006-2012) and principles for further development, 2013: German / French / Italian

Information of Swiss Post:

[7] Documentation and reports

[8] Explanations

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Fabrizio	**Last name**	Gilardi
Organization	Universität Zürich		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.
I am answering this question from the perspective of a political scientist, i.e. not focusing primarily on the technical aspects. When assessing the degree to which e-voting is considered "trustworthy," I would like to know to what extent e-voting is accepted and trusted (subjectively) among voters. A key determinant of the perception is likely to be the attitude of political elites, the degree of polarization among them, and the extent to which e-voting has been politicized. Best case, there is broad consensus among the elites that e-voting is a secure tool, with no party (e.g. a populist party) politicizing the issue to stoke anti-elite sentiment. In this scenario, it is highly likely that e-voting would be perceived as trustworthy by the general public. Worst case, political elites are sharply divided along strict party lines and polarization patterns in society. In this scenario, roughly half of the population would see e-voting as trustworthy, and the other half as not trustworthy. Overall, e-voting could not be considered trustworthy in this second scenario. In the Swiss case, we are kind of in-between these two extremes. There is no consensus among elites regarding e-voting, but also no clear polarization following established cleavages. Voters are receiving mixed signals, meaning that, overall, e-voting cannot be considered trustworthy. Establishing elite consensus regarding e-voting is a key step to achieve trustworthiness.	

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
I do not feel qualified to answer this question.	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
I do not feel qualified to answer this question.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment.

	With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
I cannot assess the purely technical side of this question. It strikes me, though, that the printing office could be perceived (rightly or not) as a key vulnerability of the system, in a way that (again, rightly or not) makes intuitive sense to citizens. I would expect that many citizens could be critical of the security of this step, since it is easy to imagine ways in which things could go wrong. These considerations have direct implications for the perception (an politicization) of "trustworthiness" discussed in question 1.1. Moreover, I am not sure I am understanding this correctly, but it seems that one option that is being considered is simply declaring the printing office trustworthy given that some functionalities are assigned to it. I think this step is hard to understand for the general public, and it is one aspect that so far has barely received any attention -- the focus has been almost exclusively on the Scytl software. I would be very careful here and make sure that the status of the printing office is both technically sound and can be understood by the general public, in case it is brought up in public discussions by the media or other actors.	
2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
I do not feel qualified to answer this question.	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
I do not feel qualified to answer this question.	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
I do not feel qualified to answer this question.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission

	that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
First, I do not think that users can be assumed to know if their device is trustworthy or not. The question might well discourage users from using the systems, as they are made feel insecure about the trustworthiness of their device (and of the overall system). Second, I think that the burden of verifying that a vote was transmitted securely should NOT be on voters. Some users will not bother to check and others will misinterpret the output. Moreover, the burden may discourage voters from using the service.	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
I do not feel qualified to answer this question.	

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
Regarding my comments in 2.1.3, I am not sure to what extent the printing office is taken into account in the list of potential threats. I think it is part of several items, such as 3.1.13 and 3.1.23, but I am not sure. If not, I think it would be important to add it more explicitly.	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
I do not feel qualified to answer this question.	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might

	typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
I do not feel qualified to answer this question.	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
I do not feel qualified to answer this question.	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
Yes, I think that (assuming a motivation to do so, see next point) efforts to hack e-voting will be higher than for the other channels simply because it will be easier to attempt (even though not necessarily to carry out successfully, but see next point) given the scalability of the methods and the possibility to carry them out remotely from anywhere in the world. Regarding the motivation to hack Swiss elections or -- more likely -- direct democratic votes, I do not think that there is currently an open threat, but I also think that it is essential to consider worst-case scenarios. It is not completely outlandish to think that in ten years, some actors might benefit from influencing the outcome of a direct democratic vote, and might attempt to do so. I can imagine that much could be achieved even with limited resources, because such an operation does not need to be successful (that is, change the outcome) to be disruptive and cast doubts on the legitimacy of the outcome. That would be highly problematic especially for a high-stake decision in a polarized environment and with a close outcome. It is a tail risk, but definitely possible in the long term.	

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or dis-

	played incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
I assume there are data to answer this questions from the various trials that have been conducted, but I do not know them. Regarding incentives, I would definitely try to experiment with various options in the context of the trials, to find out what works and what does not. Generally, however, I am skeptical of the view that the system should rely heavily on voters checking the return codes and reporting suspicious observations. Again, I assume there are data from previous trials, and I would be very interested in knowing how they look like. I also would like to know if there is a minimal number of voters that need to check and report the codes in order to detect fraud, and how large is that minimal number. Overall, I do not think that relying on voters for this task is a reasonable approach, because their behavior is hard to control and because the approach puts a significant burden on them, reducing user-friendliness and potentially also trust in the system.	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
My answer for 2.3.1 applies also here.	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
My answer for 2.3.1 applies also here.	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
I do not feel qualified to answer this question.	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
I think that users can influence their level of protection using those guidelines, but the key question is how many actually do, and I am skeptical. A recent study (https://www.mediachange.ch/media//pdf/publications/SummaryReport_WIP-CH_2019.pdf) showed that in Switzerland, over 20% of 30-69 years old (and over 40%	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

of 70+ years old) self-assess their internet skills as "poor to sufficient". This suggests that a significant share of voters cannot be assumed to follow best practices (or even "good enough" practices).	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
No, I do not think that vote buying or coercion are related to e-voting. The main concerns are those discussed in 2.2.5.	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
A key criterion is certainly independence from cantons, confederation, and all companies that have a commercial stake in the e-voting technology.	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
Regarding public perceptions, the answer depends on the broader political context, as discussed in 1.1. Assuming trust in e-voting is high because it is supported by a very broad consensus among both elites and the general public, it might be possible to accept some shortcomings. But realistically, and certainly in the current context, it is essential that all security requirements are implemented perfectly.	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

Yes, I think that both the organization carrying out the examination and the organization appointing the examination matter for public perceptions. I am not sure about differences across individual areas.	
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
I do not feel qualified to answer this question.	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
I do not feel qualified to answer this question.	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
Independent experts from the public could be involved with an "observer" status. Such an involvement could contribute significantly to trust in the outcome of the examination.	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
I do not feel qualified to answer this question.	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
I do not feel qualified to answer this question.	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
I think it would be great if citizens could be integrated in some way. It would be worth exploring how "citizen science" approaches could be used in this context, for example in cooperation with organizations such as the Citizen Science Center Zurich (https://www.cc-cs.uzh.ch/en.html). It seems that within that context, citizens could be involved in meaningful ways in the technical task of code verification. The potential benefits in terms of public trust could be large.	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
See 4.2.	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
See 4.2.	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
See 4.2. It is worth exploring how a citizen science initiative could be involved in the process.	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
I do not feel qualified to answer this question.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
I do not feel qualified to answer this question.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?

I do not think that the current scale of usage is relevant to assess trust issues. Arguably, the long-term goal is that as many people as possible will make use of the e-voting channel, not least due to cost considerations. Limiting the scale of usage sounds like a trial, and arguably makes sense only as a transitory measure. Moreover, scaling up usage (eventually) would likely raise new trust issues, which would need to be addressed separately. In sum, I do not think that scale is a useful angle to address trust.	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
I do not feel qualified to answer this question.	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
I do not think that publishing e-voting shares necessarily increases trust, but NOT publishing them likely decreases it, since it reduces transparency for no obvious reason and it encourages conspiracy-theory thinking.	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)
I am not sure which measures would help specifically, but in general, the more transparency the better. Of course, more transparency implies a higher likelihood that problems are uncovered. The larger, harder question is how to deal with the unavoidable problems that will emerge in a way that increases trust.	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
Comparison with other voting channels is not necessarily meaningful because voter composition is likely to vary across channels, so differences are to be expected. It might be worth exploring how methods developed to test for electoral fraud (e.g., [1] https://www.sciencedirect.com/science/article/pii/S0261379414000390?via%3Dihub and [2] https://www.cambridge.org/core/journals/political-analysis/article/election-fraud-a-latent-class-framework-for-digitbased-tests/047BDA1F6D2A82474908DABCF8DDA119), might be applied to this specific context. (I am not an expert on these specific methods.) The publication of results and methods would definitely be highly beneficial, of course assuming they are sound.	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate

- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
Most academics do not have much spare time, and participation in these contexts is something that is of little value for an academic CV. Therefore, the conditions for participation are probably a mix of intrinsic motivation and (monetary) incentives.	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
Participation in political debates is generally a sensitive issue for academics, especially in controversial areas. In general, academics are most comfortable with participation in public debates in areas in which they have directly conducted research themselves (as opposed to just having some general expertise). Therefore, something that might work could be funding research on e-voting (via the SNF or other channels), so that academics have concrete research results that speak very directly to the political debate. Willingness to engage with political debates could be a prerequisite for the research grant.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
I think the problem is not specific to e-voting, but rather a common issue in science communication. I would reach out to science communication experts here. Moreover, the citizen science approach mentioned in 4.2 could be helpful.	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
See 5.3.	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
Again, I find the citizen science approach promising because it is aimed at bringing together non-expert citizens and academics to work together on a specific research problem. It is an established format that has been used in many different contexts, and which universities are interested in expanding, so there is already a certain level	

of know-how and resources that could be mobilized to focus on e-voting. For example, a citizen-science project could focus on statistical tests to detect irregularities (see 4.12). Hackathons are also a good idea; the difference with citizen science is that in hackathons, participants are experts (even though not necessarily academics), so they do not fulfill the same function in terms of involving the general public.

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
I do not feel qualified to answer this question.	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
I do not feel qualified to answer this question.	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
I do not feel qualified to answer this question.	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
I do not feel qualified to answer this question.	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
I do not feel qualified to answer this question.	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?

I do not feel qualified to answer this question.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be out-sourced? To whom?
I do not feel qualified to answer this question.	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure compre-hensiveness and consistency in this set up?
I do not feel qualified to answer this question.	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
I do not feel qualified to answer this question.	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet vot-ing? How should the fact that internet voting involves multiple actors be taken into consideration?
I do not feel qualified to answer this question.	
7.2	What are the right events and thresholds for an activation?
I do not feel qualified to answer this question.	
7.3	Who should be involved in crisis management, with which role?
I do not feel qualified to answer this question.	
7.4	How should the communication be organised (internally and externally)?
I do not feel qualified to answer this question.	

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
I do not feel qualified to answer this question.	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
I do not feel qualified to answer this question.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
I do not feel qualified to answer this question.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
I do not feel qualified to answer this question.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
Intuitively, I would say that a voting result can be declared as valid as long as the margin of error of the investigation rules out that the outcome might change (e.g. in a referendum, that it is accepted instead of rejected).	

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Stéphane / Sergio	**Last name**	Adamiste / Alves Domingues
Organization	SCRT S.A.		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

Most important questions we need answers to to conclude that internet voting is trustworthy include:

- Is there a strong legal framework defining the way electronic voting is governed?
- Does the governance around electronic voting enable enough independence, control, transparency to provide assurance that ballots be not manipulated by any kind of malicious actor or entity?
- Does the electronic voting system support features allowing to meet its security objectives and reducing the risk of fraud to an acceptable level?
- How is it verified that the security objectives are indeed met?
- Are the information systems that support the electronic voting capabilities, the organization, processes and people involved, subject to information security controls?
- How are the aforementioned information security controls defined, designed and implemented?
- What are the mechanisms in place to assess whether those controls are adequately implemented and effectively reduce the risks of fraud / information security incident?
- Do the applied information security assessments methodologies provide a reliable image of the electronic voting system's posture in terms of information security? Do the security assessments performed provide accurate results?
- Are information security assessment results made available to the public?

Ideally, we would expect the answers to emanate from official independent sources with the necessary competencies and means to provide accurate answers. A full description of the electronic system, both from a technical and organizational points of view, including legal framework, governance principles, procedures, system specifications, security concept, risk assessment, applied security controls during the build and run phases should be made available to the public.

We would also expect regular audits of the electronic voting system to be performed by qualified personnel, using methodologies able to evaluate the residual risks of fraud and information security incident with a high degree of accuracy. Audit conclusions should be shared with the public.

In Switzerland, several key elements exist. However, the public is not able to judge whether those key-elements conform to best practices. We are personally unable to raise potential caveats regarding the legal framework around the electronic voting, by lack of knowledge on the topic. Contradictory expert's opinions would be welcome to help the public better apprehend the stakes and requirements of a safe electronic voting system. In this regard, we value the popularization effort made to explain some of the security mechanisms involved in the Swiss electronic voting through educational videos.

As information security specialists, we lack information to form an opinion about the electronic voting trustworthiness. The opening of the source code of the solution and the bug bounty program conducted by SwissPost in 2019 provided some transparency on the effective robustness of the application, but the assessment methodologies and the scopes applied allowed to evaluate a certain number of threats only. The organizational aspects were not considered for instance. Comprehensive threat trees would be appreciable to map identified vulnerabilities to threats.

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEIeS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEIeS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEIeS in conjecture

with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
In our opinion, while not completely impossible, this scenario seems unlikely as cryptographic standards are generally verified and reviewed by a large community of experts before being adopted. But even considering that these cryptographic building-blocks could be flawed in an exploitable manner, its exploitation (at least at scale) should most probably also require some form of compromises of the e-voting platform itself. **What seems, on the other hand, much more likely is a flawed implementation of a cryptographic standard which would introduce implementation-related vulnerabilities.** **This is however only an "opinion" as, despite being information security professionals, we are not cryptographers and do not pretend to have any form of expert opinion on matters related the design and standardization of cryptographic protocols.**	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
We consider that this question is outside of our domain of expertise.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
From a trust perspective having a formal verification – or even better: a generation - of the return codes by an "official body" would, in our opinion, be interesting. One critic that could be opposed to the Swiss Post system from a simplistic point of view (and subject to our understanding) is that Swiss Post thus have control over the verification codes that are sent as well as on the system responsible for displaying those verification codes to the voters. They could thus abuse this to alter the votes unnoticeably. While this hypothesis is simplistic and probably not even true, it may correspond to the perception of some voters lacking an understanding of the system's internals.	
2.1.4	**Independence**

	The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
In our opinion, the best value in terms of security would come with a proper implementation and review of the software. In other words, it is best to rely on a single properly coded and thoroughly reviewed implementation of an algorithm (e.g. a cryptographic protocol) than on different implementations just for the sake of difference. Of course, having 4 different well-coded and reviewed implementations would be appreciable (but also more complex to achieve). If not, we would give priority to proper implementation and review over diversity. As a comparison, it is commonly considered as a best practice to use a well-known and reviewed software library for cryptographic use than to try implementing a custom (yet different) one.	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
As in 2.1.4, in our opinion, priority should go to proper implementation and review in order to ensure that the implementation matches the designed algorithm and does not introduce vulnerabilities.	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
In our opinion the major difference between operating systems and software-layer is that OS are completely out of control of the e-voting system vendors/operators (and much more complex from a software perspective). Consequently, we cannot extrapolate our opinion in 2.1.4 and 2.1.5 by saying that "it is better to ensure that OS is properly coded and secure". **Based on that, we see diversity in operating systems (as well as hardware) as a beneficial measure.** **As Swiss Post's solution is based on Java, the value of having different Java Virtual Machines could also be considered.**	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission

	that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
We are unsure about the specific details and implications of the proposed scheme. However, unless dedicated devices are provided to the voters (which does not, in our understanding, seem to be the proposal here) assuming a trusted device on voter's side seems dangerous and unfit for non tech-savvy people. In our opinion, the mechanism based on return codes is user-friendly and simple to understand and thus quite elegant.	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
The Microsoft Security Development Lifecycle (SDL) provides information security and data privacy good practices with regards to software development and implementation. **In order to ensure that the correct software is running, a hash of its code should be produced and verification should occur systematically. Those two processes should require the involvement of several independent parties, in order to avoid the risks of fraud and collusion.**	

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
Yes. This lists only considers human intentional threats (i.e. attacker's actions). It neglects accidental behaviour such as a bad manipulation or configuration errors by an administrator for instance. It does not consider breakdowns/malfunctions, vandalism, environmental hazards which could affect the availability of the electronic voting system.	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
ISO27002:2013 §14, §15, §17, §18 are not covered.	

Some critical controls from §9 and §12 such as Network Access Control (NAC), authentication, privileged access management, vulnerability management are not considered. Hardening of components is not required either. **§6: segregation of duties is also paramount in our view and is not mentioned.** **Some controls from §11 (supporting facilities, clear desk, clear screen policies, secure disposal of equipment, etc.) are not considered.** **Moreover, the annex refers to the 2005 version of ISO27001, which is obsolete since 2013.**	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
As mentioned in the questionnaire, security in acquisition, development and maintenance has not been addressed in a satisfactory way in the Swiss case. **Implementing security controls from known frameworks such as ISO27002:2013 would lead to more effectiveness if all controls likely to mitigate applicable threats were considered.**	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
The VEleS theoretical requirements for integrity and secrecy exceed other domains. However, the assurance process has already proven to be faulty (the assurance process answers the question: are the theoretical requirements implemented correctly and are they efficient?). So we would not state that the cast votes are far better protected than other critical data.	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
This question cannot be answered easily without specifying the exact attack scenario (what security property (ies) is (are) broken, what is the scale of votes impacted). **It is, in our view, far easier to compromise voting by postal mail at a small scale (e.g. prevent a small number of votes to be taken into consideration or compromise voting secrecy by breaking into a mailbox).**	

Likely powerful threat agents in our opinion include Swiss political parties, Swiss and international lobbies depending on the purpose of the vote, foreign intelligence services. We imagine that the easiest ways to manipulate or read votes include malware on the voter's workstation, alteration of the electronic voting software source code, and alteration of the ballot results between the time they are calculated by the voting system and the time they are reported by the assessors

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
Yes it seems reasonable. The voting material should emphasise this point clearly. A warning message could also be sent during the voting process to encourage voters to check the code. A more constraining way could be to ask voters to input the result of the verification done	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
Same as 2.3.1	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
Same as 2.3.1	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
We do not feel competent to answer this question	

2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
We think that the MELANI guidelines or anything similar form a sufficient basis for voters to protect their individual workstation.	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
Vote buying or coercion are not linked to the voting channel used, therefore there is no reason to believe that internet voting would increase these phenomena in our opinion.	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
Technical competency and audit experience should determine what individuals and organizations are mandated with an examination. **The scopes of examination should include, in our opinion: certification of the electronic voting software against common criteria (are the features implemented?), electronic voting software security assurance (i.e. does the code contains security flaws/bugs?), implementation status of ISO27002 controls likely to mitigate threats at the software vendor, software provider and cantons level (i.e. is the environment in which the electronic voting system developed and operated subject to vulnerabilities?)**	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.

We believe it may be reasonable to postpone fixing a vulnerability if the associated threat is considered as a low risk.

Moreover, individual flaws do not necessarily imply that a given threat scenario can be exploited. Successful exploitation may require specific conditions, or additional vulnerabilities. Depending on the case, this argument could be invoked to postpone the fix implementation.

Putting in place a temporary workaround (e.g. a WAF rule for instance) may also be a valid reason.

However, we would fix immediately all missing items from the common criteria, as the security objectives are part of the core specifications.

In such case, a clear communication towards the citizens should be drawn up.

3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

Potential conflicts of interest should be avoided (e.g. if the vendor or provider of the electronic voting software mandates the software certification audit, if the cantons mandate the audit of their security practices during operations, etc.). In those cases, the credibility of the outcome may be affected. Ideally, an independent authority should be in charge of mandating examinations.

3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?

Existing standards such as ISO27002:2013 or NIST publications include all necessary best practices. However, those standards should be applied entirely to respect the holistic nature of the information security discipline, and their practical implementation should be assessed at all lifecycle stages (development, implementation, operation)

3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?

An acceptable practice would be to determine a frequency for recurrent audits as part of an ISMS regular process.

Changes should trigger additional examinations according to predefined criteria.

3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?

Independent experts could be invited to contribute to the definition of the scope and methodology for examinations.

Independent experts could be invited to further participate to some kinds of examinations (i.e. public code reviews / bug bounty programs).

Examination findings could be disclosed to a panel of experts for challenge prior to their public disclosure.

3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
A procedure should be defined, agreed upon and applied to handle differing opinions. Maybe the precautionary principle should apply and the authorization be not granted, maybe a third opinion should be sought, etc. Possibilities should be explored and a procedure established in advance, so that proof can be made that a defined approach has been followed to handle differing opinions.	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
A significant part of criticism against 2019's source code program came from the fact that the source code was indeed made accessible but only through an explicit registration and the acceptance of strict conditions. This approach could be perceived as in opposition with the concept of "publication" and introduced a duality which was used to fuel controversy about the program. As an example of this, the publication of a copy of the source code (which was indeed against the rules imposed by Swiss Post but did not cause actual harm as the code could be accessed by anyone) was presented as a "leak".	

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

As a "transparency" measure, the publication of the source code would most certainly benefit from a transparent publication approach in which it would be accessible to all without any registration or conditions perceived as restrictive. The intellectual property of Swiss Post can still be ensured by limiting the licensing to testing purposes (and explicitly forbid-ding any unauthorized production or commercial usage). This approach may lead to better perception of the program, which may, in turn, help as an incentive for community's participation.	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
In order to allow for meaningful scrutiny, the published material should include all necessary elements to allow the setup of a "mock" system. This includes not only the source code of all the system components but also comprehensive documentation for these elements to be built end deployed in a production-like setup by the public and specialized community. Any partial publication or the lack of documentation allowing the system to be fully setup may be perceived as a voluntary retention of information or some form of preventing actual thorough scrutiny of the system. **As an exception to that, details about any peripheral security systems or additional measures deployed in production environments may however be excluded from this publication as they are not part of the e-voting system itself (which must be self-sufficient in terms of security) and are only used to increase security and apply "defense-in-depth" principle. These systems should however not be key-elements for the security of the e-voting solution.**	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
In order for the publication to achieve the "transparency" objectives, the published code and documentation should correspond to the "production-ready" version.	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
Currently, VEleS only states that "the documentation on the system and its operation must explain the relevance of the individual components of the source code for the security of electronic voting. The documentation must be published along with the source code". It does however not impose any requirements documentation related to compilation and setup of the system. **As stated in the response to question 4.2, we believe that the publication should also include all necessary documentation for building (compiling) the code and setting up a full-fledged test environment, identical to production setup. Because of this, we indeed believe that it is appropriate to go beyond the current requirements.**	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
Our understanding here is that the term "public reactions" refers to potential issues (or concerns) that may be identified in the source code of the e-voting application by the public and/or specialized community. **These should, in our opinion, be submitted to a panel containing at least representatives of the following entities:**	

- **The software vendor/developer**
- **The Federal Chancellery**
- **The Cantons**
- **One or several independent technical experts**

This committee should have the capability to understand the details of the reported issues and reactions (including the underlying technical details if those are relevant) and then assess the implications of these findings in an unbiased and transparent manner.

4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?

In our opinion, for the sake of transparency, it is imperative that all the security issues that have been identified are published. The best (and certainly simplest) solution is to publish the details when the issue has already been fixed. However, this may introduce long delays in publication which may be perceived as information retention. A commonly accepted delay for what is considered "responsible disclosure" in the industry typically extends to a few (e.g. 3) months.

On the other hand, it is our understanding that no voting should occur using a version of the software which would be affected by a known vulnerability (even if this vulnerability has ne yet been made public). Because of that, as soon as a vulnerability is reported the software should not be used until a new (corrected) version is deployed. If this is indeed true, there seems to be no specific risk at publishing a discovered vulnerability as soon as the affected software is no longer in use. In that case, this publication should however be accompanied with an expected date of fix.

These publications should be primarily done by the software vendor. However, in order to build trust, they should be "endorsed" and commented by the Federal Chancellery and/or the Cantons which in turn could confirm that this vulnerable version is no longer in use.

4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?

As organizers of the PIT, we believe that yes, both security and public trust can be built or improved from some form of public intrusion test or bug bounty however some significant changes to the format and modalities should be considered:

1. No distinction should be made between "source code program" and "PIT". This distinction (while clear for all the organizing stakeholders) seems to have been misunderstood by the public and the researchers and contributed to fuel controversy (e.g. difficult to explain why serious conceptual flaws reported on the source code were not publicly rewarded by significant bounties).

2. A larger timeframe should be provided or – ideally – a continuous bug bounty program should be established.

3. Whilst some "non-specific" risks like Social Engineering, DoS, … should be acknowledged and mitigated they may probably be excluded in some way from the scope of the program. However, this scope should be revised to include at least not only "theoretical vulnerabilities" found on the source code (see point 1. above) but also any issues on "peripheral systems" (e.g. DNS) if they are realistic in nature and if it can be demonstrated that an exploitation of these issues could lead to a compromise of the e-voting platform. Additionally, back-end systems should also be fully "in-

scope" and not only as the result of a previous exploitation on public-facing systems. In other words, it should be possible to test the security of components which are only accessible to operators of the system (e.g. Cantons) Finally, significant bounties should be payed for the reporting of serious flaws in order to incentivize people to participate.

4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?

The enforcement of low-scale use of e-voting may increase security (by limiting the potential consequences of a successful attack) but is, in our opinion, not a proper way of promoting trust as (on the contrary) it conveys the impression that e-voting is untrusted and thus limited to marginal use.

This approach may however be defended in some contexts. As an example, it can be argued that e-voting is a good solution for some groups of citizens (as an example just for the sake of illustration: citizens living outside of Switzerland) and that it may, in these cases, improve the security of the existing voting mechanisms while having a limited impact in case of fraud or attack. However, it is assumed then that e-voting is not fully trusted and is used as the "least worst-case" option for such scenarios.

4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?

Defining how this process should be carried falls out of our scope of expertise. However, in our opinion, credibility and trust come with transparence. This process should thus be carried by an unbiased party in the most transparent manner. Ideally, relevant data and details should be published to make the tallying and verification independently verifiable by the public (at least those having the technical knowledge to do so). While we don't know if such a level of transparence is technically possible, it could however act as a strong argument in favor of e-voting compared to traditional tallying where the public has no "technical means" of verifying the results that are announced.

4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?

In our opinion, trust benefits from transparency. Consequently, we believe that this publication could be beneficial and do not see any downsides to it.

4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

As discussed in §4.9, we believe that transparency regarding the tallying process as well as providing some way of independently verifying those proofs could promote trust. In addition to that, clear information campaigns should be carried in order to popularize and demystify the details about e-voting internals. Whilst the technical details may be inaccessible for a vast majority of the citizens, the general concepts should however be presented to and understood by all (not only to a specialized public).

While this remark may fall outside of the scope of this question (or even the scope of this questionnaire), we also believe that the level of trust towards an e-voting solution may be increased if this solution is publicly owned and operated and not provided by a private company.	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
Statistics about the usage adoption of each channel, the percentage of invalid votes per channel (mostly for traditional channels as invalid votes should be impossible with e-voting).	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
Involvement from experts as well as the general public may be driven by several motives and depend on the specifics of what is expected. Participation in public scrutiny may be motivated by "simple" interest, willingness to contribute to the community's effort or pure technical challenge. However, as it takes time for the people involved (be them experts on the subject or not) which may have to be spent at the expense of other activities significant involvement may require a real incentive be it monetary of equally appealing. As an example, for a "public scrutiny" activities where the general public's involvement would be desired (e.g. the PIT) a "bug bounty" approach may be well suited. For more dedicated tasks (involving a smaller group of persons, like obtaining consulting from technical experts) it seems necessary to identify (nationally or internationally) the appropriate industry or academy experts and to establish a clear project with a properly defined (business or academic) relation with these people.	

5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
In our opinion, representatives from science are most likely to participate in the political debate if they feel: **1. Concerned by the matter;** **2. That their opinion is relevant and useful for the debate;** **3. That they actually can make a difference (their remarks are taken into account);** **The stage at which these people will be brought into the debate may also shape the form of their participation. Early inclusion in the debate (and thus perception that their input can make a difference) may translate to a greater involvement.**	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
As discussed in 4.11 we believe that clear information campaigns should be carried in order to popularize and demystify the details about e-voting internals. This could include simplified explanations of verifiability process as well as tools to help understand the concepts. A playful approach could – for instance – be a web-based simulation game allowing to "play" with a (very simplified) version the e-voting system and to see the "internals" at all stages of the process.	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
Same as 5.3	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
In order to get involvement from the general public as well as from a broader panel of science representatives it could be interesting to take the debate to more popular channels (e.g. mainstream media and popular Swiss TV debates, …) Indeed, whilst the topic is far from new and has been at a quite advanced stage of testing in Switzerland, it seems to be discussed mostly in specialist circles with only the biggest events (e.g. PIT) and controversies (e.g. discovery of critical issues in source code) reaching the mainstream media and general public.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
The continuous risk assessment process could be supported by traditional ISMS, implemented by the various stakeholders according to their own scope. The methodology should be as objective as possible in order to provide tangible, actionable output. **We would suggest having an independent authority providing the risk analyses in order to avoid conflicts of interests.** **The first step would be to agree on the risk assessment scopes, methodologies, frequencies and the associated responsibilities. Additional analyses could be performed as part of a change management process.**	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
Benefits include: - **Increased transparency, less suspicion from the public** - **Popularizing a risk-based approach, which is the only possibility to handle information security** **Downsides include:** - **Revealing current weaknesses, which may be leveraged by hackers** - **Controversy, as different experts may have different opinions regarding the criticality of risks and how to respond to them**	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
Supply chain risks could be handled by implementing the controls defined in ISO27002:2013 at §15.	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
We suggest considering a risk-based approach (highest risks handled first). Concerning the implementation of countermeasures, we suggest considering the following criteria for prioritization: Implementation effort and the risk reduction factor of controls. This allows differentiating quick wins (low effort / high risk reduction) from long-term initiatives (high effort / high risk reduction) from low hanging fruits (low effort, low risk reduction) and from nice to have's (high effort, low risk reduction).	

6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?

We would recommend an approach that follows the ISO27005 recommendations, tailored in order to avoid as much as possible:

- **Subjectivity (e.g. using a scale that considers the frequency of an event occurring to estimate the likelihood factor)**
- **Lengthy calculations for estimating risks**
- **Too high a granularity level in the listing of risks to keep the process lean**

we would consider a more extensive list of threats including non-human adverse events and accidental behaviours.

we have personally used the OCTAVE Allegro methodology for over a decade. We find it clear (emphasis is put on describing the criticality of information types and their associated requirements in C, I, A), pragmatic (very much compatible with threat modelling techniques, including identification of likely threat agents) and requiring a moderate effort.

More than the methodology by itself, what matters is to have a comprehensive approach and to carry-out the necessary effort to implement controls.

6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?

Independent experts could be involved to optimise the risk assessment methodology (including the definition of a comprehensive list of threats and associated mitigating controls, a risk scale, etc.).

If the Confederation or the cantons lack expertise to perform the risk assessments, one can imagine that experts be mandated to assist.

We do not see what added value could be brought by science in the risk assessment process. Existing risk management methodologies are mature and efficient. The problem does not lay in the identification or assessment of risks, but in the adequate definition of the scope, and the correct identification and effective implementation of adequate controls.

6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?

When performing a risk assessment, it is critical to analyse the responsibilities of the various stakeholders in the mitigation controls implementation. In the present case, the Swiss Post provides an e-voting commercial solution procured from a software vendor to cantons, which are accountable for the safe operation of the software.

The vendor should be made accountable for providing a software that meets the security objectives defined for an electronic voting solution (i.e. implementation of all security objectives, secure implementation of the security objectives). It should also ensure, among others, that the code it delivers has not been altered by a malicious internal or external actor. The vendor should commit to those requirements

towards its client (the Confederation) by applying strict Security Development Lifecycle principles in particular. **Given the criticality of the solution, the Post should exercise its right to audit in order to assess whether the security objectives are met and to which extent the development of the solution is performed in secure conditions.** **The cantons are in charge of the operation of the electronic voting solution. If the solution is operated in their respective premises, they should be in charge of the implementation of relevant technical and organisational controls at the physical, network, operating system, middleware layers, and also mitigate the risks induced by human actors likely to interact during the operation phase of the solution.** **The Confederation could issue a core security concept that inventories threats, proposes mitigation controls in a comprehensive manner and defines the responsibilities for implementation. All stakeholders (vendor, provider, operators) could be involved in this initiative in order to reach a consensus.** **Outsourcing of the elaboration of the security concept to independent experts could be foreseen if a lack of internal competences is observed, and to avoid potential conflicts of interests.**	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
As suggested above, we would rather have one working group (but composed of all stakeholders' representatives) performing a comprehensive security concept, including the build and the run phases of the target of evaluation, in order to ensure that the approach is consistent and does miss critical elements. A security concept would detail applicable threats, corresponding mitigating controls, implementation details and responsibilities for implementation. **The practical risk assessment should focus on the residual risk, by assessing whether the applicable controls listed in the concept are implemented and are efficient. In our opinion, independent experts should be mandated to assess the residual risks in order to ensure transparency.**	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
We believe Octave Allegro is recognized as a straightforward, pragmatic and popular methodology for IT risk management and it could be used in the context of the electronic voting. we repeat that the choice of the methodology itself is not critical in the process of securing a system. What matters is the adequate definition of the scope, the comprehensiveness of the analysis and the correct implementation of controls. **The strengths of the methodology, in our view, are its clarity (the critical assets description provides a very clear picture of the security requirements for each of the assets), and the fact that it does not consider the likelihood factor, which is subjective and thus subject to controversy and approximations. For the sake of credibility, it is important to base risk estimation about rationales and tangible elements.**	

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

The weakness of all current risk assessment methodologies, including Octave Allegro, is the absence of link between threats and controls. The definition of applicable controls is left to the appreciation of individuals and the process does not provide assurance about the comprehensive nature of the proposed lists of controls.

To overcome this issue, we use a catalogue of generic threats that we have mapped with corresponding mitigating ISO27002 controls. Thus, we have the assurance that we do not miss any control when working on a risk strategy mitigation. Applying this method would help identifying threats and applicable controls pertaining to the electronic voting system in a comprehensive manner.

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
Incident/crisis management must be a clearly defined process beforehand with all relevant stakeholders clearly defined. As multiple actors are involved, a "crisis management" committee should be defined and should contain representatives of all these actors. This committee should be responsible for handling the incident and taking appropriate decisions. Members should then be capable of involving the required people in their respective organizations upon need (e.g. the vendor operating the platform must be represented in the committee and this representative should then be able to engage the required resources in its team if a technical investigation is needed). **It seems also important to have a list of potential external partners in case of need. Such partners would include official bodies like GovCERT or MELANI but also potentially private companies capable of assisting in the crisis management.**	
7.2	What are the right events and thresholds for an activation?
Incident "types" and categories as well as corresponding procedures and "playbooks" must be defined beforehand. This includes a reflection on which incidents are considered as "benign" and can be ignored or handles automatically (e.g. banning an IP address which has triggered automatic attack detection mechanisms) and those that must – in any case – be discussed and handled by the crisis management committee. **Defining this exact threshold is a task that must be done by commonly with all parties involved however a reasonable assumption would be to consider that any "incident" which is suspected to have an impact on the voting results MUST be investigated.**	
7.3	Who should be involved in crisis management, with which role?

At least the following parties should be represented in the incident management committee:

- **Federal Chancellery**
- **Canton(s)**
- **E-voting solution vendor**
- **Hosting/operation provider (if different from vendor)**

In addition to that, an independent technical actor should also be involved.

The vendor/operator should be responsible for any technical investigation related to the incident. The independent technical actor is responsible for validating or challenging the results of this investigation (and thus prevent any conflict of interests). Cantons and Federal Chancellery should ultimately be in charge of taking any decisions having a potential impact on the voting process and results. They should also take care of the communication with the public (which must come from an official body).

7.4	How should the communication be organised (internally and externally)?

Communication channels between the members of the committee should be clearly identified beforehand. These should be used for frequent updates on the situation and to ensure that all members have the same level of information.

External communication should be handled by the Canton(s) with support of Federal Chancellery. In case of an incident, the public should be quickly informed at minima of the occurrence of the incident and the fact that an investigation is ongoing (in order to prevent misinformation from spreading and loss of trust).

7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?

See 7.1. GovCERT and MELANI should be in the list of stakeholders as well as potentially a few identified private companies capable of providing expertise and/or manpower. For this last category, it could be interesting to assess the possibility of relying on existing organisms like Swiss Cyber Experts (SCE).

7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?

The process of investigating an incident may heavily depend on the incident itself. In a general manner, this process could be based on well-known and recognized frameworks, e.g. the one promoted by SANS Institute and defining the following steps:

- **Preparation**
- **Identification**
- **Containment**
- **Eradication**
- **Recovery**
- **Lessons Learned**

As discussed in 7.2, possible incidents as well as response playbooks and investigative measures should be – as much as possible – defined beforehand and be ready before the incident happens.

7.7	What are the requirements and stakeholders for digital forensics and incident response?

As discussed in 7.3, technical capabilities for digital forensics and incident response should be provided by the vendor/operator of the platform (as well as the hosting provider if different). However, it important that an independent third party is involved in order to

prevent any conflict of interest (or mistrust emanating from a perception of possible conflict of interests). **In addition to that, it may be required to establish partnerships with private companies that would be capable of assisting in the investigations if needed. The companies should however be previously trained on the solution.**	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
From a technical perspective and given that sufficient data sources (logs, etc…) are available it is reasonable to consider that investigation is possible in an effective way. However, attribution of an attack as well as prosecution of the authors may be very complex and subject to several other factors (e.g. international cooperation and laws).	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
This question is very complex. However in our opinion, as a generic rule if the investigation indicates that the voting results have or could have been tampered in any form (which includes the impossibility to clearly prove that they haven't) the voting results should not be considered as valid.	

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	David Srdjan	**Last name**	Basin Capkun
Organization	Contego Laboratories, GmbH		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

Relevant factors (things you need to know to trust system)

Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny)

Which are the most important answers you need in order to conclude that internet voting is trustworthy?

Here we give answers for both questions:

1. What are the main components, who controls them, who built these components (e.g., Scytl, Post, BK …), and how independent, capable, and ethical are the entities who built and control these components? E.g., who is running the printing office, which is assumed trusted, who developed the software? Past track record for successful e-voting or projects of similar complexity and criticality?
2. What are the trust assumptions and are they reasonable? That is who and which components and entities (persons) does one need to trust for the system to be secure in terms of confidentiality, integrity, etc.?
3. What is the attacker model and is it reasonable? I.e., does/will it reflect realistic attacker capabilities today and in the future? For example, does the attacker possess a quantum computer?
4. If the trust assumptions and the attacker model are reasonable, how robust is the system to the compromise / failures of different components? E.g., are there single points of failure? This is relevant when assumptions fail to hold.
5. Does the system provide out-of-band mechanisms to achieve / verify security properties (e.g., verification if the votes are recorded, counted correctly etc)? E.g., to what extent does the system achieve software independence?
6. How do the citizens vote and verify the results of the election? How much control / insight do they have over the tallying process?
7. What quality assurance activities have been taken that ensure the security and functional correctness of the system? This includes activities taken by developers and evaluators. Here the Common Criteria provides a catalog of such activities, e.g., specification and design, security policy modeling, verification, systematic testing, configuration management, delivery and operation, life cycle support and vulnerability assessment. Moreover, what are the results of these activities and how are these results themselves evaluated? How are issues uncovered resolved?
8. Has a comprehensive and holistic security and risk analysis been carried out? In other words, the individual activities in #7 must be carried out in a rigorous comprehensive way. For example, the design must be precisely defined. The design must be rigorously shown (i.e., proven) to meet its functional and security requirements with respect to the model of the adversary and trust assumptions The implementation must be shown to conform to the design. The analysis must establish that the system must be appropriately built, distributed, and configured in a way that ensures its correctness and integrity and, moreover, that the system cannot be modified after installation. Etc.
9. Is the system complex or simple? Does its complexity make it hard for it to be properly analyzed?
10. Does the system rely on well researched, understood and widely deployed technologies? E.g., does it rely on well established Zero-Knowledge proofs or new, not yet fully tested constructs and trust assumptions?

How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)?

For Questions 1-2 above, the source could be the Bundeskanzelei (BK). Note that for Question 2 the answer could be more comprehensive though than it currently is, e.g., the example of quantum computers. For Questions 3-10, the answers would be provided by security experts based on the design, implementation, and related artifacts. Answering question 8 of course requires input too from developers, those responsible for deployment, etc.

Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting?

Here we focus on specific observations we had from previous analyses:

- The system is cryptographically complex which makes its analysis difficult and the implementation risky.
- The system may fail to instill public confidence due to its complexity.
- The system doesn't provide post quantum resilience.
- The voter interface allows manipulation, e.g., the adversary could mislead users on what checks they should make.
- The design documents for the Post/Scytl system were imprecise and incomplete. The documents failed to describe the complete design of the Swiss implementation. Future documents should explicitly describe all options (e.g., extended authentication, receipts, etc.) that will be used in the final system. Also, all control flow should be made explicit in the design documents, including how errors and exceptional cases are handled.
- The relationship between the protocol models verified and the design documents were not direct and it is difficult to relate the two. The relationship between these two artifacts should be explicit and transparent. For example, keys, data, procedures, and protocols phases and steps should all be identically named across the different artifacts. When models omit or modify details from the design, this should also be stated explicitly and justified.
- The protocols verified abstracted away details that could (and did) lead to errors, such as parameters to functions. Where these are missing, they must be checked carefully in the implementation by experts in cryptography. The models previously given should be extended to formalize the relationship between different keys. Moreover, missing control flow details, which are present in the design, should have been added. In cases where such details are inadequately explained in the design documentation, then the design documents must also be extended.
- The relationship between Post/Scytl's design and the actual implementation was indirect and not checked by the auditors with sufficient rigor. Clearly design verification, while necessary, is not sufficient given a buggy implementation.
- The Zero Knowledge (ZK) mechanisms that are used are complex and are not widely used in many systems. They are difficult to analyze and implement, although they do provide additional privacy guarantees. Even so, the main security goal (integrity of the votes and tallying) can be achieved with more standard, well understood and easier to deploy techniques. To illustrate this point we note that it took many years for the community to correctly design and implement TLS, which went through numerous revisions, and it is cryptographically and in terms of security goals much simpler than electronic voting. Separating integrity protection from privacy might have some minor impact on efficiency but would result in important security benefits. The use of Trusted Computing technology, like Trusted Execution Environments could be an alternative to ZK and might simplify the design.

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented

with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effective-ness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

The answer to this question depends in part on the building-blocks used and their complexity.

In the case of the Post/Scytl system, the Zero Knowledge (ZK) mechanisms that are used are complex and are not widely used in many systems. They are also difficult to analyze and implement, use various hardness assumptions, and therefore there is a risk of their compromise. If the crypto mechanisms that are used are those more commonly used (signatures, encryption, etc) then this risk would be lower.

But even the use of simple primitives is not enough: the use of correct building blocks themselves is no guarantee of a correct system. We know from experience building substantially simpler protocols for tasks like authenticated key exchange that most ways of building protocols from basic cryptographic functionality (encryption, hashes, MACs, etc.) in seemingly reasonable ways will fail to achieve desired security objectives. The analysis is particularly subtle in the presence of powerful adversaries like those considered by the VEleS that can completely corrupt different components.

The risk that attacks go undetected depends ultimately on how the building blocks are used in the overall design. For example, incorrectly constructed zero knowledge proofs would subvert a system that is supposed to offer verifiability guarantees (but actually does not).

2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?

From the question it is unclear if “the protocol” is an arbitrary one or a specific one such as that of Post/Scytl.

There are different kinds of flaws that could result in attacks. Proofs are with respect to models of (i) the protocol, (ii) the attacker, and (iii) a specification of the desired properties. If any of these are inaccurate, then the wrong thing is proven and even when the proof itself is mathematically correct there are no guarantees with respect to the actual protocol, attacker, and desired properties. (Hence the relevance of the previous comments that past models were lacking precision.)

If a proof is done by hand, then it may be flawed as humans err, and the more complex (i)-(iii) are, the more likely errors are. Complex models lead to complex proofs! Flaws can also arise because one works with abstractions of cryptographic primitives and the actual primitive can be attacked in different ways (e.g., parameters are not modeled and inappropriate parameters are used in practice, there are side channel attacks, etc.) that are not reflected in what is proved.

If proofs are sufficiently rigorous, ideally machine checked using the state-of-the-art, and the model is carefully made (independent validation would help here), and the cryptographic primitives can be assumed to be secure and well implemented, then the likelihood of the protocol security analysis being flawed is low. Note that provisos just stated may appear prohibitive and one may wonder what the gain is with formal models and verification given these provisos. The gain is substantial: one can have rigorous mathematical guarantees together with a precise understanding of the assumptions upon which these guarantees are based. Of course, these assumptions must then themselves be subjected to analysis as part of a certification process.

2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office).

	How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?

We are glad this question is raised as we see it as a critical one.

According to the abstract model of VEIeS, the print office is trustworthy. In both the symbolic and computational models previously made of the Post/Scytl system, the print office is used not only to *print* ballots, but also to *carry out computations*. These computations include parts of the Secure Data Manager (the *offline SDM*), which are used, for example, to generate voters' secret data. There is a clear security risk here since a compromised offline SDM would allow the adversary to covertly modify votes and break vote privacy. Here are two examples to illustrate this (terminology used below comes from the Post/Scytl protocol):

i. The offline SDM is specified to generate SVK and BCK at random. A compromised offline SDM software generates BCK as a keyed hash of SVK. Since the voter enters the SVK into the voting device, this allows a compromised voting device to cast a ballot on behalf of the voter, even if the voter attempts to abort the vote casting, violating the complete verifiability property.

ii. The compromised offline SDM software communicates the internal state of its random number generator through the SVK. The adversary uses a few dishonest voters' SVKs to reconstruct the state of the random number generator and thus all the voters' key material. This breaks voter privacy.

Is it acceptable to assume that we can trust these computations by fiat, simply by placing them in the printing office? We caution against this! In designing secure systems one should always work to minimize trust assumptions. The alternative extreme would be to place the entire voting server in the printing office (where, by assumption, it could not be compromised), which would be absurd. An alternative approach would be to mistrust almost all computation except perhaps very simple computations like printing. Indeed, we recommend that the printing office does just that: it prints! More complex computations should be done in a way that reduces the risk of corruption (e.g., by being replicated and subject to the requirement of [VEIeS, §4.4.13] *"The control components must be set up, updated, configured and secured in an observable procedure."*) or so that the results are independently verifiable.

2.1.4	**Independence** The VEIeS allows us to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEIeS allows the use of application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?

Software and hardware from different providers should be used in each component to guarantee true independence. This would be easier to achieve if the deployed system would be less complex and would use commonly deployed cryptographic primitives. The implementation of ZK crypto in the Post/Scytl system is relatively specialized and complex, which makes it harder to have independent implementations.

2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?

This would be beneficial as it weakens the required trust assumptions.

2.1.6	The VEleS requires operating systems and hardware to differ. How relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
If one wants true independence, one should also have independently developed applications that implement the control components and auditor technical aids. The downsides of this are the complexity of such implementations and the feasibility of finding enough experts if the used technologies are not widely deployed and tested. Different operating systems and hardware though should not be a problem.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you assess long-term privacy issues?
For both questions: such designs could increase integrity and public confidence. They might also be simpler to implement and to understand by the voters. There might be some privacy risks, in particular when using a public bulletin board, but (depending on the approach taken) these may be acceptable. Clearly, one needs to look at specific designs in more detail. Overall, this direction seems promising.	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
Software correctness is critical; a correct design guarantees nothing given incorrect software as was previously seen first-hand. Even relatively small software errors can invalidate the election. Hence software correctness is of critical importance for "the final product". Humans are incapable of writing correct software even of modest complexity on their own. In particular, ensuring a correct implementation requires formal verification, either by theorem proving or, possibly, using algorithmic methods such as some variant of software-based model-checking or static analysis. The Common Criteria requires formal methods for its highest Evaluation Assurance Level, in particular EAL7. Note that the VEleS mentions EAL4 for hardware security modules (which is standard) but only EAL2 for testing functionality. EAL2 is not suitable for mission-critical systems like those for voting. EAL7 would be appropriate, however it is quite costly, and, moreover, recertification may be required after system changes.	

Herein lies the conundrum of designing critical systems like voting: voting authorities are not immune to economic and scheduling pressures and hence resort to pragmatic compromises that have less rigorous guarantees than state-of-the-art high-assurance development methods. The current Post/Scytl system is, in its current state, beyond what the state-of-the-art could feasibly verify. Verifying critical parts of the system or control components should be possible (although not easy or cheap) if they were designed from the start with verification in mind. Again, simplicity helps tremendously in this regard.

Concerning secure deployment and integrity protection: of course downloaded code must be authenticated, e.g., by checking a signature. But this is not enough. Controls must be in place on who signs the code on the provider's side and to ensure that it is built from the code that was actually verified. Moreover, the integrity of the code must be protected on the host systems where it runs. Needless to say, there is overhead in getting this right. Stronger guarantees are possible when using trusted execution environments to attestate the actual code being run.

As to the role of experts: ideally some experts in building high-assurance systems using formal methods are employed within the company building the system. Others would be used to check the appropriateness of the assurance activities taken and the evidence (proofs) themselves. This is analogous to what might be done in a Common Criteria EAL7 development and certification.

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?

In this question and other questions it is unclear whether the question is asked with respect to the Post/Scytl system or in general. We shall assume it is asked in general here as it concerns a general ordinance. In this case, the question is difficult to give a precise answer, as we explain below.

Threats are potential causes of unwanted events, e.g., a malicious entity enters a harmful string into the system, causing a buffer overflow. These events can be caused by different threat agents and can affect the confidentiality, integrity, or availability of data or processes related to voting. The actual threats possible depend, in part, on the architecture and protocols used and hence which events may exploit potential weaknesses. Said another way, it is difficult to do an actual threat (or more generally risk) analysis on a system, without a description of the system itself. The attack surface is open-ended.

Without a system description, probably the best one can do is to:

1. assume that basic components are present that communicate with each other and
2. assume the existence of a basic data model describing data that must be present

The threat catalog amounts to stating that the adversary cannot read, write/modify, or disrupt associated data (in storage or transit) or processes. For example, the threats 3.1.6 and 3.1.7 that the administrator changes/adds votes are examples of this: an election system must process votes and ensure integrity requirements. (Note though that the threats can be given without naming the threat agent, e.g., for the threat "infiltration by criminal agents", presumably infiltration by other threat agents such as foreign intelligence services would also be problematic.)

One class of threats that needs to be carefully considered are those related to socially engineering the voter to omit security-relevant checks present in the design. For example, the threat that the attacker manipulates instructions displayed to the voter on his screen, causing the voter to ignore return codes (e.g., by printing "Congratulations you have successfully voted!" and not displaying the return code).

2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?

Currently controls are missing that ensure that the implementation conforms to the design. At a minimum that the design logic (control flow, operations taken, etc.) is reflected in the code. Ideally the code is formally verified as well.

An important principle (not a “measure”) is that the system needs to be built on well understood and widely accepted security primitives.

2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?

Deficiencies (also noted elsewhere in this questionnaire) include

- Clear, sufficiently detailed design documents
- Holistic security analysis should be used to evaluate the system in addition to (or part of) certification/compliance
- Correctness of the implementation
- Questionable trust assumptions (e.g., putting critical computations in the printing office)
- Post quantum resilience
- Resilience to social engineering attacks

Addressing these can be done within the context of the current measures and standards.

2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).

What makes the e-voting different from e.g., e-banking is that in e-banking there is no expectation of privacy with respect to the bank and also that the bank is trusted with the integrity of the account. Furthermore, each bank client is concerned only with the integrity of its own account. This makes such systems cryptographically simpler than an e-voting system, which must perform processing (e.g., tallying) over encrypted data (i.e., votes). Note too that if there is an error in banking (e.g., transfer to the wrong account), transaction logs can be used to roll-back the effect of errors.

In principle, an e-voting aims to (1) satisfy stronger security goals than an e-banking system and (2) against a much stronger adversary. Due to the fact that e-banking data is not confidential with respect to the bank, its processing and integrity protection can be simpler. An e-voting system doesn’t protect the integrity and confidentiality better than an e-banking system, it simply protects it under more stringent trust assumptions and therefore with more complex protocols and crypto.

2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?

It is clear that, unlike with in-person or per-post voting, a badly designed electronic voting system could allow large-scale manipulation, whereby the attacker can change the election’s results. An e-voting system must be designed to eliminate such manipulation even by highly motivated, skilled, and financed state adversaries. Internet voting cannot be considered a gain in security. In-person voting is the safest, followed by postal voting, followed by remote e-voting, due to the substantially increasing

attack surface. But e-voting can provide more convenience than these other alternatives and may lead to higher voter participation.

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or dis-played incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
There were a number of studies showing that users typically do not check security indicators. An additional problem is that, in case of phishing, the webpage might display instructions that differ from the ones that the voter received via mail. It would be better to design a system such that the voters cannot fail in this regard. It is not clear that much can be done here. Perhaps some variant of code-voting would require less effort and would result in better security.	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
This is a long standing problem in web security. It is not clear that much can be really done unless external devices are used to check the domain.	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
Aside from installing browser extensions/plug-ins or external devices, there is little that can be done.	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
Quantum computing would have a detrimental effect on the security of any protocols using conventional public-key cryptography for key establishment or signatures, such as RSA, ECDSA, ECDH, and DSA. If these are used in the voting protocol then (depending on their use) vote secrecy and integrity can be compromised. Each year the likelihood of having an operational universal quantum computer becomes higher that can utilize strong quantum algorithms (e.g., Gover and Shor's algorithm), which makes public key encryption schemes like RSA and Elliptic Curve Cryptosystems completely insecure. There is also a risk that such a quantum computer already exists (or will exist in the near future) and is in the hands of intelligence agencies, and we simply do not know it. Hence it is unclear if we can determine when	

a post-quantum cryptographic redesign is necessary. There is hope though that basic security mechanisms like TLS will be updated in a timely way with new quantum resilient crypto (ref NIST competition).	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
Basic security hygiene is always good, but it is hard to scale up. We would not assume that the voters would follow MELANI guidelines. Moreover such guidelines may reduce risks of platform compromise, but they do not eliminate these risks.	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
It would make it easy to sell votes anonymously. It is hard to predict if this would be wide-spread but technically it can be done. See, for example https://arxiv.org/pdf/1903.00449.pdf	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
Where existing standards are used such as ISO 27001 or the Common Criteria, it makes sense to use organizations approved by those standardization bodies to carry out certification. A central problem is how to ensure the system's security and functional correctness. As was previously carried out, this problem was split into: **1.** A proof that a model of the protocol design has the desired properties (checked by an external expert) **2.** Evidence that the model correctly represents the design (this should also be checked by the external expert) **3.** Evidence that implementation conforms to the design. Checking (1) and (2) need to be done by external experts. Moreover, (3) does **not** correspond to an ISO 27001 certification or systematic testing under CC EAL2. If this is left to the 27001 auditors, it is	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

questionable whether, for a complex design like that of Post/Scytl, they have the necessary skills to do this well. We suggest that (3) should also be carried out by experts with a deep understanding of applied cryptography. These experts are typically professors or researchers working at the forefront of this area, not consultants from a typical accounting company.

Depending on the design of future systems, it may be sensible to bring in specialists to analyze their design and implementation. For example, the use of trusted execution environments, Byzantine fault-tolerant algorithms, etc. would benefit from consultation with experts on these topics during the evaluation process.

Finally, no matter how the tasks are sliced up, it is important that they include a holistic security and risk analysis. As part of this, experts should be able to judge that the system is simply too high of a risk to be used, even if it contains cryptographic and formal proofs for various parts. Every system has residual risks stemming from parts not modeled and verified, or assumptions made for the verification.

3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.

This would need to be considered on a case-by-case basis based on which requirements are violated and the difficulty and associated risk of exploiting the system as a result. Releasing a system with known deficiencies is very likely to produce a strong public backlash, given how important and sensitive the topic is.

3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

Yes! Those doing the certification should not be dependent (financially or otherwise) on those who benefit economically from the adoption of the system, i.e., the government should engage the experts rather than the vendors.

The credibility also depends on the process around certification: it must be clear that certification can fail, rather than the system minimally patched to work around the main blocking objections.

3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?

See answer to 3.1 regarding adaptations to scope and depth.

3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?

This is a function of how detailed the examinations are. If one does an examination at the level of ISO 27001, which focuses on ***processes***, then the examination results are fairly robust, i.e., the ***product*** (system) may change provided there are still appropriate security management processes. So for security management aspects, e.g., as described in Section 5.3 of the Annex of the VEleS, the terms of validity mandated by the standard are probably adequate. In contrast, minor changes in design or implementation can completely undermine security. If the examination is at the level of the correctness of the design or code, then such changes should, ideally, trigger some form of recertification. Admittedly recertification after each change would be an enormously high price to pay and one can certainly consider “pragmatic compromises” such as recertification after major changes and lightweight checks after minor changes. However, it is hard to quantify the risks that such shortcuts entail.

3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?

Difficult question. Putting questions of IP aside, ideally all artifacts, including design, implementation, and evaluation documents, should be in the public domain for review prior to the system’s usage in elections. This increases transparency and allows for greater scrutiny. However, a prerequisite for this is that these artifacts are all of very high quality as otherwise this will not increase trust. Moreover, modern systems are not built to be correct by construction (using formal methods) and so they will

have many flaws, in particular in the implementation. Publishing the code makes it easier for attackers to find and exploit those. Clearly any additional presentation and "review" will require sufficient additional time for remediating any controversies that may arise. This should not be underestimated as e-voting is rather controversial.	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
This is difficult to say in general and it depends on what the differing opinions are about and whether the opinions actually hold merit (not all opinions do). Obviously there must be a person or group that takes responsibility for dispute resolution.	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
The "specialized community" actually has different subgroups of "security researchers". The first kind work at universities and are interested in finding security vulnerabilities in complex and important systems and publishing the vulnerabilities they find. Some of these researchers might even use this to showcase their own analysis tools. Most such researchers are responsible and serious and are motivated by publications and also possible positive exposure in the press for their findings. For them, the right to publish their findings is essential although they may be open to accepting a responsible disclosure process. They will largely abide by the law. The second subgroup is the hacker community who hacks for fame, notoriety, and sometimes for bug bounties. They tend to be less tolerant than the first kind of researcher in terms of restrictions on what they can and cannot do. Members of this community may have an anarchistic streak and even republish the source code anonymously. In general, they have fewer scruples about violating the	

5

6 Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

law. Openness and few, if any, restrictions are important to them. If they are treated well, they may go along with a responsible disclosure process.

Both subgroups are helpful in finding problems. The first subgroup may be more successful in finding subtle design errors or bugs concerning the use of sophisticated cryptography. The second kind probably generates more "noise" but also uncovers significant bugs, in particular in the implementation.

If code is released to numerous security researchers, IP protection is hard to achieve even with legal restrictions since attribution is difficult once code is released anonymously. There have been proposals from the research community to mitigate such problems, e.g., to watermark source code for attribution purposes, but usually such schemes offer inadequate guarantees.

4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?

What can be scrutinized depends on what is released. If code is released without design then public reviewers are most likely to find just coding errors and improper use of crypto (which is useful!) and the kinds of bugs one would find with a good code scanner. But it will be difficult to detect design errors as one must reconstruct the design from the code, which is very time consuming. If design documents are provided, then (1) the design can be analyzed as well as (2) the conformance of code to design. If configuration files are provided this can also be analyzed. In short, anything that helps an auditor would be meaningful to help those members of the public (security researchers) carrying out analysis.

A separate question is what SHOULD the *public* analyze versus paid *auditors*. This boils down to the question of "trust" versus "trustworthyness" and also how the system is built. If the system is built with high assurance methods and the paid auditors are sufficiently skilled and have sufficient time, then the system should be trustworthy. But the public may trust more an open system that "they" (or their "representatives") can analyze rather than experts.

4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?

This depends in part on the complexity of the system. The more complex a system is, the more time it takes to check it. For example, the proofs for Post/Scytl took many months to prepare. They were nontrivial to check as they corresponded only indirectly to the design. A code review, if done thoroughly, can also take weeks or months, depending on the complexity of the code base. This is impossible too if the system is still undergoing change. And there must be time to respond to problems.

If the system is not overly complex and the documentation is in order, checking design and code could be completed in some months, assuming no problems are found and further iterations are needed.

4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)

The VEleS states: *The documentation on the system and its operation must explain the relevance of the individual components of the source code for the security of electronic voting. The documentation must be published along with the source code.* It is unclear what this really should entail. It appears to be a high-level security rationale for a (not explicitly given) design. If you are going this far in making the system public, and the system has sufficiently precise design documents (which it must have if one is to produce a model of the design for verification) then wouldn't it be better to give the design along with the rationale?

Instructions for building and using the system so that security researchers could carry out trials and generally play with the system would also be helpful.

4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?

	What are the goals? If it is just to get input for system improvement, the feedback can be addressed to a neutral party like the Bundeskanzelei who ensures it is accounted for. If the goal is to improve trust, then the feedback and the reaction to it should be in the public domain. It is important that the parties providing the feedback get the rewards they seek for their efforts, e.g., ability to publish, recognition/publicity, bug-bounties, etc. Handling the security research community is not so easy!
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
Difficult question. For commercial (rather than open-source) projects it is fairly rare. If there are too many (especially simplistic) bugs then publishing this will probably not increase trust in the system. But in some cases (e.g., see answer to 4.5) notification is probably necessary, in particular when security researchers find the bug. In this case it is important also to publish the fix.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
We have commented above on the benefit of making more artifacts available for the PIT and the motivations of the different kinds of security researchers in the public. Note that it is advisable to have a private “intrusion test” prior to the public one, where competent specialists are hired for this purpose.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
The restricted use of the system reduces associated risks by reducing the impact of a breach. Such usage can potentially increase trust as one can argue that the system has been successfully used in elections in a limited way, prior to large-scale usage. One could make an analogy with test flights under realistic conditions prior to flights with passengers. Of course, for elections with small margins, the impact of abuse may still be substantial. The public must also have trust that any abuses will be detected and reported. Moreover they must believe that the adversaries would be attracted to attack a system used at a small-scale are the same adversaries as those who would attack a system used at a large-scale for an important election.	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
Process and associated tasks depend on protocol used, e.g., if homomorphic encryption is used for tallying, each party can perform the computation itself. If NIZPs are used, these need to be checked. To be credible, the checks must be credible. In the ideal case they can be carried out by the public using independent software. The risk though is that if the protocol isn’t post-quantum secure or there are bugs, then this may compromise confidentiality. Hence restricting access to encrypted votes to a group of independent auditors (e.g., from different political parties) might be best.	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
See answer to last question.	
4.11	What additional transparency measures could promote security and / or trust? (Infra-structure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

In theory, the more the better. In practice there are limits due to financial and timing constraints. It takes time and money to produce documents fit for publication, the public must be given time to look at them, there must be a response/remediation period, etc. Also, if published, the quality must be very high, or it will result in reputation damage and loss of trust.. While this is ideally the case, in practice not all documents produced by companies and auditors are at this standard. Augmenting code with design documents and audit reports might be a reasonable compromise. But then, as just explained, more time and budget must be allocated for this.	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
Any plausibility checks should have a sound statistical basis. The theory of risk-limiting audits is promising and it has been suggested that these ideas can also be used in the context of some protocols for electronic elections. See, for example, *Verifiable European Elections: Risk-limiting Audits for D'Hondt and its relatives,* by Stark and Teague (2014) where the conclusion points to possible applications to electronic voting, e.g., using homomorphic tallying. If there is a sound statistical basis, then the results (and method) could be publicized and it should serve to increase trust. Of course, the audit must be done well as otherwise the result may make false statements about the election result.	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
For 1: See in part the answer to Question 4.1 on how to get members of this community involved in public scrutiny: let them analyze your design and code and publish the results! For those who have tools operating on binaries (e.g., Fuzz testers), give them access to your binaries. For 2-3: These tasks amount to consulting so hire them as consultants. Most security researchers/faculty have some flexibility to do limited amounts of consulting.	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
This varies in part on the debate and the representatives. Some scientists may be happy to take part in debates as a service to the community or as a way to learn about voting in practice, to	

demonstrate the practical impact of their knowledge, and further their network and career. Others, especially if the time commitment is substantial, may prefer to work as independent consultants. Motivations vary.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
To be understandable to the public, the facts would have to be presented at an appropriately high level. This might be suitable as news articles, popular articles in technical magazines (like Communications of the ACM) or reports written for a generalist audience. Modern forms of communication include tweets and blogs; this often does not convey sufficient seriousness, but might be acceptable if the source was well-respected. The problem is not so easy to solve though. Anyone can communicate via a tweet or blog and the general public cannot easily distinguish experts from loud, opinionated non-experts. An option here might be to have "white papers" or commentaries published on the webpages of the Bundeskanzelei, where they could carefully moderate what is published there.	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
Many options are available. These include general explanations about relevant topics, such as how verifiability works, notions like software independence, the relevance and importance of the checks the public is asked to do (such as, verify server certificates, return codes), etc. These would be written for the general public. It is conceivable that more technical documentation on these topics is written for a more specialized audience. E.g., to debunk plausible-sounding but wrong statements in the popular press. And as discussed in Question 4, the results of evaluations (which can be highly technical) can also be published.	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? ● Public debates on selected issues ● Hackathons around selected challenges ● Others you might think of
As discussed in Section 4.1 motivations vary. See the previous discussion concerning motivations of different subgroups of security researchers. The public may well be interested in a debate on selected issues. But note that the topics of such a debate are subtle and finely nuanced. Consider just one example: even the full verification of design and code does not entail "no risk", but rather pinpoints, via assumptions, what risks remain. Subjectivity will come in as to the magnitude of such risks and how the risks are increased when one does less than demanded by, say, a Common Criteria EAL 7 evaluation. One can have a similarly nuanced discussion, say, about the benefits of using a simpler design hardened using a trusted execution environment. These events should be organized by a neutral party, not a vendor. The Bundeskanzelei would be ideal in this regard.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an

authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
Some kind of continuous risk assessment and adaptation is needed. Any voting system used will involve one or more hardware/software stacks, including hardware, OS, libraries, cypher suites, etc. If vulnerabilities or new kinds of attacks on any of these are discovered then the system may be insecure. Examples are that cipher keys become weak, algorithms are shown to be insecure, new side-channel attacks are developed, etc. Such issues must be constantly monitored and accounted for. It is therefore important to reduce any active components and reliance on software or crypto on the voter side and focus on systems that rely on the voting backend solely. Such backends can then be audited ahead of each election. Tracking all these dependencies is difficult. A careful analysis of the design, implementation, and deployment could be used to develop a detailed catalog of such dependencies that would help to track these issues and ensure that appropriate measures are taken (e.g., patches deployed) before each election. This is nontrivial as it would involve the concerted effort of multiple parties and must be updated with each system change.	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
The benefit is it builds trust in the case of a positive assessment. The downsides is it exposes risks that are not adequately mitigated. Moreover, if the assessment is not done professionally and the results are of high quality, publication could reduce trust. (Opponents of e-voting would presumably be quick to spot such issues and use them to generate negative press.)	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
Supply chain risks usually refers to the risk of disruption. Presumably here the issue is what if the system provider/contract do not deliver in a timely way that fulfills certification requirements. Presumably this is handled contractually, with financial penalties and by working with providers who have a proven track record of delivering high quality (certifiable) voting systems in a timely way. Careful planning of the development time and costs of the voting system (accounting for all the certification activities) can also help, although this is a notoriously difficult task.	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
We don't recommend that conditional authorizations are issued.	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
We have not studied this in detail and have no specific recommendations here beyond consulting some of the standard guides such as the NIST special papers (SP 800-30, 800-37, 800-39, 800-53) and BSI Grundschutzhandbuch, both of which have detailed descriptions of risk analysis methodologies. There has also been work on Common Criteria protection profiles for electronic election that may be helpful here. Risk analysis is important in providing a structured way of analyzing assets, possible vulnerabilities, threats, and associated risks. The quality of the analysis is dependent on the quality of those performing it. It is also aided by the quality of the supporting documents, e.g., concerning the design and implementation. (An abstract risk analysis without these would be useless.)	

6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
We cannot make recommendations here as we do not have a comprehensive overview of which companies or consultants do a good job in this area. Risk analysis is not per se, "scientific" as the results have a large subjective component. Nevertheless, having a team do this that includes scientists with deep expertise in the protocols/crypto/infrastructure/frameworks being used would be helpful. Involving expert developers who have previously built/implemented/debugged similar artifacts would also be useful.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?
As indicated above, different (advanced) technical competencies will be needed. It is unlikely that they are all available in house. Subdividing roles and responsibilities is difficult without first fixing the risk analysis methodology.	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
This could be sensible. But a concrete answer is difficult to give without a specific system architecture and risk analysis process. Note that if a system is divided into two subsystems, and these subsystems are analyzed in isolation, there is no guarantee that the risk analyses compose, i.e., the risks may not simply be the union of those risks associated with the individual subsystem. This is because the different subsystems may interact in ways or depend on assumptions of the other subsystem, that the individual risk analyses did not account for. So, if the risk analysis were to be factorized, then some kind of additional analysis will be needed to identify new risks that come from the interaction between the (two sets of) processes and infrastructure.	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
We have no direct experience with this methodology. As explained in its documentation, the approach *"is designed to allow broad assessment of an organization's operational risk environment with the goal of producing more robust results without the need for extensive risk assessment knowledge."* Looking at examples given, e.g., the risks of confidentiality breaches to data in transit might be mitigated by using SSL when communicating with the server. We believe that such a lightweight ("allegro" emphasizes fast and light) approach will likely miss subtleties arising from the particular adversary model considered by the Bundeskanzlei (e.g., inside attackers) and problems in the actual implementation or configuration. While employing such a lightweight methodology is surely better than no risk analysis (again, as it provides a structured way to think about the assets, threats, and mitigations), it does not seem suitable for a critical system like voting where *Larghissimo* or *Largo* would be more appropriate than *Allegro.*	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
The first step is to monitor and know when you have a crisis. The monitoring can include monitoring what is happening within the network and servers, monitoring feedback from the voters (e.g., lack of access or individual verifiability checks failed) and monitoring feedback from election auditors. The second step is to be able to resolve disputes. Here it helps if the election protocol is designed with *dispute resolution* in mind. Observing a problem is not the same as being able to attribute the source of it and determine corrective actions. Clearly this needs to be worked out before hand, e.g., problems with individual verifiability presumably can be resolved by having the voters vote in person. How about problems with universal verifiability where zero-knowledge proofs fail to check? If there are steps that cannot be resolved or recovered from then a communication and action plan should be determined *before* the election and followed at the election. This should include who is responsible for communication, e.g., the Bundeskanzelei.	
7.2	What are the right events and thresholds for an activation?
Presumably *everyone* should have the right to vote and have their ballot recorded as intended and cast (if not electronically then in person or by post). If this is not possible then the election is invalid. Clearly if there is evidence that the talley is incorrect then the election should also be invalid. Breaches to confidentiality, while problematic, do not affect the election outcome.	
7.3	Who should be involved in crisis management, with which role?
There are different roles associated with different kinds of monitoring (see above). For building trust it would make sense to involve individuals from the Bundeskanzlei with those running the election (e.g., those responsible at the Kanton) and those responsible for the system (e.g., Post). A neutral party though should lead this (e.g., Bundeskanzlei).	
7.4	How should the communication be organised (internally and externally)?
We do not have an opinion on this.	
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
We also do not have an opinion on this. It is a possibility if it would substantially increase trust or they bring in competencies not available elsewhere.	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
This needs to be outsourced to an external company that specializes in this topic. This should not be left to individual cantons or to the BK.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
The voting system needs to be designed such that it allows for proper forensics investigation. This might present a tradeoff with respect to its privacy guarantees. It is important that technical means are in place to assure that recounts can be done and that the system has enough redundancy to cross check the results in a manner understandable to the general public.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
As seen with US elections, this seems hard. Prevention should be priority.	

7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
This is highly system dependent. So it is hard to say how this would look like. But it would be good to integrate the robustness to failure and recovery into the voting system.	

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Florian Johannes	**Last name**	Egloff
Organization	ETH Zürich – Center for Security Studies		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

Which are the most important questions you would need answers to? (Think for ex-ample of roles and responsibilities, operations, system, scrutiny)

Preliminarily, I would not need answers, as the U.S. National Academy of Sciences has assessed that "we do not, at present, have the technology to offer a secure method to support Internet voting." (NAS 2018). I believe this still to be the case and would not advocate to use internet voting in the short- to medium-term, at least not before the technologists believe it to be secure enough for use.

However, since this answer is unsatisfactorily short, I will expand. I will be answering this questionnaire from the standpoint of political science, with a particular emphasis on socio-technical and socio-political processes that are touched upon by the introduction of internet voting. Thereby, as a preliminary matter, I would encourage the project leaders to see voting security wholistically and assess the impact of a change to current voting procedures on the (perceived) security of the overall system.

Note: at least since Anne-Marie Oostveen's PhD research on e-voting and trust in 2007 (Oostveen 2007, Context Matters. A Social Informatics Perspective on the Design and Implications of Large-Scale e-Government Systems), it should be clear that there is a difference between the mathematical/technical security of a voting system, and the perceived security of and trust in a system. She said: "Many technologists think that the solutions for security and trust issues lie in adjusting and improving the technology." She asked: "Will users trust the system more when it is more secure? Will offering voter-verifiable paper trails work to gain trust from people or are there other non-technological issues that are of equal or more importance?" (p.141).
Many of the questions that follow seem to be oriented in a techno-centric mindset, which assumes, that improving certification, using more secure cryptography, and getting more publicly verifiable notice boards will lead to more trust in the system. That may be part of the answer.

However, a socio-technical view of voting would stress other factors, such as the social context, including political structures that have enabled trust in the current voting process, despite its (demonstratable) insecurities. Thus, under such considerations, other topics would be of relevance, including what political work is necessary to earn voters' trust? How does the e-voting technology need to be designed for and by the Swiss political process? How are voters part of that design process? How is the system shaped by the localities, including the village level politics?

With that preface, here are my answers:
One of the fundamental elements of democracy is the peaceful transfer of power through elections. In semi-direct democracies, referenda are the final arbiters of political conflict. Thus, it is key that the population has trust in the process and its outcome. Any change that has the potential to disrupt this trust is per se to be looked at with some scepticism. Internet voting has such a potential.
Questions I would thus ask:
Given an allegation of cheating/misconduct, is the remediation trusted and trustworthy by the population (voters, non-voters, non-eligible residents)?
Given multiple threat actors deliberately injecting doubt&mistrust into and around the voting process, is the outcome still trusted and trustworthy by the population?

Which are the most important answers you need in order to conclude that internet voting is trustworthy?

- a more secure fall-back option, i.e. given a digitally competent adversary, the potential for disruption lies both in the internet and physical voting. Particularly, the risks to the pro-

cess of voting should be seen as integrated (e.g. electoral rolls, printing, counting, vote tallying etc.). This means, significant efforts need to be spent to make physical voting more secure, before internet voting should be introduced. This may include for the federal administration to expand its regulations regarding the use of computers/digital equipment in the physical voting process. This should be within the scope of the discussion, when considering internet voting.
- rough consensus of the technical experts that secure internet voting is technologically feasible (currently not existing), and adoption of a solution that follows such a consensus
- open-sourced software system
- ownership and management of the election infrastructure by the state.
- political ownership of running the election, including the risk management

How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)?

- the local (i.e. communal) voting authority needs to be able to explain the system, how it works, and how they are in control of the process, audit, and establish the outcome. They need to be able to competently answer how conflicts are remediated, i.e. how allegations of cheating or occurrences of hacking are dealt with.

Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting?

- I am missing a theory of change towards the building of trust into an internet voting channel. The design, development, testing, and introduction of internet voting has to go hand in hand with building social trust in the new voting channel. In my opinion, this is best done by building trust bottom up: start at the communal level, decentralize the system, and build trust over time.
- I am missing serious efforts to secure the digitisation of the physical voting process. As explained above, digitsation risks do not just occur in the "new" internet voting channel, but are also present in the physical process (see e.g. Killer & Stiller 2019). I would encourage to first demonstrate mastery at managing the digital processes in the physical space, before tackling internet voting.
- I am missing a clearly identifiable strategy for crisis management and response. There are (to my knowledge) no clear, pre-defined and publicly communicated procedures for crisis communication. This may be lack of knowledge on my part, but given that I am a politically interested voter, that I do not know about it seems to indicate a lack of transparency / active communication.

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEIeS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEIeS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEIeS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEIeS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three

state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

Answer: this question should only be answered by cryptographers. I will defer to them. Whoever selects the building-blocks should be a trained cryptographer and only select from best practice.

The only example where such a building block was standardized and backdoored that I would point to, is the history of the Dual_EC_DRGB. It went through NIST standardization and was, presumably, backdoored (see e.g. Egloff 2018, DPhil thesis).

2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?

Click or press here to enter text.

2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?

Answer: I do not understand why "assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy". If this is axiomatic, i.e. we assume the printing office is trustworthy, then this statement is highly problematic. We, of course, want to design procedures where we minimize the functions given to a node that we axiomatically consider trustworthy. Rather, nodes should prove that they are trustworthy.

2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?

Answer : I believe it the security benefit would be greater, provided, that the software is properly architected, implemented, and tested (ideally open-sourced).

Regarding independence, one should also ask an additional question: Is the SwissPost the right partner to manage the online systems, given the significant trust

placed already into the SwissPost in the physical remote voting channel? Ideally, the election infrastructure avoids single points of failures and cross-over trust problems between channels.	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
I believe in the added value of multiple different verifying tools, thereby decreasing susceptibility to human error and making it harder to cheat.	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
I find this a good, relevant, but at the same time difficult question to answer. I would like to preface this answer by stating clearly that I am unsure. **The trade-off is between independence and complexity of managing the system. On the one hand, the separation does mean that an attack is less likely to scale, i.e. that an attacker has to make more of an effort to compromise the entire system. On the other hand, if an attacker manages to compromise a control component, then they are likely skilled enough to also compromise the other components. In addition, the diversity of systems and platforms increases the knowledge and skill level required in managing the systems on the system operators' side.**	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
The first question I do not have a good answer to. **The second question of the public bulletin board seems, to a non-cryptographer, problematic. If you do find serious flaws in your system later, or, if enough time has passed to break the trust-assumptions made now, long-term privacy could be at risk, which, given the long-term nature of a voter's life (80+years) is a real concern.** **The privacy questions, thereby, are not only present in the public bulletin board (which could, presumably, be engineered to be privacy-preserving), but also in the privacy risks from voters' infected devices, or from a compromised system operator (many of these considerations can be found in: Bernhard, Matthew, Josh Benaloh, J. Alex Halderman, Ronald L.**	

Rivest, Peter YA Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach. "Public evidence from secret ballots." In *International Joint Conference on Electronic Voting*, pp. 84-109. Springer, Cham, 2017).	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
It may be an idea to look into the US DoD's trusted foundry, resp. the secure supply chain programs. Given that any sufficiently competent maliciously inserted backdoor/access will be indistinguishable from a bug/flaw, it is pertinent to have a much stronger insight, oversight, and assurance over how the product is created, from design to actually running the code in production. This does not mean, one couldn't open source the product. It just means one needs reproducibility, understanding, and oversight of the development process. The fact that a flaw from 2017 was still present in 2019 and not spotted seems to indicate a lack of taking responsibility for the actual system on the system operators part, and a too high degree of trust in the system operator by the state.	

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
Yes, though the scope of the threat modelling in 3.1. is unclear. I am missing state based threats (they are not criminal organisations). **To start with, the threats listed are system specific. However, the security objective is not just to have a secure system (though that is important), but to have a trusted election/voting outcome. For that social factors need to be taken into account. An example of missing threats could therefore be:** **A hostile state wants to sow doubt and distrust into the integrity of the election/voting procedure (security objective: trusted outcome).** **Another example of a missing threat are more complex attack models: E.g. an attacker colludes with the printing office and infects voters' computers at the same time to be able to change results (security objective: result equals voter's intent).**	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
I would add to 3.9. something about espionage / foreign-intervention risk. You cannot just manage this risk with an "education" module about information security.	

I was not able to identify where you included a communications plan & transparency strategy that you need, when your results are alleged to be wrong. How are you convincing a distrustful electorate that you are trustworthy, within a few hours?	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
I believe in the Swiss case, there was no clarity of how your plan to earn the voter's trust. The new channel can be objectively the most secure channel, if there is no social trust in it, then an attacker has many opportunities to discredit it. **I would encourage you to think about how you can decentralize the system, so that the municipal level is involved in overseeing the process. This would have the benefit of starting with a procedure voters are used to (overseeing elections, counting etc.) and tacking the system onto that.**	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
I am not sure that this is a hard bar to meet. Given the breaches in banking, health care, and infrastructure, the reference points do not inspire trust.	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
Part I: Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? **As an attack vector, the internet has two significant advantages: scaling of the attacks and no requirement of physical presence. Both combined make it a lucrative attack vector and potentially invite new attackers into scope that would not be able to undermine the system otherwise, due to the inability, riskiness, or unwillingness to be physically present. Thus, introducing internet voting broadens the threat space. Whether or not this leads to a gain in security is dependent on how you define security (see Part II).**	

Part II: Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?

Which kind of powerful organisations?

E-voting faces the full gamut of threat actors, from benign curious, technically literate voters, to domestic participants in the political process (e.g. a political interest group), to advanced persistent threats controlled by states.

What methods would likely be used?

Advanced persistent threats are threat actors that are able to select from the full-breadth of attacking techniques, and use whatever is best suited to achieve their goal. The methods are thus not predetermined, but rather, are selected based on the target and the operational goal at hand.

The question mentions "manipulate or read votes". Both are important concerns, though not the most important.

Democracies survive if the peaceful transfer of power is achieved via legitimate elections. Thus, the worst outcome an attacker can achieve is to negate this process. An attacker only needs to attack the appearance of trustworthiness of the process or outcome, not the actual trustworthiness. If the elections can be made to appear to be "rigged" then the attacker has a chance to disrupt the fundamental value in democracy, namely, that the losers accept the outcome. Internet voting has the potential to introduce such a means of sowing doubt. This has nothing to do with the objective "security" of the system, but rather, with the social familiarity & trustworthiness of the system by the population.

Uptake of internet voting thereby is no indicator of the absence of that vulnerability. The relevant question is not "do you trust internet voting enough to use it?" but rather, "given a scenario of widespread allegations of abuse and cheating, do you trust the process designed to prove to you the trustworthiness of the process and the result?" Thereby, I assess, it will be very hard to convince an (adversary stoked) distrustful population that one should trust the authorities' claims that the technical systems worked properly, that the programs claimed to be running were running, and that the outcome is correct. This is not a remote possibility, but rather the baseline threat any change of democratic voting has to deal with.

Thus, a first operational goal an APT could have is to influence public confidence in the process and result. Methods to support such an operation can include both information operations (overt and covert) and cyber operations (blending HUMINT and SIGINT as needed). The cyber operations could be designed in a way to produce irregularities in the voting process, ranging from voter compromise to infiltration of the supply chain, to using benign channels to produce suscpicioulsy looking statistics.

Another operational goal may be to sway an election outcome. One way to achieve this would be by compromising the printing office and widespread distribution of malware in the voting population. Thereby, with advance knowledge of the confirmation codes, a state adversary could produce the correct confirmation codes on the voters machine, but use the vote for a different outcome. Since real voters' comptuers could be used for this, this would be hard to detect server-side. Due to privacy of the vote, individual voters could also not detect the compromise, having been given the correct verification codes.

Another way to achieve a malicious outcome would be to use a vulnerability in the system itself. The source-code review process has, for example, demonstrated a vulnerability that would allow for a true vote to be rejected in the vote tally. An adversary present widely could thereby sway the outcome of the vote. One wonders whether the Swiss/cantonal governments have records to prove that such vulnerability was not used in previous elections/votes where the system was used, and why they have not (to my knowledge) published the records proving it.

Are there also reasons why they would not apply certain methods?

I would not exclude methods from the threat modelling ex-ante. Any voting channel should be built for a changing threat landscape, and procedures should be adopted not to secure only against threats from today, but realistic threats that could occur in a voting process.

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
This seems like a question that needs usability studies to answer robustly. The closest I am aware of are Fragnière, Grèzes, and Ramseyer's (2019) How do the Swiss Perceive Electronic Voting? Social Insights from an Exploratory Qualitative Research. However, their sample size is to draw any general conclusions from this.	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
Checking the fingerprint is a measure to detect an (off-device) person-in-the-middle. The security industry has been trying to get people to check the certificates for decades – with limited success. The best research in this area, I would expect, comes from usability studies in Human-Computer-Interaction research. I would encourage you to design a system that does not rely on voters having to spot this for preventing a person in the middle.	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
I preface the answer by clearly stating, I do not know, and my thinking on this should not be taken as expert advice. **I am also unsure I fully understand your question. If the client application is tampered with on the server-side, does that not mean that the server is compromised? If so, what hinders the attacker from running different control components or different election software in general?** **Having said this, one idea from the area of trusted computing is called "remote attestation". Couldn't the server verify that the correct application is running on the client and vice versa?**	

2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
Disclaimer: this is again a question where the project leaders should only follow the advice of trained cryptographers. **Quantum-computing, if and when it becomes usable for large scale decryption, will be taken up by very large technology companies and signals intelligence agencies. I believe in this context it makes sense to follow the NIST Post-Quantum Cryptography Standardization project, which is currently in round 2 of evaluations. To the extent that the secrecy of the vote is vulnerable to a quantum attack, it is paramount to select a quantum-resistant algorithm.**	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
Against some threats, they cannot. It is infeasible to expect voters to operate a secure platform against a well-funded and operationally competent state-based threat. **Thus, whilst voters can protect themselves against run-of-the-mill infections, the higher-end threats that would be relevant in an election context are not normally defended against. Data that supports this conclusion is offered by the CitizenLab's research, various industry studies (e.g. Verizon DBIR which tracks the mean time to discovery in organisations that are well defended), or by NGO's that are supporting activists (e.g. Amnesty, AccessNow).**	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
I do not know. **I think the introduction of e-voting would make anonymous vote-buying and coercion logistically a lot easier, which would lead you to believe that to the extent capability is the hindering factor, vote-buying and coercion would become more prevalent.**	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEIeS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certifi-

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

cation based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
Click or press here to enter text.	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
Click or press here to enter text.	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).
Yes. It seems to me that the examination needs to be appointed by the risk owner (election official in charge), and the reporting needs to feed back to the risk owner, who should be the one deciding about the publicity levels of the examination.	
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
Click or press here to enter text.	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
The key to the overall topic of certifications and examinations is to understand their merits and limits.	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
A continuous, well-funded, bug bounty program for the core voting system seems to be a smart way to include indepdenent researchers. This would mean allocating sufficient funds to this.	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
Opinions about what? The output of a certification process is supposed to give you a baseline assurance, but will not "prove" security to you. Hence, certification should	

be based on objectively assessable criteria that are either met or not. I do not see how opinions would come in.

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
Some of these issues should be ironed out by partnering up with a well-respected bug-bounty organiser and fund the program adequatly. They will not only be able to facilitate insight into the best way to organise this, but will also have a community of bug bounty participants that will scrutinize the systems. It may also be possible to learn from other public administration agencies that have previously done bug bounties, such as the US Department of Defense (Hack the Pentagon). **Ideally, the evoting solution is open-source and the bug-bounty ongoing continuously. It is unclear why one would limit the duration of a bug-bounty for a critical part of democracy.**	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
Ideally, the system is running as it would be running in a real election, source code is public, and documentation readily available. Ideally, testers are able to run the election system on their own systems as well.	

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

In addition, all the audits and certifications should be publicly available as they give indications to which parts of the code-base was previously found lacking in security. One ought to assume that a competent adversary has access to them.	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
I do not know. However, ideally, an evoting solution will have a constantly ongoing bug-bounty.	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
I do not know but would think yes. If security is rooted in the architecture of the system, rather than in obscuring processes, then full transparency should be welcomed.	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
Primarily, the bug bounty has to be run professionally, with contributors being compensated for their work. The output should be as transparent as possible, whilst taking care to not endanger currently live systems. Thus, feedback has to go to the maintainer of the system, the risk owners (election officials of the cantons), and as a matter of course, to the certfier of the system (Confederation). A scientific committee is an interesting idea, but I would only give it advisory capacity. It is important not to dilute the political responsibility for allowing/denying a system to be in operation. The risk owners should ensure they build competent organisations that are skilled enough to make informed decisions regarding the security of the system (risk ownership).	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
Yes, publicly and also towards the election commission where the system is/was running.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
Opening up the system to public scrutiny has demonstrated that it is one (amongst other) effective measure to gain awareness of the (in-)security of a system. If you look at the responses of the "Vernehmlassungsverfahren" it seems to be a pre-condition to earn public trust. Generally, the more you allow for scrutiny of your actual system, the more one seems to benefit from a public intrusion test. In terms of incentives, I would encourage coordinating with the bug-bounty community for engaging with the public. This is, of course, not sufficient for security testing. I would also advise to hire competent penetration testing firms to assess the security of the system. The two operate complementarily to one another. The findings of both should ultimately be	

made publicly available, including responses by the system maintainers / operators on how issues were addressed.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
Yes, though we should be specific what kind of trust. Limiting the electorate is a risk limiting measure that promotes trust in the election officials taking the risks in internet voting seriously. This does not necesarrily promote trust in internet voting, but rather in the overall voting process being run responsibly.	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
Ideally, the system is designed in a way to bootstrap on trust in the current analog system. Hence, I would advise to evaluate how trust in the current analog voting system comes about, and bootstrap trust from there. This may mean designing systems so that there are functions for "Stimmenzähler", communal "Wahlbehörden", etc… **The trade-off for introducting such extra complexity would be a gain in explainability and trustworthiness at the lowest democratic level. This may mean that introducing the system takes longer, but may also mean, that trust earned at the local level may be more stable (assumption on my part).**	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
I think publication should be done, no matter whether it is good or bad for trust. I believe people have a democratic right to know how the voting process took place.	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)
Transparency and voter inclusion in every stage. Note that the function of a "stimmenzähler" and the possibility of a "wahlbeobachter" is not to have the most secure version of a process, but to have the most democratic accountability of a process. The same principle should apply to electronic voting procedures.	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
Following the National Academy of Sciences' 2018 report, I recommend instituting risk-limiting audits (as also explained in Lindeman & Stark 2012). **I believe, properly instituted, statistical audits can increase public confidence in the results and hence should be published, provided there are pre-defined procedures/thresholds for when a recount would become necessary.**	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary

work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
1. Public scrutiny is encouraged if you start developing an open-source election/voting system that is tailored for Switzerland. **2. I am unsure how you would do that. Possibly by encouraging participation in an oversight board?** **3. I believe, this questionnaire is a bad example of science involvement. The questionnaire is not tailored towards the expertise of the person you are asking the question to. The one day allocated to answer the 62 questions leaves a bit more than 10 minutes to answer each question. Spreading my attention across so many questions leaves me in doubt whether this is the best use of my time.**	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
It must be a fact based, open debate, which can digest a complex argument and gives space to nuance.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
I believe some scientists can reduce complexity without loosing too much nuance. For example, Kenny Patterson gave a great interview in the Tagesanzeiger, entitled "So knackt man ein Chiffriergerät" (dated 14.02.2020), which is not only technically accurate but also communicates to a wider audience. **The importance in the communication about internet voting is not only to present the facts clearly but also be equally clear about the uncertainties and knowledge gaps that we are facing.**	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
I believe in a differing level of details for different audiences. The communication has to be tailored to the channel and audience that is addressed. Since you are trying to build trust in	

the whole population, you should be working out a communication concept that makes key pieces of the system available to everyone in a format that is understandable. **I recommend adding to this question: How should the system be architected and introduced in order to earn voters' trust?** **Personally, I believe earning voters' trust goes beyond presenting "information". Rather, the system should be built in a way that integrates into the lifeworlds of individuals, starting with their established trusted procedures, and build on that. Thus, if voters currently trust the remote voting option via mail to be counted by peers and local election officials, build an internet voting system that mirrors that.** **Local election officials should be in charge of the oversight of the local "internet voters". There should be local peers (Wahlhelfer / Stimmenzähler) in charge of verifying the internet votes. Build the system accessible enough, so that it can first be used for communal elections & referenda.** **I would recommend to tie into the federalist structure and start building subsidiarity into the actual system (i.e. everything that can be managed locally, should be managed locally). With the current structure, you run into the problem of the "built and managed in Bern" problem. Politically, it may be advisable to start at the grassroots level and built trust iteratively from the bottom to the top, rather than the other way around.**	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
Tacking on to the proposed question in 5.4., I would recommend working with communal councils (Gemeinderäte). Gemeindeversammlungen are great places to reach the interested voting public. Start by building touchable systems: i.e. replicate the system with physical objects for a workshop-like experience. Give people the option to "touch" the system logic. Explain how trust in the system is established & give people the option to "practice" internet voting right there.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
This is really a whole consultancy question in itself, which can only be inadequately answered in the time allocated. **Suffice to say that a continuous risk assessment process does need to take a 360degree view to risk. The updating needs to take place regularly: at minimum before deciding whether to use in a specific referendum or election and if used in an election/referendum, then in continuous situation analyses. The technical, political, and threat environment can change to such a degree that a change in the analysis is warranted.**	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
It is unclear to me that the (operational) risk assessments need to be published. This is to be distinguished from the overall risk analysis of the election system, which I think should be published.	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
This question presupposes that the cantons cannot be the system providers themselves. Why not? It seems unclear why a state would not build its own election infrastructure, an investment that will hopefully pay off indefinitely, particularly also for enabling future digital democracy options (such as more varied voting decisions than just Yes/No).	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
I am the wrong person to answer this question.	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
I am the wrong person to answer this question.	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
I would work closely with with election officials from across the different cantons, and then in a next step, exchange views with election officials from partner states. For threat modelling and risk identification, relevant agencies at the federal level might be of help (Lagebild des Bundes, NCSC, NDB). Science can help to establish baseline evaluation models and offer factual assessments.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?
Risk management of the election is a sovereign task that should be matched with a sovereign capability. I would caution to outsource that to anyone. As the elections are political proceses, risk should be owned by public officials and not third-parties.	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system

	provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
Cantons own the responsibility for its infrastructure and processes, including such provided by the provider. I would not ask the provider to give separate analyses, as this forces cantons to actually be in control and own the risks. If you separate it, you appear to spread responsibility.	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
Click or press here to enter text.	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
A lot can be learned from other confidence & trust upholding crisis management techniques. For example, the Federal Department for Health (BAG) has great expertise in leading through a public health crisis. The principles for the communication style will be similar, with some important differences pointed out below. **In addition, the Federal Chancellery may find it useful to consult its own experts in the Strategic Management Support Section. They are the centre of expertise at the Federal level, offering both crisis management training and logistical and methodological support and advice for supradepartementel crises. As any crisis in e-voting would touch upon actors from various departments, their expertise may be of use.** **There are some special considerations to take into account for voting:** **First, as voting is a political process, crisis management and response need to be political too (this cannot and should not be attempted to be done in a technocratic manner). There need to be clearly identifiable politically responsible officials (ideally elected officials), who are in charge of running the election.** **Second, for crisis management and response, it is key that the different stakeholders know one another and have built trust into each other's processes before the crisis takes place. This means all stakeholders (including voters) have to know in advance who is responsible and authorized to communicate about the status of the election/referendum. This includes trust building with all major parties and clearly defined lines of communications during a crisis, which ensures that the parties are constructively working with you, not against you.**	

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Ideally, all election officials of the cantons should be organized in conference, and link up to the election security and information security related elements on the federal level (govCERT, Melani/NCSC, BK, NDB). **Third, when you do spot disinformation or election meddling activities, democracy gives you a huge communication opportunity: if you are open and transparent with the electorate, voters can take such information into account when voting. Thus, it is democratically better to inform voters of your ongoing information before the election/referendum takes place, than to inform after the election about irregularities and thereby cast doubt on the legitimacy of the process/outcome (for a case study where this was not done, see the US elections 2016).**	
7.2	What are the right events and thresholds for an activation?
There needs to be a continual situation awareness cell that monitors the election environment. The cell should regularly brief the chief election officers (cantons/federal level), who should be able to trigger crisis management (political act).	
7.3	Who should be involved in crisis management, with which role?
This differs with which type of election it is. There should be a clear hierarchy and pre-defined & practiced roles.	
7.4	How should the communication be organised (internally and externally)?
See also answer to 7.1.	
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
Yes, see 7.1. (Ideally, all election officials of the cantons should be organized in conference, and link up to the election security and information security related elements on the federal level (govCERT, Melani/NCSC, BK, NDB).)	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
Click or press here to enter text.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
Click or press here to enter text.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
That would depend on the case.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
This is a political question that needs deliberation and acceptance by all stakeholders beforehand. It is also "the key question". I raised this in 1.1., and reiterate it here again: the trustworthiness of the system can be measured by how trusted/accepted its remediation procecesses are. If they are politically accepted, the system is trustworthy enough for the democratic elecetorate, if not, it should not be used, as it cannot settle political conflict, i.e. the key function it is designed to solve.	

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Tobias	**Last name**	Ellenberger
Organization	Swiss Cyber Experts (Vice President), Oneconsult AG (COO)		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

Most important questions

- **Registration and onboarding process: It is important to be able to understand how the onboarding (sending of the voting documents) and the process from registration to voting looks like. in the best case, a video will describe in advance what possible security gaps are and how to protect against manipulation. These builds trust. For me it is important to be able to understand what thoughts have been made about authentication and verification in order to be able to estimate the risks of a typical, known attack.**

- **Who maintains the system where the core application / database of e-voting runs? How many parties are inovled: Every single party involved must be trustworthy. If a party has a dubious reputation or obvious (own) interests, the statement will be weighed on the scales. Here it helps if the statements are independently confirmed by neutral bodies. It is also important that it is as easy as possible to prove that the parties involved can demonstrate their know-how (without marketing in the style of we are the best). In this case I would also research via the personal network and the Internet what the experiences, values and goals are that the parties involved live with the system and whether they are actively involved in various circles (security industry, evoting committees etc.) and whether they are involved.**

- **Who has access to code, infrastructure, hardware, software, building, etc.: it must be possible to understand how the secrecy of votes, the security of the systems, etc. is guaranteed. This includes, among other things, how risk management is carried out, how security gaps are handled, what the update concept, authorization concept etc. looks like. This is not only to be shown, but in the best case also to be proven. It is not necessary to disclose everything in the smallest detail, but sufficient for the general public, for technically interested people and researchers should have the opportunity to question the concepts etc. and to add comments. To this end, the fears of the public and reservations about relevant scenes (security) should be taken into account. It should be obvious that all aspects that contribute to security have been considered. In addition to the security of hardware, software, applications etc., physical security and the human factor should also be mentioned.**

- **How is information transported to the voter and back? What is the protection of data during the entry, transmission and storage of the vote. Furthermore, during opening and what is the process of destruction? Is it checked by an independent party to ensure that no conclusions can be drawn about the person? Is the description comprehensible and intelligible? Was a technology used which is known and considered safe or one which is generally considered insecure? If insecure: is a statement made on this?**

- **How is it ensured that the recipient of the letter (if the voter receives the documents by post, as in Switzerland) is actually the voter afterwards? (e.g. multi-person household, flat-sharing communities etc.) The idea behind this question is this: something "new" (voting over the Internet) should be better (faster, easier and above all safer) than the tried and tested. Example: Today it is not possible to verify who has filled out the ballot in a 5-person household (all are entitled to vote). This would be possible e.g. internet voting in combination with an electronic ID or similar. From this it can be concluded that "exclusively" modern technologies are used, and the system is well thought out - in the sense of additional security by using a new system.**

- **Which devices can be used by the voter and is it the same channel and system across the country? This information can help to estimate how well maintained a system is. If in a country several systems are operated in different ways, this means for me that several parties have to make the same effort. The fewer systems, the less vulnerable they are. The more resources are concentrated on one thing (one system nationwide) the more secure the system potentially becomes. Comparing the principle with the Cloud. The big cloud providers have a level of security that can hardly be achieved by an SME. A similar principle applies to the number of available devices/browser/systems which can be used. The more the use is restricted, the more precisely security mechanisms can be controlled. This is against usability. The more devices/browsers etc. are allowed, the higher the probability to find a vulnerable one that can be abused.**

- **How and by whom was the entire internet voting ecosystem examined and tested? (Four-eyes principle, transparency etc.) offers interested parties the possibility to verify if the system is used at other locations, if there were incidents (e.g. bug bounty) and if it was possible for a single person or party to make changes independently without anyone getting wind of it.**

- **Are tests (organizational and technical) carried out regularly, at least before each election, preferably continuously by different, trustworthy parties? provides an indication of how well maintained and managed the systems are and the level of security of the entire system. A system that can potentially be attacked every month (due to many elections) and therefore is under constant scrutiny is likely to have a higher level of security than a system that is only used for elections every four years.**

Most important answers to conclude, that internet voting is trustworthy

Should be answered at least (and from which source)

- **Process of Information handling internet voting <-> voter (federal government and/or canton, as well as test results from university and private company (experts))**
- **Risk analysis (federal government and/or canton)**
- **Protective measures (system owner and at least two independent neutral bodies such as universities and private companies over a longer period of time)**
    - **User (Clientside)**
    - **Transport**
    - **Internet voting ecosystem**
- **Audits / Assessments -> Transparency (system owner and at least two independent neutral bodies such as universities and private companies over a longer period of time)**
- **Response to security breaches (federal government and/or canton)**
- **Did a public discourse take place (system owner, canton, internet)**
- **Is it possible get in touch**

How does the origin of the answers influence the conclusion?

The origin of the information has a great influence on the formation of opinion. It seems most trustworthy to me if several independent bodies give the same answer on the same topic without conflicts of interest (e.g. security of systems, transparency maintained, security and meaningfulness of processes, etc.).

Under certain circumstances, a public-private partnership (established for this purpose) or a "Prüfstelle" composed of different actors.

Important actors:

- **Confederation/cantons (but have a vested interest in ensuring that e-voting works)**

- **Expert groups/associations that have been dealing with the topic for a long time or are important**
- **Universities with relevant research**
- **Private sector actors (individuals, companies) with relevant experience**

Pay attention to the qualifications or check and proof them. In my opinion the statement of the operator of the internet voting solution has no value. It should be noted that any "concealment" or "exclusion" of possibilities triggers an "I want to hide something" reaction.

Related to Switzerland (if the reference to Switzerland in the above text cannot be deduced)

Low hanging fruits:

For me it was not plausible that apparently the source code was checked by several parties, but the vulnerabilities in the code were first discovered at the PIT. This could be improved e.g. by a mandatory code review by different parties before each release. The PIT again shows that this is worthwhile, as no serious vulnerabilities were found in the application (as tests were performed intensively by various parties). The known researchers - who have discovered and reported real security holes - should be mandated and involved. Several companies should be accredited, including those with relevant know-how and no possible conflict of interest.

Further comments on the situation in Switzerland:

in contrast to the system used in geneva, the system used by the post office (scytl) cannot, to my knowledge, be fully installed and tested in its own laboratory environment in its current state. thus, important correlations are not apparent and the "public" is dependent on the trustworthiness and reputation of the testing companies. Trust in Internet Voting can be promoted by even more transparency

Given the situation, the question arises as to whether citizens do not have more confidence in a solution provided by the state than in that of a private company, which operates profit-oriented and also pursues other interests.

various tests / assessments have been carried out and partly published (but often by "only" one party). here, for example, every test could be consistently published (after correction of the findings) and the "4-eyes" or "2-party" principle could be implemented more consistently -> higher trustworthiness

Higher weighting of the factor social engineering and creating more awareness of where and how manipulation can take place. For me this also includes a more detailed explanation in the videos of the post office how manipulation is prevented in concrete terms. for example, it is shown that 4 people have the key to decipher the results. what if these 4 people belong to the same political party and decide to destroy the results? is not the best example, but I think there is still room for improvement in the area of education (although it is good from my point of view). This can also be done for postal voting, I think that internet voting will be more accepted if there are concrete use cases that show that electronic voting is more secure.

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEIeS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEIeS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEIeS in conjecture

with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
There are encryption methods, which are generally considered secure. The probability that these (if implemented correctly) become vulnerable or will be cracked in the foreseeable future is small to very small. Also, should this be the case, successors would already be available. It must be ensured that consideration is already being given to how to respond to this situation.	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
No answer.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
there is a risk that an employee of the print shop will record the codes and thus know the response codes of a voter. in this case, the functionality of the printing house should be limited as much as possible. generating them in the printing house increases the attack surface, since an additional system with corresponding functionality must be installed, operated and maintained at another location. Apart from decoding and printing, the printing house should not take on any additional functions. As soon as something is not traceable, verifiable and controllable, there is a possibility that trust in the process will decrease. this can be increased by control and transparency. Another possibility would be to automate the printing and mailing process as much as possible (done by machines) or to make sure that e.g. one person puts the codes (without personal data) and another person puts the personal data in an envelope for mailing (separation of data). If necessary, additional measuring instruments for control and security can be introduced, alone or in combination. e.g. check that employees do not take cameras, smartphones etc. with them, measure the average time for packing and monitor whether much more time passes somewhere (consequently someone tries to remember the data). however, it must always be considered whether this is the "biggest" problem in the process. Think the mass falsification of a vote (not just a single vote) is so difficult to do.	
2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are

	distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
Basically the model with the control components makes sense this way. The objection with the complexity is justified. The complexity is acceptable as long as it is controllable. In other words, as long as sufficient resources are available to maintain, update and monitor the various systems on an equal level. If this can no longer be guaranteed, the complexity must be reduced by reducing the systems. Basically, it is not possible to exclude the possibility of an attack that works on the different systems. However, the risk is much smaller than that it happens on only one system. On the other side (attacker) the complexity is higher, which requires more resources. It is important to make sure that the principle is not circumvented on another layer. the actual status can be maintained.	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
in general, i don't see any problem in this, as long as the software for verification is tested in the same way as the voting software. I believe that the measure that this software does not come from the manufacturer strengthens confidence in the system.	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
the approach is good, as long as the resources are available to maintain the corresponding hardware and software (see 2.1.4). otherwise, it is better to secure one system properly than to half secure different systems. the probability that an attacker will attack the application layer software, which is the same on all systems, is higher, since the effort required to find something is lower there (1. software itself was 2. greater probability of faulty execution of the software, since it must be compatible for several operating systems). Nevertheless I would stick to the status quo, because the more you can restrict where an attack is likely to take place, the more you can look at a place. Separation of duties should go as far as possible. wherever possible, the concept should be implemented. exceptions should be noted. here too, the challenge is with resources. The auditors' technical aids should be commissioned, tested and then used by independent, certified experts. If this is guaranteed, I see no reason to use different hardware and software.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-

	friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
Keine Antwort.	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
such errors can almost only be prevented if security is integrated into the development process. Principles for security by design must be taken into account. Microsoft SDL is the obvious choice. An agile development (as it is almost standard today) is a challenge for security. A concept could help here, where "always" or at very short notice, a qualified and reviewed team of experts from academia and industry is available to review the individual sprints or to advise the development on questions in the process and implementation and to review them again at (partial) completion. The final review of individual parts or the entire software is to be carried out by teams other than the expert team mentioned above. The prerequisite is complete transparency of the developer of the software towards the user and the reviewers.	

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
was a large-scale social engineering campaign being considered?	

I didn't think the scenario to the end, but it might be possible to launch help videos in a village/region, which refer to a fake platform and ask for all necessary information (login, verification codes etc), so that the attacker can vote for himself **Is the use of a zero-day vulnerability considered? (f.e. spectre/meltdown, heartbleed)** **or the compromise of a certification authority / path? (use of alternative infrastructure like the SCION project?**	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
no additional input	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
In the case of Switzerland, it is not clear to me how the manufacturer (Scytl) implements the required measures and has them inspected. I think that the error is to be found there. Whether the code, which malicious code was checked and by whom is not known to me. Also not where the different checkpoints are and how transparency of the CH provider can verify this. **Experience shows that hardware or software always has weak points over time. It is important to include security right from the start. To check this from the planning stage, through the production of hardware and software and in the manufacturing process and at the end. Depending on the threat scenario, the entire supply chain must also be considered. Just as important as secure development is the plan for dealing with weak points / errors, as well as how to react to them and how quickly they can be eliminated.**	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
I would not describe it as much better, but at least equal. There are different levels of security in banks and in e-health, critical infrastructures, etc. But the system is not worse. I think that if only the technical side and not the user is considered, the system can keep up with the secure systems. A comparison with banks therefore suggests itself that e-banking was also generally considered insecure at the beginning, but is now accepted. It should be noted here that part of the acceptance is that the banks will pay for any losses. There are also very few successful attacks on the technical level, but mostly on the e-banking user. For this reason, social engineering should be assigned great importance (see 2.2.1) **Comparison of cryptography: most systems (banks, e-health etc.) use the mechanisms that are considered secure. This is usually not the case in the banking environment (closed source). The trusted components approach, however, is only maintained by very few banks. Here, the assumed system according to VEleS requirements is certainly at the forefront in terms of security. Independence and protection from**	

trusted components is often given in the banking environment. However, the software can often not be verified in the banking environment. It should be noted that some banks write their software themselves and can perform appropriate checks. However, this is not visible to the e-banking user. **A comparison is therefore made more difficult by the fact that the measures mentioned in VEleS are often generic in analogy to ISO. It is not clear how exactly the implementation is done. A measure can be implemented more securely or less securely. This should also be examined on a case-by-case basis and then compared.**	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
I estimate the risk of fraud to be equal to that of internet voting as in 2019, and postal voting. In my opinion, the trust of the voters in people who count a ballot box is greater than if "any" computer does it. A big advantage for internet voting could be the combination with E-ID, because then it could be technically ensured that only one person opens the envelope. However, there is still some way to go before E-ID is rolled out and the additional difficulties (decoupling of vote and E-ID) can be guaranteed. **(Successful) large-scale attacks will mostly be carried out by states, or by globally organised interest groups, because - if the system is securely established - it will require significant resources. Based on experience, the attackers always take the easiest way, which is difficult to predict. But mostly the same tactics are used (-> Mittre Attack Framework, NIST). Parts of this are social engineering and the exploitation of (un)known vulnerabilities. For governmental actors in particular, attention should be paid to (hardware) backdoors and purchased vulnerabilities that are not yet known. do you only want to prevent the election? do you want to falsify the election? do you want to influence the election?**	

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or dis-

	played incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
If Internet voting is new, there are probably many voters who report inconsistencies for various reasons (e.g., proving that it is not secure). Once the process is established (see e-banking), people become negligent. As with other "technologies", the "yes-click" syndrome and a certain indifference will take over. Comparable to the unread sharing of blogs / tweets etc. in social media. **The only way to prevent this, in my opinion, is a continuous awareness campaign and the "slight" change of the appearance / movement of the buttons to keep the voter always alert.**	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
The fact that some people don't do this is again demonstrated by e-banking, despite the fact that banks and groups such as EBAS or SISA are constantly launching new awareness campaigns. Often such attacks are difficult to detect because they are combined with social engineering, and the fraudster points out to the victim that the certificate is "green". **Here it would be more effective to switch to an alternative, more secure technology (-> SCION project). Otherwise, an additional reminder can help, which during the process or before the final vote is taken, indicates again whether the certificate has been verified.**	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
Keine Antwort.	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
Quantum computers should be monitored, especially in the area of encryption, and research should be monitored in this area. They will primarily be used by large, global organisations and by states. There are places that record / store all data today with the hope of being able to decrypt them later - when the appropriate equipment is available. In order to keep an eye on the current status, an exchange with the companies involved should be maintained regularly (e.g. Google, IBM).	

In order to guarantee the security of the data, it should be stored on another, inaccessible system and locked away safely to prevent the risk. **Difficult to say, when quantum computing will be ready.**	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
The voters themselves have an important, if not the most important, influence on whether or not election fraud can take place. This is where the usual instructions, such as those issued by MELANI, help. **The connection with the unencrypted filing of votes is something I am not sure about at the moment.**	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
I don't think this will have any impact because voters today are just as susceptible to vote-buying.	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
Important criterias are: **Trust, reputation of the person/company, objectives/goals of the person/company, ethics of the person/company, experience in similar issues, professional experience,**	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

approach, background, network, transparency regarding price, ownership and expertise, and education.

Testing should be based on international standards (ISO, NIST, CC, CIS) taking into account regional working groups (ENISA, BSI) or more in-depth "de-facto standards" for specific topics (e.g. application security - OWPAS, Microsoft SDL).

The chapters from ISO 27002 (from physical security to the human factor), each supplemented by specific standards, are recommended as a basis. It makes sense to have all points checked by the respective experts. These can be different experts per test point.

3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.

an evaluation system should be deposited to answer such questions. this can be combined with risk management. As a general rule, unfulfilled requirements should not be accepted unless the consequences of this vulnerability can be accurately assessed, mitigated and monitored. if the risk can be clearly limited, acceptance may be possible for a very limited period of time. this period of time should, if possible, include no choice.

Example:

- Perfect Forward Secrecy (PFS) is not implemented in a function (PIT Finding) -> can be clearly limited, implementation may be difficult or not sensible. Can be accepted, provided this is corrected

- Heartbleed: not foreseeable (at an early stage) what exactly is at risk. Influence on security of data transmission and more -> cannot be accepted.

CVSS Score can help with categorization, but the calculation of the score would have to be adapted to the topic e-voting.

It should be noted that certain "uncritical" findings may have to be accepted due to system or application reasons. In such cases, mitigating and monitoring measures should be taken to enable a rapid response in the event of misuse.

3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

Yes, the credibility of the result depends very much on the organisations chosen.

The organisation that carries out the audit will always be critically reviewed by certain parties. For this reason, two different organisations with different backgrounds and characteristics should, if possible, be commissioned to avoid conflicts of interest. Certain organisations with a corresponding reputation cannot be avoided. Also, a potential conflict of interest can probably be found almost everywhere, if the search is long enough. At some point, the possibilities are also limited.

Example infrastructure (penetration tests):

There are well-known companies in this field in Switzerland / worldwide that can be called in. The really good ones are accepted by most groups in the security scene. However, this means that these companies will probably work with the e-voting provider from the outset. -> potential conflict of interest, which is almost impossible to avoid.

Example Source Code Review

Specialists from as many different fields as possible should be consulted (university, private sector, other specialists). Here it is important that institutions are involved which are considered "the specialists", but also those which have a brand (e.g. Big4) and carry out research or expose themselves to this topic accordingly. In this case, it is best to set up a group (PPP) which will accompany the topic over the long term, publish on it and thus build up a trustworthy reputation.

3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?

The depth of testing should be as high as possible. ISO (superficial, leaves a lot of room for manoeuvre) and BSI (sometimes very clear instructions) complement each other well.

3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?

Testing should take place regularly, depending on exposure. Example:

- The infrastructure should be continuously scanned for vulnerabilities (vulnerability scanning)

- Attack attempts / more detailed examination when serious security holes become known or during major upgrades of a system / application

- Segregation of Duties / process should be checked before each election

- a detailed overall audit every year.

3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?

regular panels should be held where demonstrable experts are given space and time for discussion. Results can be published in each case. it should be noted whether anonymity is granted or not. Exponents can be invited. it should also be published if they refuse to participate.

3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?

No answer.

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons

agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
Parts of the source code (e.g. verification, login, encryption) that are of public interest could be made available to everyone without registration to leave no doubt. If necessary, benefits can be linked to the registration (Q&A or similar) **For critical parts (where property rights or similar apply) registration and proof of qualifications could be required. Communicate the reasons for this transparently. E-voting Hacking Days" could also be organized where the complete infrastructure is simulated and qualified participants can try attacks without any restrictions.**	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
The dependencies of systems / functions should be visible. However, complete traceability requires disclosure of almost all documentation, which is probably not desired by the operator. Here the way could be taken that qualified on demand receive appropriate documents. The added value must be weighed up whether this is actually available.	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
No answer	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

No answer	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
Regular events can be held where questions from the public are discussed. Anyone can attend and participate in the discussion under certain rules. The most burning issues can be selected on the basis of a rating to be defined (e.g. hits, trending in social media etc.) **A new unit (Public Private Partnership?) could be founded for the topic internet voting. This could also be used for other topics that affect all citizens (E-ID). Otherwise, the one federal agency (NCSC?) could also accept it.** **If possible, all stakeholders should be involved in the discussions so that it is clear how diverse the topic is and what interests need to be taken into account. At the very least, these are the Confederation, the cantons, universities, the economy, experts, guests, topic-related exponents.**	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
For the purpose of transparency and in order to create trust yes. a channel should be defined for communication. it is suitable, for example, a dedicated website/feed, which then automatically uses the most important channels so that everyone can inform themselves easily (social media). It is important to ensure that any further security gaps linked to the vulnerability or resulting in combination are also eliminated.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
it has been proven that critical vulnerabilities have been discovered through the PIT. a bug bounty program is almost a part of the good reputation today and shows that there is nothing to hide. it is important to note that a bug bounty program does not replace a detailed, mandated assessment because a) bug bounty programs are limited in scope and b) the quality of the people participating in them cannot be verified. As a supplement, however, it makes sense. **The restrictions can be relaxed a bit, but the tests must still be conducted. Thus, the possibilities of social engineering attacks are exciting to experience and measures can be derived from them. Other things (e.g. DDoS) are not worth testing, because they always work if enough resources are spent on them.** **As a reward money is probably the best. Many people in this area are satisfied with money, fame and honor.** **For certain tests without restrictions (or with very few restrictions), for example, "hacking days" could be held, where everyone with sufficient qualifications is invited, but the whole thing takes place in a protected environment.**	

Limited tests / bug bounty (e.g. on the infrastructure) do not necessarily have to be limited in time. The infrastructure has the claim, if available / reachable, to be safe.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
No answer	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
No answer	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
No answer	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)
In my opinion, transparency always helps to strengthen trust in a system. As long as no rights or public interests are infringed and the law permits this. In this way, transparency was to be created where possible.	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
No answer	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation?

	1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
The participation of independent experts could work even better if the organisation of the cooperation is "outsourced" (e.g. PPP) and not carried out by the Internet voting operator. Under certain circumstances, long-term cooperation with universities on the subject could be developed. An additional review body could be created, which is once again independent of the PPP. **The committees could then look like this:** **- independent PPP with certain tasks** **- Testing institute which critically examines the work and investigations of the PPP and carries out independent checks.** **The PPP is independent, the testing institute is attached to the BK, for example.**	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
Besides a non-disclosure agreement and a vulnerability disclosure policy, there should be as few hurdles as possible.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
No answer	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
No answer	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
the events and activities should be organised through the PPP. alternatively, I think the BK is a good place to be. **The further answers to the question can be taken from the previous answers**	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
Risk management should be based on ISO 27005. The risk analysis should be reviewed at least every six months and updated if necessary. The input for this are **- scientific evidence** **- Insights from the current threat situation (MELANI, GovCERT, media etc.)** **- Insights from PITs and events** **- Changes in the environment** **- Research** **It should be possible to obtain the information actively through cooperation. The risks should be examined in detail on an annual basis, provided that the resources are available**	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
Advantages: **- creates trust** **- Possibility to receive input from the general public** **- fresh perspectives** **Cons:** **- someone who sees what's been forgotten doesn't point it out and take advantage** **- enables criticism and thus ties up resources** **- can promote mistrust in the sense of so many risks that cannot all be considered**	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?

This is almost impossible to achieve by the cantons due to their authority and limited resources. here, it is sometimes necessary to rely on disclosure and the opinion of experts. **It is possible that there will soon be testing institutes on this subject, which may also create a legal basis for addressing this important risk.**	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
Criticality **Urgency** **Impact** **Costs / Benefits** **Feasibility**	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
ISO 27005 **NIST Cybersecurity Framework / RMFNo**	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
The PPP mentioned several times. A committee of experts can be formed in it. Otherwise, representatives familiar with the subject from **- Federation** **- Insurance** **- Economy** **- Research / Teaching**	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?
No answer	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton’s processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
Ideally, a neutral and an organisation-specific (whether operator or canton) risk analysis is carried out. in order to exploit synergies, a body created for this purpose could take over both. Otherwise, independent providers can also be chosen, but the results must then be submitted to a kind of audit, which checks whether consistency etc. is guaranteed. This "revision" could then also exclude providers if the quality is not right.	

6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
No answer.	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
No answer.	
7.2	What are the right events and thresholds for an activation?
No answer.	
7.3	Who should be involved in crisis management, with which role?
No answer.	
7.4	How should the communication be organised (internally and externally)?
No answer.	
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
No answer.	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
No answer.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
No answer.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Click or press here to enter text.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
Click or press here to enter text.	

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Bryan	**Last name**	Ford
Organization	EPFL		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

Some questions I would ask, discussed in more depth in the subsequent answers below:

- **Have relevant and diverse (international and local) experts been involved in the development, evaluation, and deployment of the e-voting system continuously from as early in the formulation and design process as feasible?**
- **Are all trust-critical elements of the system, "end-to-end" from the voters' devices all the way to the back-end "control components", web servers, PKI servers, etc, operationally open and transparent, so that relevant experts and the public alike can verify the entire system's operation in its deployed form (or find/hire their own choice of authorities to do so)?**
- **Is the open and publicly-available documentation for the system complete, and available at multiple levels of detail, ranging from a brief high-level summary accessible to almost everyone to detailed "line-by-line" specifications adequate to convince the world-leading experts (if perhaps accessible to not many people other than them)?**
- **Do all trust-critical elements of the system, "end-to-end", ensure diversity at all levels (e.g., software, hardware, firmware, human administration) and avoid any single points of failure or compromise? Or are there still major elements of the system, especially elements that must be "blindly trusted", such as a trusted printing service or trusted postal system?**
- **Have all the realistic risks and threats anticipated by international e-voting and security/privacy experts, including coercion or vote-buying threats, been adequately considered and addressed in the design – even those risks that might seem low or politically non-critical in the country in question?**
- **Does the software development, build, and deployment pipeline in particular embody a fully transparent, open-source, no-single-point-of-compromise development pipeline as prototyped for research purposes in the CHAINIAC architecture (Nikitin et al, USENIX Security 2017) for example?**
- **Has some systematic architecture been put in place for the deep analysis and quantification of software/hardware/adminsitrative diversity, dependencies, and correlated failure risks been put in place, as discussed in Independence-as-a-Service (INDaaS) (Zhai et al, OSDI 2014) for example?**
- **Has an "N-of-N-version programming" and bug bounty effectiveless amplication framework framework been put in place along the lines of the Hydra framework (Breidenbach et al, USENIX Security 2018), to make effectively-large bug bounties affordable and incentivize responsible disclosure?**
- **Have not only relevant experts, but the public itself – or at least a study/focus group composed from a statistically-representative sample of the public – been involved in the requirements-setting, design, validation, and public messaging throughout the e-voting system development and deployment process? For state-of-the-art examples of ways to involve public representation in democratically representative and legitimate but cost-effective ways, see for example the works of Yale political science professor Helene Landemore, and Stanford professor James Fishkin on deliberative polls.**

In the Swiss case, I see many important positive features and developments already (e.g., the split-trust control components at the back end, the expectation of "cast-as-intended" vote integrity verification across multiple independent channels starting from the voter, the requirement of a certain degree of code openness, the requirement of universal verifiability for maximum deployment, etc.). However, I also see many opportunities and needs for improvement in both the short and longer term, including many of those items mentioned above and discussed in more detail in answer to the questions below.

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent,

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
I do not believe that a sudden undetected break in the cryptographic building blocks is very likely, provided those building blocks are being used correctly in a sound design and correct implementation. I believe that slow erosion of the cryptographic building blocks (e.g., eventually compromising vote privacy due to gradual cryptanalysis improvements and/or eventual development of practical quantum computers) is a more significant, but also by definition much more forseeable, risk area. Another high risk area of course is flawed use of the cryptographic building blocks in design or implementation.	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
I am fairly confident overall design of the current Swiss E-voting protocols achieves its intended goals according to its stated trust model, and has been in most respects adequately specified and independently analyzed by multiple competent parties at the design level. In this respect, I feel Switzerland is technologically far ahead of almost all other countries in the world that have deployed or considered deploying E-voting. My larger outstanding risk concerns are more with the concrete software implementation of the protocol, with the highly-centralized validation and deployment of the protocol with limited public transparency, and with what I see as several major latent weaknesses in the chosen trust model itself.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?

In general, this is one area in which I have major concerns with the adopted trust model itself. The assumption seems to be that anything in the E-voting process that uses paper can simply be assumed to be a perfectly-trustworthy abstraction, requiring neither transparency nor internal verifiability, in contrast with the electronic parts of the E-voting workflow.

This assumption flies in the face of the fact that all the cost-efficient modern methods of producing and handling paper in large quantities, as needed in elections for example, unavoidably depend on numerous electronic, computer-assisted, networked and even Internet-connected devices, many of which we can be almost certain have many latent and potentially-exploitable security weaknesses. State-of-the-art printers are almost always networked, require software updates, etc. The trusted images to print must be generated on other general-purpose computers at the printing authority, run by people who must in turn be blindly trusted, and which send the trusted images to the trusted printing devices over an internal network (hopefully not the Internet!) that must in turn be blindly assumed to be trusted as well. Thus, simply assuming the printing service is trusted effectively brings an almost-certainly-enormous amount of opaque computing and networked infrastructure – likely comprising most of the printing service's operational network – into the E-voting system's trusted computing base, and subjecting the entire E-voting system to potentially-undetectable tampering via a compromise anywhere in that printing authority's complex hardware/software/network infrastructure. To me this assumption of a trusted printing authority thus constitutes a huge and underappreciated risk.

Another closely-related and I believe underappreciated risk is in the Swiss voting system's assumption that the postal mail service is likewise an opaque but blindly-trusted abstraction. Modern mail-handling systems are extremely complex and opaque proprietary systems full of computers and networked interdependency of numerous forms, and it would be a huge surprise if they were truly secure. Placing the entire postal service in the blindly-trusted domain opens the system to a huge array of potentially scalable and difficult-to-detect attacks, such as a foreign influence using remotely-hacked mail-handling systems to misdirect a random percentage of ballots coming from jurisdictions known to vote in "undesirable" ways to an attacker-injected destination, where the ballots might be silently destroyed (e.g., buried or burned) or simply be delayed until after the election deadline.

The risks get even more concerning when one considers possible collusion between compromised or hacked elements within the trusted printing office and the trusted postal service.

Of course whenever generation of cryptographic parameters is concerned, it is always useful if the generation of those parameters can be made more transparent and verifiable rather than less. But the difference in security one way or the other will probably be minor, when the (many other) main functions of the trusted printing office (and postal service) in the E-voting workflow are inherently opaque and unverifiable in design.

2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?

Requiring that trust in the control components be split is an extremely important and valuable step forward, and should definitely be retained and built on further. This step is necessary but not sufficient to make the control components truly trustworthy enough, however, from my perspective.

Requiring software diversity in the implementations of the control components would be another valuable and important next step, to reduce the risk of a single software bug rendering all four control components simultaneously and identically vulnerable to the same exploit. The multiple software versions should be written in multiple distinct programming languages by independent teams In the longer-term path toward real security, this will be another necessary step but still not sufficient. This multi-

version software will inevitably be costly, but the costs can be mitigated in various ways – such as by having some asymmetric participants play "verification-only" roles for example, as discussed below, or by leveraging the software diversity to reduce the cost of funding adequate bug bounties also discussed later.

A further necessary (but still not sufficient) step is to consider and ensure the diversity of the complete hardware/software stacks underlying the collectively-trusted control components. The language runtimes, operating systems, hardware platforms, processor architectures, etc., should be chosen and evaluated for diversity as well. This is especially true for the hardware platforms, which in today's technology still tend to be mostly-proprietary and necessarily opaque and unverifiable, in contrast with operating systems and language building blocks, for which open source options generally exist. The fact that increasingly-severe exploitable bugs have been found with increasing regularly in the system management devices built into hardware platforms, the non-patchable hardware ROMs, etc., further underlines the critical need for hardware platform diversity supporting the control components.

A further necessary step in this direction will be to make the diversity of not only the voting software - but also the underlying hardware/software platform – sufficiently transparent, risk-quantifiable, and publicly verifiable as well. A short-term "baby step" along this path would be for some of the control components to make use of trusted hardware attestation features (e.g., Intel SGX and equivalents from other vendors), so that it is publicly verifiable (at least given trust in the hardware vendor) that the control component platform is running exactly the binary software image(s) it is supposed to be running. However, utilization of trusted hardware attestation features like this must supplement, not replace, the diversity considerations above. It is much better for just one control component to be running in an attested SGX enclave with the others exhibiting other diverse implementations, than for all four control components to be running in SGX enclaves but lacking software or platform diversity.

In the long term, there must be quantifiable and automatically-checkable criteria for evaluating the diversity of the control components, which can identify and reveal subtle correlated failure risks that may subtly compromise the diversity. For example, while there are multiple open source and proprietary operating systems from which to build platform diversity at the software level, many of these might use exactly the same implementations of certain trust-critical libraries – such as the OpenSSL library that the Heartbleed vulnerability brought significant attention to. The deep choices of which specific libraries and other swappable components each control component platform is using need to be part of the (eventually partly-automated) diversity analysis, so that any such common-mode failure risks can be identified and corrected.

This objective of platform diversity transparency and public verifiability need not mean that every component choice and piece of software in the control components must necessarily be open source or publicly verifiable. For example, there may be reasonable argument that some or all of the control components should include certain some secret/proprietary software for intrusion detection or analysis, which should (arguably) be secret precisely so that an attacker who finds a critical exploitable bug in the open source part of the system does not have complete information with which to execute a perfect and undetectable attack. However, even if the presence of such deliberately-secret components might be justified, the control components should be architected in such a way that the proprietary components need not be trusted by the public or by independent expert evaluators. That is, for a control component to be effectively secure, it should be sufficient either (a) for all the open and publicly-verifiable parts of that control component to be secure and bug-free and all the secret/proprietary components to be fully compromised, or (b) for the open

and publicly-verifiable parts of the control component to be imperfect but the secret component successfully detects or prevents an attack or vulnerability in question.

For some further technical background on diversity analysis and publicly-transparent verification processes like this, please see for example the research of Ennan Zhai (Alibaba Research), such as: "Independence-as-a-Service" in OSDI 2014; "An auditing language for preventing correlated failures" in OOPSLA 2017; and CloudCanary in NSDI 2020.

Of course the full platform diversity and transparency evolution path sketched above will inevitably be expensive and take many years, perhaps decades, before it can be fully completed. But in the near term, the current E-voting system design and evolution plans need to recognize those long-term necessities and be placed on that path.

2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?

I see a great deal of added value in developing diverse verification software - not just written by a different provider but ideally in a different language and with different dependencies, e.g., different underlying cryptographic libraries as well. I see particular varlue in this path in the shorter term, before independent implementations of the full control-component stack may yet be feasible economically or logistically, because verification-only software can likely be much smaller and simpler than the full stack, and hence more realistic to develop independently in the near future.

As a closely-related opportunity, I think that at least one such independent verifier software implementation should be built with a full mechanically-checkable proof of correctness, e.g., using a theorem proving system like Coq or Isabelle. While creating a mechanically-checkable implementation of a full e-voting software stack might remain impractical or economically unaffordable for a number of years yet, building a mechanically-checkable formally-verified implementation of only a cryptographic proof verifier may be feasible and economically viable much more quickly – perhaps in six months to a year. This would be an extremely valuable step, even if the diverse implementation (and eventually machine-checkable verification) of the entire control-component stack remains critical and must also remain on the longer-term roadmap.

2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?

I guess I already answered the first part of this question above: yes, it is extremely critical for the operating systems and hardware to exhibit diversity.

Other machine components that could embody significant risks include GPUs or other accelerators (if incorporated in order to accelerate the cryptographic tasks for example); system management controllers of any kind whether integrated into the plaftform's chipset or implemented externally; and even attached peripherals such as disks.

For example, suppose all four control components are extremely diverse in hardware and operating systems otherwise but use the same type of disk, which proves to have an exploitable firmware bug. An attacker might be able to exploit that bug (somewhat

differently in the case of each control component due to the different operating systems etc) to plant a hard-to-detect boot-time rootkit on each of the control components. Proper use of disk encryption, boot-time security mechanisms, and/or trusted hardware attestation mechanisms of course can reduce such peripheral-related risks. But most hardware platforms were designed generally around an assumption that peripherals (especially high-performance ones) are usually trusted, meaning that a common-mode vulnerability in a common peripheral could create significant risk even across otherwise-diverse control components.

In any case, the general threat from system management hardware components needs to be taken extremely seriously. Since built-in system management hardware usually comes from the processor/chipset vendor, it should generally be easier to get diversity in this respect provided the control components have the diversity of different processor/architecture vendors in the first place (e.g., AMD, Intel, ARM, RISC-V).

2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?

Users routinely store all kinds of highly-sensitive personal information on their smartphones and other personal devices, including such things as intimate photos, whose privacy they may often in practice care about even more than how they vote – perhaps for good reason. The problem of hacked intimate photos being used for revenge porn is already a demonstrably serious problem fairly widespread in the public's consciousness. Similarly, much other personal information that can often be found on personal devices tends to be useful for, and frequently used for, attacks such as identity theft or cryptocurrency wallet theft. Thus, without discounting the importance of both the integrity and privacy of votes, it may be safe to say that the average voter spends much more time worrying about the security and privacy of other personal information on their devices – and yet still uses them and stores this highly sensitive information on them, because the convenience is so irresistible.

Thus, it certainly seems reasonable to assume that voters can and reasonably do make decisions to trust certain devices. Whether these decisions are well-considered is another matter, of course, but voters are gradually becoming more aware, educated, and careful in this as well. For example, users have been gradually and increasingly adopting practices of keeping their software up-to-date for example (or at least opting in to vendors' automatic update mechanisms). These are practices that an E-voting system provider ultimately cannot control, of course, but the general

trend towards both users trusting devices, as well as becoming more aware of how to keep their devices reasonably trustworthy, seems to be progressing.

An E-voting system should not just assume that users always make good trust decisions, of course, or that users will detect a compromised device without help. If only one of a user's devices (i.e., the same device the user cast the vote with) is able to verify the encrypted vote posted on the public bulletin board, then I would consider that a serious weakness and security risk. Since many people tend to use the same popular devices, a single exploit in such a popular device could present a foreign adversary the opportunity for a quite scalable and perhaps nearly-undetectable attack against the entire class of users with the compromised device or software version.

Thus, I think the device diversity goal should apply just as much on the voter's personal device side as on the control-component back-end side. It is increasingly common and even routine for users to have multiple devices of different kinds (e.g., a smartphone, a tablet, a laptop. A future E-voting system should allow users to use one device to check the correctness of the votes they cast on another device. Of course this will not apply to all users: some will have only one device (or be willing to trust only one device with their vote privacy).

The threat posed by vulnerable personal devices increases with devices that are not (sufficiently) well-supported by the vendors with regular security updates. The risk also increases in proportion to the popularity of the device and operating system in question, in that an attacker who exploits one flaw in the device or operating system has a chance to scale the attack to a larger voter population at once (potentially without detection if the attack succeeds in remaining stealthy). A reasonable precaution might be for E-voting software running on the device to check the device and operating system on which they are run against a list of known devices and/or operating system versions known to be both common (popular) and vulnerable or poorly-supported by their vendor, and to recommend (or even require) the voter to upgrade the operating system or device as appropriate before using it for E-voting. The usability costs of such personal device validation or blacklisting measures must be weight against the expected improvements to security and vote privacy, of course.

A special-purpose device such as a smart card or YubiKey-like dongle with a small display capable of confirming that votes are cast-as-intended independently of a (single) main voting device is also a promising option to explore – but even if implemented, I don't think such a device should be considered universally trusted or required for all voters to use. It should only be "one of several" second-channel alternatives for vote integrity checking, and the mechanism should be architected so that multiple vendors can produce such devices, limiting the risk if a serious zero-day exploitable flaw exist in all the devices of a particular type or version from one vendor.

In any case, I personally think that a multi-factor vote integrity-protection architecture based primarily on multiple client-side device channels, with appropriate diversity, would be much more secure in the long-term than universally relying on the postal service as a blindly-trusted channel for vote integrity protection. (See considerations above about the weaknesses of treating the postal service as trusted.)

2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure

	that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?

The most important measure that needs to be put in place is a policy to encourage, or even require, an open process in the development and progressive testing, evaluation, and hardening of the E-voting software and system. International experts need to be involved early on and periodically throughout the development process, with regular independent peer review and "red team" testing, initially focused on units and gradually expanding to the whole system.

Establishing such an expectation of openness and regular independent peer-review will help the process and outcome in multiple respects. The main software development team will have the benefit of getting feedback much earlier and more regularly, and more likely avoid the trouble and embarrassment of major flaws being discovered only at the end when everything is supposedly complete and "certified". Regular independent code peer-review will also help the development team increase the quality and clarity of the software itself, by establishing a culture that every line of code a developer writes must not only "work" but must be extremely clear to multiple independent reviewers who they know will definitely be reading it, must match up in an extremely clear and obvious way (ideally "line-by-line") with the corresponding specification document, etc.

And finally, keeping independent international experts in the loop throughout will hopefully help ensure that those experts have reached some "buy-in" to the quality and utility of the result, have a deep understanding of the system and the reasons it was designed the way it was by eventual release, and can help explain those decisions, tradeoffs, and ultimately the reason it should be considered trustworthy enough, to the public upon final release.

If flaws are still found after release (which some probably will be), they will almost certainly be less severe or disastrous, and it will be much harder for critics to claim that the government has rushed to deploy half-baked technology without sufficient care for security.

The above considerations focus on the development process, but the deployment process is important too of course. As discussed earlier above, the use of trusted hardware attestation technologies such as Intel SGX to make it publicly verifiable (assuming appropriate trust in Intel and SGX's security) that a given control component is indeed running the exact software image that it is supposed to be running. And similar "trusted boot" facilities can and should be used to help ensure that it is running the correct operating system, and ultimately the correct entire software stack.

Between development and deployment is the issue of correctness and public verifiability of the development toolchain (compiler, linker, etc) and the correct and publicly-verifiable transformation of given software source code to a given binary image to be deployed. This addresses the issue that Ken Thompson famously spoke about in his Turing award lecture, "Reflections on Trusting Trust": how do you know that a compromised compiler has not inserted a back-door between the correct and certified source code and the binary that will actually be run? To secure this part of the software pipeline, the software process should adopt deterministic build practices as the Debian Linux distribution has been adopting, and should incorporate independent deterministic build and automated cross-checking and witness-cosigning techniques as laid out in my DEDIS lab's CHAINIAC work (USENIX Security 2017).

In these processes, academia can and should play multiple roles. Academic institutions can help review and vet software designs, of course, and perhaps sometimes

(parts of) implementations. Line-by-line detailed code analysis is perhaps better done by dedicated industry experts working on a contract basis, who must have the appropriate (especially cryptographic) expertise. Both academic and indepependent industry or non-profit players could also assist in various offline- or online-verifier or observer roles, for example, running independent deterministic build servers to verify and attest to the correspondence between a certified source image and a binary to be run on a specific control component, or to run witness-cosigning servers that monitors and independently verifies the operation of the main control components.

Academic institutions should not be expected or required to run "24/7" high-availability services with continual support, but a well-designed deterministic build pipeline or witness cosigning architecture need not and should not depend on each such independent server being highly-available in any case. The main system still can and should continue to function and remain available even if some (or in the worst case all) of the witness cosigning parties were to become unavailable at a critical moment, which would merely reduce the attestation and public transparency level during that period, rather than interrupting or compromising service.

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?

Criminal organization or foreign adversary infiltrates the trusted printing office (physically, socially, or electronically) to exfiltrate the codes on mailed voter cards and compromise cast-as-intended security.

Criminal organization or foreign adversary infiltrates the trusted postal service (physically, socially, or electronically) to misdirect some percentage of ballots from selected neighborhoods to an alternate address where they are held or destroyed.

Criminal organization or foreign adversary offers a potentially-large number of voters money or cryptocurrency in exchange for installing malware or spyware on their devices, which verify that the voters cast votes the way the adversary prefers (large-scale electronic vote-buying or coercion). An adversary could even carry out such an attack with almost complete anonymity with appropriate use of cryptocurrency and smart contract technologies: for further discussion see Juels et al, "The Ring of Gyges: Using Smart Contracts for Crime" (http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf).

Compromised web server or App store serves a compromised version of the voting Web app and/or native apps to users.

Compromised certificate authority, code-signing certificate, or developer signing keys used by an adversary to produce correctly-signed but compromised versions of the voting Web app and/or native app to distribute to users.

Network denial-of-service attacker prevents (targeted) users from casting votes electronically, forcing them to fall back to the mail or in-person process, in the expectation that many targeted users will give up and not vote at all due to the inconvenience. A network attacker who can disrupt the vote-casting process at the "critical moment"

after the codes have been received but before the electronic vote has been confirmed would be particularly effective, since the voter cannot try again in this case.	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
All potential single points of compromise in the end-to-end voting process must be identified and addressed however feasible. This means any single device, human, or organizational role that by acting alone could compromise election integrity or voter privacy, especially if in a scalable fashion. **Potential single points of compromise include not just the control components and voters' personal devices, as discussed above, but all their trusted dependencies. For example, this includes common processors, operating systems, or libraries used by most or all of the control components or user devices (see diversity discussions above). It includes any public key infrastructure (PKI) dependences in which a single compromised "root" or other certificate could allow an attacker to impersonate multiple control components or many voter devices, for example. It includes any centralized government web servers that provide information and/or a Javascript-based voting Web app to voters. It includes centralized vendor-provided App Stores that could potentially serve compromised versions of a native voting app to a large number of users without detection. Transparency techniques such as witness cosigned apps and updates (e.g., see discussion above and CHAINIAC paper) can help address these later threats without giving up the convenience of Web apps or vendor-provided App stores.**	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
While I understand the reasons for excluding coercion resistance as a requirement in the Swiss case (e.g., the known difficulty of achieving coercion resistance combined with the fact that the Swiss "base case" of postal voting does not achieve coercion resistance either), nevertheless I feel that coercion is a large and underappreciated risk factor in the Swiss e-voting system that must be addressed in future designs. Even if coercion is not currently a major concern in the political or regulatory communities in Switzerland, one of the key responsibilities of technical experts in domains such as e-voting is to bring to policymaking circles increased awareness of not only technological possibilities but also technological risk factors that may currently be underappreciated – and I strongly believe coercion-resistance falls into this category of risk. **For example, while it may be true that there is no evidence that actual coercion or attempts at coercion or vote-buying is prevalent in Switzerland, neither does there seem to be solid evidence that it is not – or any reliable statistics at all – because the country has not even invested in enough systematic researcher on the question to have a solid evidence-based understanding of how large or small the real threat may be. I have heard anecdotes about whole villages in Switzerland in which the "village elders" traditionally get together before each election and decide how everyone in the village is going to vote. I do not know whether these specific anecdotes are true or any further details, but they are concerning to say the least. It may not matter much**	

in practice whether such coercion occurs by the coercer outright capturing and casting ballots on behalf of the voter, or by vote-buying of some form, or merely through pure psychological intimidation. While Switzerland's law-abiding culture certainly seems to make it less likely to be a highly prevalent problem than in many other countries, nevertheless incidents such as the recent McCrae Dowless postal voting fraud incident in North Carolina should amply illustrate that even advanced, mature, and supposedly-stable democracies are not immune.

Partly for the reasons discussed earlier about the major latent vulnerabilities that the current Swiss e-voting system inherits through its dependence on the postal service as a blindly-trusted abstraction, I feel that it is not adequate for the Swiss e-voting to target security ONLY "as strong" as the prior postal voting system, because that level of security is simply not strong enough especially in today's world. For similar reasons, the fact that the baseline postal voting system does not achieve coercion resistance is not sufficient reason to conclude that E-voting designs need not address it either.

For one thing, E-voting presents opportunities for much more scalable, cost-effective, and anonymous attacks by resourceful criminal organizations or foreign adversaries than postal voting might traditionally have presented. For example, the the fact that personal devices can often be turned into instruments of mass surveillance in many ways, either with or without the knowing cooperation of the voter. Consider for example the "Dark DAOs" scenarios that Juels et al discuss in their paper "The Ring of Gyges" mentioned above, where a criminal organization might create a smart contract living on a decentralized system like Ethereum, which is funded anonymously and effectively untraceably to any real-world actor, but which offers (say) Swiss voters some amount of money (cryptocurrency) in exchange for installing spyware that monitors their E-voting behavior to confirm that they are voting in the way the mass vote-buyer prefers. While not seen so far, such attacks could be both scalable and extremely difficult to trace or shut down in the future.

2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).

Yes, provided the E-voting system's end-to-end verifiability and other security/privacy provisions are well-designed and properly-implemented, I would definitely agree that the system's protection of cast vote integrity and privacy is already significantly ahead of the protection of that of sensitive personal data in many other fields including banking, e-health, etc.

However, this is not a complete story, in part because protection of the votes cast themselves are not necessarily the only privacy-sensitive information in practice in an E-voting system. The fact of whether or not a given voter has voted at all, as well as the mode with which the voter choose to vote, might also be sensitive in some situations, and it is not yet clear whether the Swiss e-voting design necessarily protects such voting metadata adequately (it certainly does not do so with the strength with which it protects the privacy of the votes themselves). Similarly, voter registration information is currently considered "out of scope" of the voting system entirely and hence unaddressed, even though some of this to some degree may arguably be considered sensitive as well – not least because it may facilitate profit-motivated actors, criminal organizations, or foreign adversaries to engage in individually-targeted

mass influence campaigns of the kind that were uncovered in the Cambridge Analytica incident for example. Any personally-identifying information can turn out to be sensitive in unexpected ways, and our experience is that it almost always does.	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
I believe that with the right design and sufficiently secure implementation and deployment, Internet voting could eventually be much more secure than postal voting, for the reasons discussed above. I don't believe that Internet voting will ever be more secure than properly-implemented in-person voting, all other things being equal, but it need not be much if any less secure either, and the convenience advantages could definitely and greatly outweigh the costs. Furthermore, for citizens traveling or living abroad for whom in-person voting is simply not an option, Internet voting could be far more secure and preferable in general to commonly-used alternatives such as relying on (foreign) postal services to deliver paper ballots, sending scanned ballots over unencrypted and unauthenticated E-mail, etc. **The current Swiss e-voting design, however, cannot ever be more secure than postal voting, for the trivial reason that it still depends on the postal system and treats the postal channel as a blindly-trusted delivery service. This is one of the big weaknesses of the current E-voting design, as discussed above, which I hope will be addressed in future designs. Thus, Internet voting could eventually become more secure than postal voting, but only after it becomes "fully dematerialized" and no longer dependent on a blindly-trusted postal service.**	

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
I believe it is reasonable to assume a sufficient number of voters will correctly follow the process and check the return codes, so that the code-based cast-as-intended protection mechanism can be considered reasonably secure. I don't believe that the percentage of voters who actually check the return codes needs to be extremely high	

in order to ensure a high probability that any systematic, large-scale attempt to modify intended votes (e.g., by exploiting a widespread operating system vulnerability in a popular device) will have a high probability of being detected. For example, even if a rather low estimate of 10% of voters actually check the return codes, then an attacker's attempt to modify votes via even just 100 exploitable devices would have a near-certainty of being detected - provided of course the attacker cannot learn or effectively guess which voters will and which won't check the return codes.

One could envision clever attackers designing their device exploits to use side-channels or human-behavioral "tells" to try to guess which users are not checking the return codes and modify only their votes – but such automated guessing attacks would probably have to be extremely sophisticated to achieve any significant accuracy, and thus are not likely in practice.

Furthermore, the mere uncertainty about which voters will check the return codes and report irregularities will certainly represent a powerful deterrent to most attackers, who likely risk various consequences (international embarrassment, censure, sanctions, not to mention losing valuable zero-day exploits) if such attacks are attempted and detected. Not all such attackers will be deterred in this way, but many will be.

I believe essentially the same logic applies to other alternative channels for cast-as-intended integrity checking as well: for example, to checking across devices rather than via mailed codes. It would not necessarily require a high percentage of voters to have multiple diverse devices, and actually use them to cross-check their votes, to ensure a high probability of detecting any widespread attempt at vote tampering, or to ensure a significant deterrent effect even on attempts at such vote tampering.

Of course there will always be measures that could be taken to increase the prevalence of voters actually checking their votes. With proper UI/UX design, ways can often be found to "force" the voter to confirm that they have actually performed such a check and can't simply blindly click "yes" even if they want to. For example, with the code checking approach, instead of just asking voters to compare a code on the screen with a code on the paper and make sure they are equal, the voter could instead be asked to enter some combination (e.g., the digit-by-digit sum or difference) of two different corresponding codes (one on the screen and one on the paper), so that the e-voting process cannot proceed until the voter has actually demonstrated that they actually read and in some way "thought about" (e.g., did mental arithmetic on) the corresponding codes. This particular example does not sound appealing from a usability perspective, since asking ordinary voters to do (even simple) mental arithmetic is likely to be too cumbersome and painful for some voters and annoying to all – but simpler alternatives with similar effects might conceivably be found.

For cross-checking votes across devices, an analogous UI/UX design might be to ask the voter to re-enter their vote choices on the second device, instead of simply displaying them – and then to raise an alert and highlight any differences between the re-entered votes and the recorded votes. Again, this presents UI/UX tradeoffs that would have to be carefully evaluated for the best balance between security and usability/convenience.

2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?

This measure strikes me as an extremely weak protection measure, almost not worth the trouble or inconvenience it causes, in large part because it guards against such a tiny part of the total "attack surface" by which an attacker might misdirect the voter.

For example, instead of sending the voter to the wrong server, the attacker might try to supply the voter a wrong or compromised e-voting app (native or Web) entirely by compromising the App store, a code-signing certificate, or one of the many dependencies the e-votin app is likely to have (see the software pipeline vulnerability considerations discussed earlier). The compromised app could advise the user to check the TLS fingerprint against the wrong "master" fingerprint, or simply avoid mentioning this fingerprint checking step at all.

Similarly, even if the client has connected to the correct server, that server itself is a single point of compromise that obviously must be Internet-facing, so if hacked, the voter will see the correct fingerprint but still be misdirected to attacker-controlled content. Fingerprint checking does not seem likely to be truly effective unless it can be the fingerprint of a split-trust collective of some kind, e.g., not only a single server but a server together with a cluster of independent witness cosigning servers monitoring, logging, and actively verifying the content it is serving.

2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?

This form of verification is indeed extremely important, but a complete solution is not straightforward and ultimately must encompass the entire software development, signoff, build, and distribution pipeline as discussed earlier. Complete distributed software images, whether Javascript-based web apps delivered via a web server, or native applications delivered via App stores or software downloads, should be not just signed by a single server but collectively signed by a split-trust of some kind – either symmetric (like the control components) or asymmetric (e.g., a primary authority along with a set of witness cosigners). Manual verification of a fingerprint can then be a reasonable protection measure if it is a fingerprint of the entire split-trust group and not just a single trusted signing key.

Further, the process should ensure that no software image (whether native binary or JavaScript bundle) can be adequately signed so as to verify against the fingerprint, or be accepted as an automatic update, unless multiple independent servers (e.g., forming either a Byzantine consensus group or a set of witness cosigners) have publicly logged the existence and delivery of that particular software image for transparency. This provision ensures that even if an attacker compromises the development or build process enough to be able to create a correctly-signed image containing a back door, no client device will accept it as an update and no fingerprint-checking user will accept it for initial install unless the backdoored image is transparently "in the public record" and hence subject to analysis and potential detection by any interested parties (such as security experts) around the world.

For further discussion of software pipeline transparency measures such as these, please see my blog post, "Apple, FBI, and Software Transparency" (https://bford.info/2016/03/10/apple/), and my lab's CHAINIAC paper from USENIX Security 2017 (https://www.usenix.org/conference/usenixsecurity17).

2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant?

	Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.

I am not an expert on quantum computing in particular, and thus cannot offer much of a guess at how realistic quantum computers will be in the near future and how soon in practice they will threaten today's public-key cryptographic algorithms. However, the possibility that they might within the next 10 or 20 years is an important risk to consider related to voter privacy. This risk should not be overblown, since in practice it is almost certain that anyone with a sufficiently powerful quantum computer at that point will generally have much more high-value targets to break than the way people voted decades ago. (For example, I would expect an attacker with a quantum computer to use that cracking power on all manner of other confidential information encrypted with today's public-key algorithms, such as sensitive business or government documents, cryptocurrency wallet keys that still hold a balance, etc.). Nevertheless, the potential long-term privacy threats from quantum computers cannot be discounted entirely either.

For quite some time to come, the simplest and most economical way to keep today's cryptography ahead of the quantum computer threat may simply be to continue gradually increasing cryptographic key sizes to levels that may be extremely over-conservative from a pre-quantum perspective.

In the longer term, of course, we need to start migrating the public-key cryptography our e-voting systems are based on to "post-quantum" cryptographic algorithms that are not expected to be affected disastrously by quantum computers. Lattice cryptography shows great promise in this respect, for example, but does not yet come with the general-purpose toolbox of algorithms that e-voting systems tend to depend on, such as efficient general-purpose zero-knowledge proofs and verifiable shuffles. Filling out that toolbox with post-quantum cryptographic primitives remains an important and ongoing area for research.

In addition, even the post-quantum cryptographic primitives we do have (e.g., lattice crypto) is far less mature than our common discrete-log and elliptic-curve cryptosystems, and thus should not be (completely) relied on in the too-near future anyway in case new cryptanalytic attacks partly or completely break these new cryptosystems in the not-too-distant future. Avoiding potential attacks by long-distant future quantum computers by increasing the risk of successful attack by classic cryptanalysis or mathematical innovations is a difficult and dubious risk tradeoff to judge.

2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?

Taking general standard precautions against malware (e.g., keeping operating systems up-to-date with security patches and attempting to remove malware when infected) can of course help improve the general level of protection of voters' devices. However, this will always constitute fairly unreliable and incomplete protection: some devices will still be vulnerable, some malware cannot be reliably detected or removed with anti-malware tools, etc. And ordinary malware – of the type these tools apply to – do not seem like the main or most serious malware threat facing a country using an

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

e-voting system, since typical malware isn't designed to care how a user voted but just wants to (say) steal user information for identity theft, cryptocurrency theft, etc., or just use the device as a platform for sending spam or infecting other machines. The real threat in the case of e-voting is the sophisticated and resourceful actor with the motivation and resources to exploit vulnerabilities in common devices in ways that are targeted (e.g., to change votes or prevent people from voting) but attempt to remain undetected by ordinary malware tools.	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
Internet voting would definitely increase the risk of efficient and scalable coercion attacks, such as anonymously-funded dark DAOs paying voters en masse to install tools that monitor their voting devices and confirm how they voted (see Juels et al, "The Ring of Gyges" mentioned above). With postal voting, scalable electronic denial-of-service attacks seem potentially feasible (e.g., deliberate misdirection of significant numbers of ballots), but coercion attacks on postal voting do not appear obviously highly scalable. With e-voting, coercion attacks can be much more automated, much more anonymous, and much more scalable. This is part of the reason for my position that the coercion threat is currently underappreciated and must be addressed as soon as possible in future generations of the e-voting system.	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
The most important criteria is appropriate expertise and experience with evaluating the particular type of algorithms and code in question, i.e., deep experience with distributed systems, security/privacy, and cryptography, at both the design and software implementation level.	

It's not clear to me that "common criteria" certification is highly important, since that is a certification standard that generally applies to defense information systems with fairly different properties and requirements than e-voting systems for public use. Requiring common criteria certification also seriously limits the range of parties who can perform such evaluations, potentially making it more difficult to find appropriate expertise along other important dimensions.	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
In some cases I think it may be justifiable to continue using an e-voting system that is known to have some weaknesses in the short term before the weaknesses can be thoroughly fix, provided the known weaknesses are not critical and the risks are mitigated as much as possible in other ways. **For example, in the case of the current e-voting system with its recently-discovered weaknesses, I feel that a reasonable course of action might be to continue making the system available to voters with special needs to use it – particularly those living outside of Switzerland – while restricting its use to a small percentage of the population for now until the weaknesses can be thoroughly addressed. Effectively disenfranchising voters for whom the pure postal-voting system is simply too slow or unreliable is not an acceptable alternative for a modern democracy, and other obvious electronic alternatives – such as E-mailing scanned ballots with no encryption or authentication, as numerous US states do unfortunately – is even less secure than using a purpose-built E-voting system with known weaknesses in end-to-end verifiability but that at least provides encryption and authentication of ballots cast.**	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).
The reputation of and public trust in all the organizations involved in the examination certainly affects the credibility of the outcome. Further, the organization actually performing the examination certainly needs to have sufficiently deep expertise in the relevant areas, such distributed systems and cryptographic software, to ensure that errors in highly specialized code are caught as well as general software development practice and operational issues. **As I am not an expert on the specific organizational issues or the specific organizations involved or available in this case, however, I cannot readily provide more specific guidance.**	
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
While I suspect that reference to existing evaluation standards may be useful, I am not an expert in those standards and thus can't make specific recommendations. Further, I'm skeptical as to the extent they are likely to be useful, because in my understanding most of the relevant certification standards essentially constitute vague process checklists, of the kind that lawyers often seek for compliance purposes, but which by no means ensure that the resulting system is actually secure "in depth" – i.e., down to the details of what the software or system is doing at a line-by-line level. To ensure that an E-voting system is actually secure, as opposed to merely "process compliant" in some legal fashion, requires careful, detailed, and systematic line-by-	

line independent analysis and peer review by suitable experts and not just a legal process compliance checklist.	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
Since the cryptography that all E-voting systems depend on is and remains a fairly rapidly-changing field, not to mention regular developments in the background field of distributed systems, an E-voting system probably needs to be re-examined at least every five years if not more frequently, and also at any relevant special events such as the discovery of significant weaknesses in the cryptographic algorithms the E-voting system depends on. **Major developments in the maturation of quantum computing technologies, which might effectively reduce the lifetime of the cryptographic algorithms or ciphertexts encrypted in the past, should also be considered potential triggers for re-examination of the E-voting system.** **Finally, newly-relealed evidence regarding the type and degree of attacks that might be expected from criminal organizations or foreign adversaries – such as nation states known to be seeking to use electronic means to sow chaos and uncertainty in democratic countries – should also be closely monitored and taken into consideration in deciding when and now to re-examine the E-voting system and what threats are realistic going forward.**	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
As I mentioned above, independent experts should be involved as early as possible and throughout the design, development, testing, and certification process. This will both help reduce the risk of unpleasant and embarrassing surprises appearing only at the very end, as well as hopefully ensure that international experts have reached some "buy in" and understanding by formal certification and deployment time.	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
This is a difficult, and necessarily somewhat political, question that I'm afraid I don't have any particularly good answers to.	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the

source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
To be truly transparent, the trust-critical source code needs to be open and public from the start, not just opened suddenly at the end under restrictive conditions. The license terms must not require people to sign special agreements such as NDAs to get access to the source code, in particular because some of the best independent experts around the world will simply refuse to sign them and hence not take part in the analysis of the system, weakening participation among arguably the most important body of participants. **Further, the open source release needs to include *all* the trust-critical software necessary to run the system and that is expected to be included in actual production deployments of the system. If the E-voting system is said to be "publicly transparent" but the public (and experts) cannot see what's in components of the system that might well hide critical security weaknesses or back doors (operating systems, libraries, etc), then the system is not really transparent but is only pretending to be transparent. Many of the relevant experts will inevitably notice this and point it out, leading in turn to supporting public (sometimes political) arguments that the system is neither sufficiently transparent nor sufficiently safe in general to use.** **As mentioned above, this does not mean that a publicly transparent E-voting system cannot have any proporietary components at all, only that such proprietary components need to play clearly-documented and untrusted roles in the architecture. For example, an independent expert analyzing and testing the system should be given explicit permission to replace all the proprietary components with deliberately-compromised software that carries out or assists in the worst attacks the expert can come up with, to verify that the proprietary components are indeed not trust-critical. The proprietary components should only be able to improve security with respect to the fully-open subset of the system (e.g., by detecting attempts at attack or disruption), and should never be able to compromise the open part of the system if the latter is bug-free and functioning correctly.**	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

The documentation should of course be as complete as possible and accessible at multiple (perhaps many) levels of detail and audience expertise, ranging rom the general public to the most specialized international experts in e-voting and security/privacy. This is of course not an easy challenge. But systematically organizing the documentation – and document-producing methodology – along multiple "levels of detail" and target audiences may help make the task more realistic and controllable.

4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?

Consistent with what I said earlier, the in-progress code and documentation should be published – and remain open – starting as early as possible in the development process, in order to get (and keep) relevant experts as well as the public "in the loop" throughout the process and avoid unpleasant surprises late in the cycle.

4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)

Yes – as described above, at least in the long term, the roadmap should endeavor to create an "end-to-end secure" software development, validation, verification, build, distribution, and deployment pipeline in which there are no single points of compromise or blindly-trusted authorities at any stage.

Ensuring that independent experts and the public at large can actually run the e-voting system, e.g., with suitable test data, is important but not by itself sufficient, if the experts and the public must merely trust blindly that the version of the e-voting system (and its configuration) that they tested is indeed representative of the e-voting system actually being deployed. If the public must merely trust in this deployment aspect, then that remains a significant weakness that needs to be addressed at least in the longer term. As discussed above, the use of trusted hardware attestation mechanisms when available, together with witness cosigned software distributions a a CHAINIAC-like development, deterministic build, and distribution workflow can help with this aspect of public transparency.

4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?

I think that involving a standing committee of relevant experts being involved in presenting explanations of the e-voting system to the public, as well as discussing reactions from the public, could help significantly. This committee should of course include appropriate scientific and technology experts in security/privacy, cryptography, distributed systems in general, e-voting in particular, etc.

However, such a committee should probably also include a broader set of relevant expertise as well: for example, at least one law or policy expert focusing on political rights and democratic inclusion, who can particularly represent and speak for those who particularly need e-voting (e.g., expats living outside of Switzerland); at least one expert in human-computer interaction and usable security (the intersection of UI/UX design and security/privacy); at least one expert in [digital] ethics; at least one expert in the broader digitalization trend.

I believe that if such a well-balanced committee can be formed, and can consistently produce independent but well-informed and realistically grounded communications

to the public – both to help present the e-voting system and to discuss public reactions – this could greatly help in providing the public with a credible and hopefully non-political "reference point" for thinking about and further discussing the e-voting system as a whole.	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
The system providers should definitely publish information about security breaches transparently, consistent with standard security/privacy best practices such as keeping the details secret for a limited time until all affected systems can be patched. I am not an expert in this process, but the standard existing channels are probably sufficient for this purpose.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
There should definitely continue to be public intrusion tests and bug bounties, but with some adjustments of course. **To start with, the bug bounties need to be much larger: a few tens of thousands CHF is simply not a credible bug bounty for something as critical to democracy as e-voting. Financing a larger bug bounty may require creating a collaborative financial structure between multiple cantons and the federal government, for example, and/or getting insurance companies involved who can help finance a larger bug bounty (at least in the 1M CHF range) without any one canton having to budget for such a bounty outright.** **In addition, at least in the longer term, the e-voting program should attempt to implement the principles of the Hydra framework for "N-of-N version programming" by Breidenbach et al, USENIX Security 2018 (see https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-breidenbach.pdf). In brief, the Hydra framework builds on the software diversity hopefully present in systems built with N-version programming (see earlier discussions on software diversity) to amplify the effectiveness of bug bounties and increase the incentives for responsible disclosure versus irresponsible/malicious exploitation of discovered vulnerabilities.** **In the Hydra framework, if a hacker discovers a vulnerability in one of N independent versions of a system with suitable Byzantine fault tolerance (e.g., the control components in the Swiss e-voting system), then the hacker can demonstrate the vulnerability and claim a (moderate) bug bounty for demonstrating it on that single software version alone. If the hacker is tempted to keep the vulnerability secret and exploit it for malicious ends, however, he would have to wait to try to find similar vulnerabilities in all (or at least a threshold number of) the other software implementations of the same component before such malicious exploitation would be possible. While waiting and attempting to find these vulnerabilities in other versions, the "ethically flexible" hacker would run the constant risk of some other hacker finding the same (first) vulnerability and claiming the single-version prize first. Thus, the Hydra framework ensures that even an "ethically flexible" hacker has a strong incentive to disclose a discovered vulnerability in a single version as quickly as possible, while doing so remains safe with respect to the security of the overall system, unless the hacker is**	

either extremely quick or extremely confident in finding corresponding vulnerabilities in the other N-1 versions of the critical system (e.g., control components).

This will be achievable only once sufficient software diversity is actually in place, of course, with at least 2 and preferably more independent versions of the system. Only two independent versions is sufficient to start achieving some benefits, however, provided both versions are required to be available and in-use in a deployed system. Of course more than two independent versions would be better, if and when feasible.

Although the development of these independent versions will of course incur both significant economic cost and logistical challenges, an economic benefit that may partially mitigate this cost is that bug bounties can subsequently be significantly lower while still being useful and credible. For example, suppose a risk analysis (e.g., as an insurance company might perform) decides that there is a 1-on-10 chance of a critical bug being found in a single-version e-voting system with a 1M CHF bounty in a given year. Simplistically, this means the expected insurance payout would be 100K CHF per year, so the insurance company would need to charge an insurance premium of more then 100K CHF/year to make the bug bounty viable. (This assumes conservatively that only the first bug bounty discovered in a given year is payable, etc.). The 1M CHF total bug bounty in effect ensures that a rational (profit-motivated) actor will claim the bug bounty instead of exploiting a discovered vulnerability, provided the economic benfit from exploitation is less than 1M CHF.

Now suppose in contrast that there are two fully-independent versions of the control component software, correctly deployed as per the principles of the Hydra framework. This way, a responsibly-disclosed vulnerability in either component version is sufficient to claim a (smaller) bug bounty, but vulnerabilities in both independent versions would be required to exploit the system maliciously. Suppose that the bug bounty on a single demonstrated vulnerability is a more modest 100K CHF, and that the risk analysis correctly determines that there is a 1-in-10 chance (independent) that someone (anyone) will find a critical flaw in either version of the control component. Now suppose an ethically-flexible hacker finds a vulnerability in one version of the system. The hacker now faces the following choice: either disclose this vulnerability immediately and collect the 100K CHF bug bounty with certainty, or keep it secret in hopes of finding a similar vulnerability in the other software version for simultaneous malicious exploitation. Even if the hacker could be certain of being the first to discover this second vulnerability provided it exists at all (an unlikely scenario at best), the hacker would face a 9-in-10 chance of losing out on the bounty for the first vulnerability to the second hacker to find it and disclose it responsibly. Thus, the ethically-flexible hacker would have to be offered (or perceive a value of) at least 1M CHF for a pair of independent vulnerabilities affecting the two software versions, yielding an expected payoff of 100K CHF or more (1M CHF x 1-in-10 chance at most of obtaining the payoff at all), before even being economically tempted to follow the more ethically-dubious course of action. Thus, the 100K CHF bug bounty on a single version exploit has been amplified to the economic effectiveness of a 1M CHF bug bounty on the system as a whole.

Since the canton(s) and/or Swiss federal government now need to finance only two bug bounties of 100K CHF each – one for each independent version of the system – at a 1-in-10 expected chance of each being paid out, the expected insurance policy cost of each should be on the order of (somewhat more than) 10K CHF each per year, or on the order of 20K per year total. Thus, a 20K per year insurance premium leverages software diversity to yield the equivalent protection of a 1M CHF bug bounty.

This amplification effect only gets stronger with additional independent versions of the system, because each additional version exponentially decreases the ethically-

flexible hacker's chance of getting any payoff at all via the non-transparent or malicious exploitation path, while only multiplicatively increasing the cost of financing all the relevant bug bounties. For example, only a 10K CHF bug bounty in each version of a 3-version system might be sufficient to achieve the effect of a 1M CHF bug bounty protection for the system as a whole, because after finding the first vulnerability the ethically flexible hacker would have to "win" two more 1-in-10 dice rolls (1-in-100 success at best) to make a 1M CHF reward for malicious exploitation economically advantageous over simply taking the 10K CHF bounty for the first vulnerability discovered. But the cantons and/or federal government need to finance only three bug bounties of 10K each, for an expected financing cost of about 3K/year assuming 1-in-10 expected payout rate.

While I fully understand that creating the required software diversity and placing the Hydra framework into practice will not be quick or easy, the long-term benefits should hopefully be clear enough to make it effectively essential to have this at least be on the e-voting system's long-term development roadmap.

4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?

I believe that keeping the use of Internet voting to a limited portion of the electorate, at least for now, can indeed be effective in helping to restore and maintain public trust. However, it is not clear to me whether this should best be done by specifying a potentially-arbitrary percentage of the electorate, or by limiting the use by some other criteria, such as by making it available (for now) only to those citizens with a clear and demonstrable need to use it. This should certainly include citizens living outside of Switzerland, and there should probably be a short list of other potentially-valid justifications as well, perhaps with a well-defined request and authorization process.

Merely as a comparative example, many states in the US, wisely I believe, restrict remote voting of any kind only to those citizens with a demonstrable need for it. As just one example, see the list of exactly six criteria by which the state of Connecticut (where I lived last and thus now vote remotely as a US citizen) allows absentee voting: https://portal.ct.gov/SOTS/Election-Services/Voter-Information/Absentee-Voting

Of course the actual mechanisms that all US states use for remote voting are terrible from a security perspective (e.g., international postal mail, E-mailing of unencrypted scanned ballts, etc) and I certainly do not suggest any of these practices being a model from this perspective. But a suitably-restrictive policy that clearly acknowledges and addresses the most critical needs for remote voting, while minimizing the risks arising from weaknesses and general immaturity in the technology, will I think go a long way to helping the public understand and accept the justification for the risks and usability/access tradeoffs in the present situation.

4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?

I feel that the cantons should still retain the freedom to make their own choices regarding the deployment of e-voting – such as deciding whether to use it at all and which primary provider to work with. At the same time, no canton should need to

"stand alone" in implementing or shouldering the economic costs of all the relevant transparency provisions, especially including but not limited to the costs of independently verifying the system's universal verifiability proofs.

In particular, regardless of any particular canton's choice of primary voting system provider, I think the federal government should work with all the interested cantons and all the (potential) voting system vendors to set up a decentralized group of passive proof verifiers or witness cosigners that provide independent proof-checking services for all the certified voting systems that may be deployed in the future. For example, suppose two vendors A and B are willing to offer a future version of a Swiss voting system, and two more vendors C and D are willing to provide verification services (only) but not a full e-voting system. Then regardless of whether a canton chooses the voting system from A or B, the canton should be able to rely on a "witness cosigning" network consisting of A, B, C, and D (at least) to provide independent verification of universal verifiablility proofs at election events. This structure could and should eventually extend to other decentralized verification practices such as (a) independent verification of transparent decentralized public-key infrastructure (PKI), such as witness-cosigned PKI records as discussed earlier; (b) independent deterministic build and verification services for transparent software development, build, and deployment pipelines like CHAINIAC as discussed earlier; etc.

In general, since the cost of independently implementing and providing verification-only services should be much lower than the cost of providing full e-voting systems, and the actual deployment of such services should be much less availability-critical if utilized correctly (i.e., the unavailability of one or two verifiers should never be able to prevent an election from completing), we can hope and reasonably expect that the number of competent institutions willing and able to provide verification services in such an architecture should be significantly greater than the number willing to provide full e-voting systems. Thus, this verification asymmetry can go a long way to increase effective implementation and deployment diversity at a more manageable cost than having many competing vendors of full e-voting systems. At the same time, ensuring that each vendor of a full e-voting system is required by policy and contractual terms to work with both other e-voting system providers and verification-only providers should help encourage all e-voting system providers to be more publicly transparent and proactively open in general.

4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?

The publication of shares (of cryptographic commitments, zero-knowledge shuffle proofs, etc) usable by the public and independent experts for verification is definitely a major trust-building benefit that should definitely be done in some fashion.

However, it is of course important to consider carefully the tradeoffs between public verificability and long-term vote privacy, especially in the event that quantum computers or cryptographic breakthroughs eventually weaken the confidentiality of today's public-key cryptosystems and verifiable shuffles. This is not an easy problem.

However, I feel that one reasonable "sweet spot" approach to this problem is to have two different "verifier circles", one public, and the other restricted to only a few well-known and collectively-trusted organizations, such as a suitable federation of e-voting providers and verification service providers as hypothetically discussed above in question 4.9. In brief, the e-voting system would be designed to produce in parallel two sets of cryptographic vote commitments and two parallel sets of shuffle proofs: one guaranteeing full integrity protection but only cryptographic confidentiality guar-

antees (e.g., based on direct ElGamal encryptions of votes); and the other guaranteeing only cryptographic soundness but information-theoretic privacy (e.g., based on shuffles of Pederson commits to encrypted votes rather than the votes themselves). The commitments and proofs providing information-theoretic privacy would be made publicly available and verifiable to anyone, while those providing complete soundness but only computational privacy would be available to and verified only by the more restricted federation of verifiers, each of which has a contractual obligation to to securely erase all privacy-sensitive material after the election concludes.

Taking this approach even further, in principle it should be feasible to use information-theoretic Shamir secret sharing among the restricted federation members to ensure that even if one of the more-trusted federation members improperly saves privacy-sensitive information (e.g., ElGamal vote ciphertexts), a single share of that information would not be sufficient to compromise voter privacy even in the long term if the cryptosystem is fully broken eventually. Nevertheless, the public can immediately verify the correctness and integrity of each election as it occurs on the basis of information-theoretic (e.g., Pedersen) commits and shuffles, assuming the cryptosystem is not already fully broken, without the risk of compromising long-term privacy.

There are many challenges and details to be worked out with such an approach, of course, which would have to be part of the long-term research and development roadmap and not something we expect to achieve immediately. But something like this goal should be on that long-term roadmap at least.

4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

Infrastructure and process inspections could of course help increase security and trust, as well as further public transparency provisions such as the use of trusted hardware attestation, mechanically-checkable formal verification of software, and witness cosigning or other online verification mechanisms as discussed above.

4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?

Enabling comparison of results across voting channels may be useful, but its utility is probably limited, in part because we can expect social and cultural biases to appear across the users of different voting channels. It is almost certainly the case that a slightly different "type" of citizen will elect to use e-voting versus postal voting versus in-person voting, and this effect will certainly result in legitimate differences between the voting patterns observed across different channels. These legitimate differences in behavioral patterns will undoubtly be difficult to disentangle from any potential true "red flags" emerging from the differences. Thus, these differences could unfortunately serve both to undermine the public trust (especially among voters who see the numeric differences but do not understand the reasons for the legitimate behavioral differences) while also failing to provide particularly "actionable" information or warnings of true irregularities across the voting channels.

Ideally it would be much better in principle to find a way to perform some kind of risk-limiting audit within each voting channel independently, using independent random samples of voters, which have more statistical certainty of not being biased by voter behavior. For example, a small randomly-selected sample of e-voting ballots might be selected for special, more extensive processing and verification in addition to the normal universal verifiability process. I have not worked out a specific such process,

and many details would of course have to be worked out, but such an approach may be worth exploring at least.

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign

I believe the general approach the federal chancellery has already been taking – choosing and inviting well-known experts both in targeted fashion, and in occasional "untargeted" opportuniuties such as public intrusion tests – is reasonably effective and should be continued as such. Whatever the process, it should ensure that a reasonable body of diverse expertise from both within and outside of Switzerland willingly participates on a regular and continuing basis.

I believe in particular that involving the open source software and internation e-voting community continuously from the early stages of development of a (fugure generation of an) e-voting system will significantly help in attracting and retaining the participation of a reasonable body of strong international experts. It will of course help if these experts can clearly see that their advice is being carefully considered and taken into account in continuing steps in design/implementation/deployment.

Another potentially-complementary approach the federal chancellery and/or cantons could take to increase public confidence is to involve an actual, small but randomly-sampled and therefore representative group of the actual relevant public in the requirements-setting, design, evaluation, and deployment process. In brief, instead of just asking a sampled group of (often fairly naïve and apathetic) citizens about a complex issue like e-voting, one convenes a randomly-sampled group in a process a bit more like a jury selection for a trial, but in this case for the purpose of learning and studying an issue in depth, hearing from and evaluating the testimony of experts chosen in party by the sampled group, etc. An already-well-known set of processes is

already fairly widely if experimentally used around the world, known variously as sortition-based "mini-publics" or "citizens' assemblies" or "deliberative polls". Certain internationally-recognized political scientists such as Helene Landemore (Yale) and James Fishkin (Stanford), for example, are experts in both studying and helping governments implement statistically-representative deliberative processes such as these. (I can provide introductions if desired.)

The results of such citizens' assemblies can in generally be much more well-informed and evidence-based than (say) traditional polls, yet also potentially more credible to the public at large precisely because of the representativeness of the group. A group of experts chosen by the government can always be argued (with some reason) to be non-independent and potentially biased in various ways. But it is harder to argue that a truly diverse and statistically-representative jury-like mini-public is similarly biased, even if it in part relies on (the testimony of) experts in the same way that the government would probably rely on experts in acting by its own initiative.

5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?

Strong and relevant credentials from the perspective of traditional scientific metrics – such as personal and institutional reputations and publications in relevant scientific venues – should be the primary conditions as always. Diversity of perspective and experience is important of course – e.g., perspectives from both inside and outside of Switzerland, and also from different complementary disciplines (computer science, law/policy, usable security, ethics, political theory, etc).

5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?

As discussed earlier, convening and maintaining a standing committee of diverse experts specifically tasked with helping to both participate in independent analysis and consultation on the e-voting project, as well as to help communicate the design, motivation, positions, cost/benefit/risk tradeoffs, etc, could be a significant aid to the e-voting program's being able to build and maintain the public's confidence relatively independently of political considerations.

5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?

All of the design elements and provisions for verifiability and transparency should be "in scope" for being prepared and addressed to voters, but at multiple different "levels of detail" as suggested above. For example, perhaps there should be one extremely concise and high-level summary readable and accessible by just about everyone; a second that might be 10x longer and similarly more in-depth, a third at another 10x level of detail and correspondingly required dedication and expertise in audience, etc. Given that the "most detailed" document for the narrow audience of international experts needs to be produced anyway, the additional "summary" level-of-detail documents all together will represent a fairly small – but extremely important – additional investment.

5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges

	• Others you might think of
Hackathons, public intrusion tests, and events similar to the recent DEFCON "voting village" challenges are all useful and should be continued. However, I feel that the most important and effective approach, as discussed already, will be to get and retain appropriate continuing partipication from suitable and diverse experts early on and continuously through the process of next-generating e-voting system development.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
While I agree in principle that establishing such a continuous risk assessment process is extremely important and should be done, risk assessment is not one of my areas of primary expertise, so I cannot offer many particular suggestions in this space.	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
Unable to comment specifically (for the same reasons as above).	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
Unable to comment specifically (see above).	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
Unable comment specifically (see above).	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
Unable to comment specifically (see above).	

6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
Unable to comment specifically (see above).	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be out-sourced? To whom?
Unable to comment specifically (see above).	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
Unable to comment specifically (see above). However, I do believe it is both important and should be possible to decompose the canton-specific risk considerations from the overall system considerations, to keep the risk analysis load manageable and share as much of the costs as possible across cantons.	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
Unable to comment specifically (see above).	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
While I agree that crisis management is extremely important and should be addressed systematically, I am not an expert in this space and thus feel unable to comment specifically on this.	
7.2	What are the right events and thresholds for an activation?

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Unable to comment.	
7.3	Who should be involved in crisis management, with which role?
Unable to comment.	
7.4	How should the communication be organised (internally and externally)?
Unable to comment.	
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
Unable to comment.	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
Unable to comment.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
Unable to comment.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
Unable to comment.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
Unable to comment.	

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	David-Olivier	**Last name**	Jaquet-Chiffelle
Organization	VIP Research & Consulting Sàrl		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

Most important questions to evaluate the trustworthiness of such an Internet voting system are related to the redundancy of the system, its development using state-of-the-art knowledge, technologies and procedures, the possibility of independent verifiability and verification, its transparency, its compliance with data protection principles, its forensic readiness and its unscalability to potential attacks, its authentication mechanisms and its overall robustness.

Doing everything to avoid problems in an Internet Voting system is not sufficient to reach trustworthiness, even if everything is verified by trusted parties. Being almost sure that there will be no problems is not sufficient either.

Trustworthiness requires four conditions to be fulfilled simultaneously:

- **(i) Everything (reasonable) has been done to avoid problems and is verified by trusted, independent entities**
- **(ii) It is recognized that problems are expected to happen anyway**
- **(iii) Any problem happening is highly likely to be detected**
- **(iv) Any detected problem is highly likely to be solved in an appropriate way**

Question 1: Does the system or its architecture suppose any entity to be fully trusted?

If yes, my trust in the system is significantly reduced. The system should be built so that nothing, nobody, no entity of any sort needs to be fully trusted. In other words, the system should be able to build trust in an untrusted environment. For me this is a necessary (although not sufficient) condition for the system to possibly be considered trustworthy.

Building trust in an untrusted environment at least requires redundancy and independency.

Question 2: Is the system redundant enough?

As for any sensitive physical system (nuclear plant, aeronautic, critical infrastructure, etc.), redundancy should be omnipresent in an Internet Voting system.

Redundancy allows to discover some possible malfunctioning. Sometimes, redundancy is necessary for cross-verification. It makes many attacks much harder to achieve and often easier to detect. As a consequence, it diminishes the incentives for an actual attack and can therefore be considered as a prevention measure.

The important issue of redundancy seems to have been severely underestimated in current Internet Voting systems.

Question 2.1: Is the redundancy built on independent components?

Moreover, in order to achieve real redundancy, redundant components should be as independent from each other as possible.

In particular, redundancy is crucial for the core components of the Internet Voting system:

Redundancy of the core components of the Internet Voting system: The core system should be fully operational with (at least) 2 different and independent versions: it should be

for example programmed in two different and independent programming languages. The versions should be developed by different and independent (private and/or public) companies. The companies should not be owned by common entities (no common financial or political agenda) and should not share or use common resources (in particular human resources, or the same standard libraries).

Redundancy of the executable/executed code: Then, each program should be compiled with two independent compilers (a single compiler should not be trusted, this is a central point) and run in parallel on different servers (brand, processors) with different operating systems.

As an alternative, we could consider one system that is fully electronic on the server side, whereas the second one combines the Internet Voting user interface with a physical printing of the vote. In such an Internet & physical combination, each voter sees on his/her screen a film of his vote being printed in real time, as well as the paper printed document then falling in a sealed urn.

Question 2.2: Are the votes recorded within two different, completely independent systems?

It is important that if one of the systems is compromised or is malfunctioning, the other one can be used for an independent verification, or an independent recount of the vote.

Question 2.3: Is there an independent way to recount the votes in case of a doubt?

If two different and independent electronic systems have been used to record the votes, it is possible to cross-verify the results. If only one system is used, each recount will give the same (possibly wrong) result with no additional trust in the truth of result.

If the Internet votes have also been printed on paper (not only recorded in electronic form in a database), an independent recount of the votes is feasible.

Such an independent recount allows to detect potential malfunctioning of the software or hardware at the core level of the Internet Voting system. Such malfunctioning can have an intentional cause (internal or external attack of the system), or a non-intentional one (e.g. bugs in the programs, hardware errors).

Question 3: Has the system been developed using state-of-the-art best practices for sensitive software development?

Formal verification, small and well-documented procedures, four-eyes verification during software development, etc. are basic requirements for such a system.

Question 3.1 Do all procedures for the deployment of the programs and their future updates follow best practices?

Signed and traceable code are basic requirements.

All key persons involved in the deployment of the programs and their future updates should be supervised. Each action should be logged and traceable. Traceability should use unforgeable ledgers; hashes of logs information (made non sensitive) should for example be stored in public robust blockchains.

Question 4: Are all sensitive responsibilities/operations split and well controlled/monitored?

Nobody, no single company should be fully trusted. If we only have software-based redundancy for the Internet Voting system, core components for example should be programmed twice, and independently.

No sensitive key or parameter should be known or accessible to any single person or within a single company. Secret sharing schemes with thresholds should be the norm.

The generation of any sensitive parameters should use and combine at least two true & independent random sources of entropy. One of them could be for example a quantum random bits generator produced by the Swiss company ID-Quantique (I have no personal advantage in this company!) or an equivalent Swiss entity.

No single person should be allowed to modify/update alone the core components of the system. Strong authentication should be used for all persons who intervene at this level. Full traceability of the operations done at this level is required (forensic readiness). Traceability should again use unforgeable ledgers; hashes of logs information (made non sensitive) should for example be stored in public robust blockchains.

Question 5: Does the system (and its architecture) allow and encourage independent verification and validation of its architecture, of its implementation and of its components?

The system needs to be transparent (in particular the programming code should be open source) so that anybody can theoretically verify what it does. Transparency is an important component to build security and trustworthiness in this context.

Theoretically, the compiler should also be open-source in order to be sure that it does not introduce either a backdoor in the executable code (such a backdoor could lead to a scalable attack) or just a non-intentional error if the compiler has a bug itself. However, this is not realistic and my proposition to compile the programs using two different, independent compilers, and to run the resulting executable codes on different systems is a more realistic/practical alternative to cope with the intrinsic weakness of choosing only one single trusted compiler.

Question 5.1: Has the government set in place a protocol to officially test/evaluate/validate the software and the architecture up to a certain trust level?

Even if the system is transparent, only specialists might really understand the used algorithms, the developed programs and the architecture, and verify them. Moreover, it is very time consuming. Ordinary citizens must indirectly trust the system. The system should therefore be officially tested/evaluated/validated up to a certain trust level by several independent entities defending (sometimes competing) values, rights or groups of interests. We could imagine verifying/validating entities representing the Swiss government and others representing citizen and defending privacy values.

Results/certifications produced by those verifying/validating entities should be made officially available on a website. Citizens can then see “who certified what”, and decide according to their preference who and what they trust.

Next to the official sponsored testing entities, any other entity should be allowed to also verify the system (or parts of it) at its own costs.

Question 5.2: Has the government set in place an official sustainable bug bounty program?

An official long-term bug bounty program, sponsored by the Swiss government, should be set in place so that reported bugs and vulnerabilities are sold to the Swiss government rather than to criminal entities. This gives an incentive for white/grey hat hackers to scrutinize and test the developed system even in the long run. This is a low-hanging fruit to increase the security of the system and its trustworthiness.

Question 6: Is the system compliant with data protection principles and vote secrecy?

Traditional data protection principles (confidentiality, integrity and availability) must clearly be fulfilled and verifiable:

The vote must be confidential. How can the voter be sure that nobody, not even the Government or the entities that developed the system, not even a hacker who has taken control of his/her computer, can link the content of his/her vote with his/her identity? In particular, the server authenticating the voter should not know the content of the vote. The server receiving the vote should not be able to know both what the voter has voted for and who the voter is. And the components of the system being able to give later a meaning to the vote should not know who the voter is. These conditions are difficult to achieve while allowing the server to communicate with the voter in order to verify that what the server has received genuinely corresponds to what the voter intended to vote. The server choosing the verification codes to be sent according to the received vote (in the Swiss Post E-Voting system) should not have any possibility to know who the voter is.

Vote's integrity has to be guaranteed (what has been voted corresponds to what is transferred, received, recorded and finally counted).

Availability means that the voting system is robust enough to be resistant against DDos attacks for example (so that voters can use the system), but also that the vote will not be lost or discarded after having been sent.

More recent further data protection principles (unlinkability, intervenability and transparency) are also important and should not be underestimated.

Unlinkability: Nobody but the voter himself or herself can possibly recognize his/her recorded vote. Nobody else should be able to link the content of the vote with the actual voter. Nobody should be able to link voting answers of the same person (either when several questions are to be answered during a given voting date, or during different voting dates).

Intervenability (nice to have but not crucial): If voters have an independent way to check that their vote is recorded, they should be able to intervene if they consider that the vote is incorrect (if they have done a wrong manipulation or an error while voting, or just decide to vote differently). This is a "nice to have" as this is not feasible with traditional voting methods (booth, mail). However, this could be an added value of the Internet voting.

Transparency (nice to have): Given the fact that most citizen will not be able to directly verify themselves the security and trustworthiness of the Internet voting system, it would be interesting to value transparency of the personal vote. Each voter should be given the opportunity to verify that his/her own vote has been recorded and counted correctly.

However, if such (nice to have) transparency is provided, extra measures should be taken to avoid the negative impact of such a transparency option. Nobody else should be able to

verify the exactness of the vote, nor force the voter to do it in order to reveal the vote (for example, if the voter is forced to do it, he/she should have the possibility to surreptitiously "ask" for any fake result of his/her choice to deceive the person who forces him/her to reveal the vote). This makes the system more complicated. Is it really worth it?

Question 7: Is the system fully "forensic ready"?

Forensic readiness requires trustworthy traceability (e.g. ledger-based traceability using blockchain technology) and detailed logs in order to investigate unusual or suspected events.

In case of a (suspected or actual) security breach, it allows a rapid access to valuable information in order to understand the issues and efficiently choose adequate countermeasures when reaction time is critical.

In a second phase, afterwards, forensic readiness also allows in-depth investigation in order to reach a more thorough understanding of the event, to assess its actual impact and to take required new preventive measures if necessary.

Question 8: Is the system prone to scalable attacks?

One of the main risks when moving from the physical world to the virtual one is scalable attacks. In the physical world, numerous attacks are not really scalable: the effort to run the attack in the physical word is more or less proportional to the number of targets. "Helping" people to vote means going from door to door and is very time consuming. Influencing the way the votes are counted, if ever possible, would require dishonest persons to be physically present within many counting teams. The decentralization and splitting of the tasks make it difficult to attack the system in the physical world in a significant way.

With the Internet voting, the risk of a scalable attack is real. Indeed, in the virtual world, an exploit for example can be used at a very large scale without requiring a significant extra effort. It might be very difficult (or very costly) to find the exploit or any useable weakness in the system. However, when such a breach is discovered, many attacks become scalable and very hard to detect if the system lacks redundancy.

Question 8.1: Is a scalable attack at the level of the centralized system feasible?

An attack grounded in the core, centralized system or at the printing office (where the verification codes are printed) would certainly be scalable. That is why redundancy, both in the components and in the controls, is so important in order to make such an attack almost infeasible with the budget available to potential attackers. The incentives of an attack and the related potential gain should stay much lower than the expected costs to realize it. An attack at the printing office could be scalable and is therefore of utmost concern. The printing office as a single entity should not have to be fully trusted in the overall architecture.

Question 8.2: Is a scalable attack realistic on the voters' side?

Voters will use a computer or even a mobile phone to vote. Those systems are often insecure, or even compromised. They should be considered as a hostile environment. Malwares can be used to take control of many voters' machines. Malware attacks are scalable. The whole architecture of the Internet Voting system has to be thought in a way that even if

the voter's computer is compromised (i.e., the voter can neither trust that what he/she enters is what is sent, nor that what he/she sees on the screen is what has been sent to him by the voting server) the vote intended by the voter is correctly recorded and counted.

Both the Internet voting server communicating with the voter and the voter have to convince each other that what has been sent is what has been received, and that an intermediary entity (the compromised computer manipulated by an attacker) cannot play both roles without being discovered with high probability.

The Swiss Post E-Voting system uses verification codes (see for example the voting card of Fribourg) and another (secure) channel to exchange an information that is supposed to be trusted by both the voter and the Internet Voting server. The voters computer (hence the attacker) does not know this information before the code is actually used. Without having access to these codes, a scalable attack is unlikely to succeed. Hence the importance to assure that only the voter and the Internet Voting server have access to these codes.

The Swiss Post mail is used to deliver these codes to the voter. The same channel is used currently for sending normal voting material to the citizen. A scalable attack of the Swiss Post mail service does not seem realistic in Switzerland. Such an attack would mean a large scale stealth interception of the Swiss Post mail. Several persons should be involved within the Post service itself. It is not realistic to realize such a large-scale stealth interception in a democracy.

In case of doubt, creating redundancy would be possible (e.g. splitting the verification codes, and then use the Swiss Post mail service for half of it and another private mail service for the second half). However, such a solution is complicated for the voters (less user-friendly) and very expensive without bringing significant added-value to the trustworthiness of the global system.

However, a scalable attack of the Printing Office (which prints the verification codes) is not unrealistic and should be an important concern given the potential impact of such an attack.

Question 9: How does the system guarantee that no fraudulent vote can be added?

How can the Government guarantee that no "ghost" voters have been added either deliberately (by the Government itself or some internal entity), or as the result of some malfunctioning or some targeted attack? Who can verify that each recorded vote belongs to one real person having the right to vote?

As a single entity, the Government itself (or its internal entities) should not have to be blindly trusted. Independent verification, typically by opinion groups having competing interests should be possible in order to avoid any possible doubt and "conspiracy theories".

Question 10: How can the system ensure that the vote has been really produced by the authorized voter according to his/her own choice?

Basic authentication credentials, like a username and a password, or just a one-time identification number, can be easily transferred and do not guarantee that the right person has voted.

Such a weak authentication protocol can even become an incentive to sell one's own voting rights. This makes such an illegal delegation even easier than with mail voting.

Even strong authentication does not prevent the voter to be coerced to vote in presence of another person who verifies what is voted. Mail voting has the same issue and does not prevent family voting. Traditional vote in a booth is however more secure from this perspective.

A way to (at least significantly) circumvent vote coercion is to allow the voter to vote again and again, as many times as he/she wants during the voting period, in such a way that other people cannot see if (and what) he/she has voted subsequently. Strong authentication that ensures that the voter knows whenever a vote is sent in his/her name should be required.

Question 11: How robust is the system?

The system should be robust against malfunctioning caused either by an intentional (internal or external) attack or by an unintentional incident.

Robustness means both (i) guaranteeing the availability of the system (e.g. the system is resistant to DDos attacks) and (ii) that any malfunctioning will be detected, and possibly corrected, with high probability. Detection of malfunctioning is crucial and highly challenging.

Redundancy measures augment robustness. Indeed, if only one of the independent components is malfunctioning, this can be detected within a system which is two-redundant. Triple redundancy would be needed in order to automatically correct single malfunctioning components. However, triple-redundancy is expensive and automatic correction is not the best approach in this context. Once a problem is detected, it is better to deeply investigate the system and understand what happened in order to take care of the source of the problem (correct a possible bug in the system, understand and stop a discovered attack), assess the impact on the results, and draw further preventive measures if necessary.

Traditional computer security measures need to be reinforced by strong forensic readiness in order to make the deep investigation possible and realistic, after a problem is detected.

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions

that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
It is difficult to assess how likely building-blocks complying with known standards are flawed. It is not uncommon that flaws are detected even in standard protocols. The Internet Voting system cannot (and should not) suppose that there are no flaws. I have seen widely used standard cryptographic libraries having flaws in the key-generation process for example, allowing practical attacks that give the attacker access to the private secret key.	

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

If knowing such a private secret key allows to decipher some publicly posted parameters (e.g. encrypted votes on a public bulletin board), then such a flaw would allow an undetected attack.	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
This is much more unlikely than for 2.1.1.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
Generating parameters outside of the Printing Office does not bring extra security as the Printing Office has access to the decrypted verification codes to be printed anyway. Actually, it is better to have the codes generated just before being printed as this avoids an extra entity having access to these codes. **However, the generation of the verification codes should use and combine at least two true & independent random sources of entropy. One of them could be for example a quantum random bits generator produced by the Swiss company ID-Quantique (I have no personal advantage in this company!) or an equivalent Swiss entity.** **A scalable attack of the Printing Office is not unrealistic and should be an important concern given the potential impact of such an attack. The Printing Office should not be completely trusted. One solution would be to require two independent Printing Offices. Each Printing Office should generate and print part of each verification code. These parts would be sent using two letters to each voter. The actual verification code would be recovered by the voter by putting together the information received in each of the letters (either concatenating both parts of the code, or adding them).**	
2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value

	and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
Running the same software on different control-components prevents the detection of problems in the software. Both redundancy and independence are central to detect problems with high probability. They are necessary in order to build trustworthiness. **The software programs should be developed by different and independent (private and/or public) companies. The companies should not be owned by common entities (no common financial or political agenda) and should not share or use common resources (in particular human resources, or the same standard libraries). Then, each program should be compiled with two independent compilers (a single compiler should not be trusted, this is a central point) and run in parallel on different servers (brand, processors) with different operating systems**	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
-	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
Once again, it is very important to require as many different and independent components as possible. Not only operating systems and hardware should differ. Programs and compilers should differ too.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
Voters will use a computer or even a mobile phone to vote. Those systems are often insecure, or even compromised. They should be considered as a hostile environment. Malwares can be used to take control of many voters' machines. Malware attacks are scalable. The whole architecture of the Internet Voting system has to be thought in a way that even if the	

voter's computer is compromised (i.e., the voter can neither trust that what he/she enters is what is sent, nor that what he/she sees on the screen is what has been sent to him by the voting server) the vote intended by the voter is correctly recorded and counted.

Providing each voter with a trustworthy (and trusted) secure device which cannot be compromised by the voter's hostile environment can certainly simplify several parts of the protocol. Such a device might also be useful to reinforce authentication of the voter, especially if combined with biometrics and smartcard technologies. However, this device should be particularly user-friendly as it would be a rarely used, extra device.

2.1.8	**Correct implementation and protection from unauthorized access**
	The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?

Formal verification, small and well-documented procedures, four-eyes verification during software development, etc. are basic requirements for such a system, as well as signed and traceable programming code. Core components should be programmed twice, and independently.

All key persons involved in the deployment of the programs and their future updates should be supervised. Each action should be logged and traceable. Traceability should use unforgeable ledgers; hashes of logs information (made non sensitive) should for example be stored in public robust blockchains.

The system needs to be transparent (in particular the programming code should be open source) so that anybody can theoretically verify what it does. Transparency is an important component to build security and trustworthiness in this context.

Even if the system is transparent, only specialists might really understand the used algorithms, the developed programs and the architecture, and verify them. Moreover, it is very time consuming. Ordinary citizens must indirectly trust the system. The system should therefore be officially tested/evaluated/validated up to a certain trust level by several independent entities defending (sometimes competing) values, rights or groups of interests. We could imagine verifying/validating entities representing the Swiss government and others representing citizen and defending privacy values. Independent experts from academia belong to entities potentially trusted by many citizens and should be mandated to participate in such tests, evaluations and validations.

Results/certifications produced by those verifying/validating entities should be made officially available on a website. Citizens can then see "who certified what", and decide according to their preference who and what they trust.

Next to the official sponsored testing entities, any other entity should be allowed to also verify the system (or parts of it) at its own costs.

Theoretically, the compiler should also be open-source in order to be sure that it does not introduce either a backdoor in the executable code (such a backdoor could lead to a scalable attack) or just a non-intentional error if the compiler has a bug itself. However, this is not

realistic and my proposition to compile the programs using two different, independent compilers, and to run the resulting executable codes on different systems is a pragmatic alternative to cope with the intrinsic weakness of choosing only one single trusted compiler. **No single person should be allowed to modify/update alone the core components of the system. Strong authentication should be used for all persons who intervene at this level. Full traceability of the operations done at this level is required (forensic readiness). Traceability should again use unforgeable ledgers; hashes of logs information (made non sensitive) should for example be stored in public robust blockchains.**

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
The threat of undetectable (maybe non intentional) malfunctioning.	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
The system should be built so that nothing, nobody, no entity of any sort needs to be fully trusted. In other words, the system should be able to build trust in an untrusted environment. For me this is a necessary (although not sufficient) condition for the system to possibly be considered trustworthy. **Building trust in an untrusted environment at least requires redundancy and independency.** **As for any sensitive physical system (nuclear plant, aeronautic, critical infrastructure, etc.), redundancy should be omnipresent in an Internet Voting system.** **Redundancy allows to discover some possible malfunctioning. Sometimes, redundancy is necessary for cross-verification. It makes many attacks much harder to achieve and often easier to detect. As a consequence, it diminishes the incentives for an actual attack and can therefore be considered as a prevention measure.** **The important issue of redundancy seems to have been severely underestimated in the current Internet Voting system.** **Forensic readiness is missing. It requires trustworthy traceability (e.g. ledger-based traceability using blockchain technology) and detailed logs in order to investigate unusual or suspected events.** **In case of a (suspected or actual) security breach, forensic readiness allows a rapid access to valuable information in order to understand the issues and efficiently choose adequate countermeasures when reaction time is critical.** **In a second phase, afterwards, forensic readiness also allows in-depth investigation in order to reach a more thorough understanding of the event, to assess its actual impact and to take required new preventive measures if necessary.**	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might

	typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
No sensitive key or parameter should be known or accessible to any single person or within a single company. Secret sharing schemes with thresholds should be the norm.	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
The question is ambiguous. The protection quality depends on the actual strength of potential attackers, and of the incentives for them to realize an attack. If Internet Voting becomes the norm, incentives for an attack can become quite high, probably high enough so that integrity and secrecy of the cast votes appear far less protected than security critical data in other fields.	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
Internet Voting without independent, verifiable redundancy appears as a loss in security right now. Many problems could stay undetected. **Moreover, Internet Voting introduces new potential, scalable attacks. Scalability of the attacks is a main concern with Internet Voting.** **Foreign countries might be tempted to interfere with the Swiss voting system. Criminal organizations might try to sell a certain percentage of votes on the Darkweb if they can use an exploit to stealthily manipulate results up to a certain percentage. In case of expected tight results, such a manipulation can make a whole difference. We cannot exclude that there is a market (potential buyers) for such illegal activities/manipulations.**	

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material

	and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
Voters are asked to check if the verification code is correct. However, the system does not verify that the voter has made this check. **An easy alternative to reinforce the protocol is to ask the voter to identify the correct verification code between two similar ones: the correct one and an anagram of it. For example, if the verification code is 4653, the anagram could be 4635 or 4563 (just exchanging two adjacent digits). Such a challenge forces the voter to actually carefully check the verification code.**	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
As for the verification code, voters should be asked to identify the correct TLS-Fingerprint between two similar ones.	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
-	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
As for the verification code, voters should be asked to identify the correct TLS-Fingerprint between two similar ones.	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
Using an antivirus, following the guidelines from MELANI certainly limits the risks of being infected by a malware. However, even a security specialist cannot guarantee that his/her computer is not infected by a malware. Whatever measures are recommended, voters' computers have to be considered as a hostile environment.	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

	voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
Definitely. Especially if Internet Voting becomes successful and is widely accepted. Like nature which tries to fill emptiness, criminals jump on new opportunities…	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
Entities independent from each other, defending (sometimes competing) values, rights or groups of interests. Independent experts from academia belong to entities potentially trusted by many citizens and should be mandated to participate in such tests, evaluations and validations.	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
Voting belongs to the core democratic foundations. Trust in the voting system is primordial, especially in a democracy where results can be quite tight. Once trust is lost, it is very difficult to build it back. No compromise should be accepted, even for the short term.	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).
Not all people trust the same entities, companies or specialists. Some prefer to trust public entities, others private ones. That is why we should imagine verifying/validating entities representing the Swiss government and others representing citizen and defending privacy values. Independent experts from academia belong to entities potentially trusted by many citizens and should be mandated to participate in such tests, evaluations and validations.	

Results/certifications produced by those verifying/validating entities should be made officially available on a website. Citizens can then see "who certified what", and decide according to their preference who and what they trust.	
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
-	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
Each update should be cross-checked. All key persons involved in the deployment of the updates should be supervised. Each action should be logged and traceable. Traceability should use unforgeable ledgers; hashes of logs information (made non sensitive) should for example be stored in public robust blockchains.	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
Next to the official sponsored testing entities, any other entity should be allowed to also verify the most recent system (or parts of it) at its own costs.	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
-	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
An official long-term bug bounty program, sponsored by the Swiss government, should be set in place so that reported bugs and vulnerabilities are sold to the Swiss government rather than to criminal entities. This gives an incentive for white/grey hat hackers to scrutinize and test the developed system even in the long run. This is a low-hanging fruit to increase the security of the system and its trustworthiness.	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
Different levels for different publics and level of expertise. **Published basic documentations should be available for the non-expert citizen.** **In depth documentation of the architecture and the components should be made available, on request, for any expert who wants to assess the trustworthiness of the system. Different levels of detailed documentation might be useful so that the expert is not lost in thousands of pages, but can request more in-depth documentation where needed.**	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
-	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
-	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
A new entity (with a scientific committee) should be created to manage an official long-term bug bounty program, sponsored by the Swiss government. Bugs and vulnerabilities should be reported to this new entity. Rewards to the white/grey hats that reported issues should be granted by this entity.	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
Existing security breaches should be fixed and then published by the entity responsible for the bug bounty program.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the re-

	strictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
Not just a bug bounty program, but a long-term bug bounty program with appealing rewards should be set in place by the Swiss Government.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
Low-scale use of the Internet Voting diminishes the incentive for an actual attacker. As long as only a small proportion of the population uses the Internet Voting, the risk of an attack is much lower. Indeed, this increases the cost/benefit ratio and makes an attack less attractive.	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
-	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
-	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)
-	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
Statistical plausibility checks is a valuable tool to make extra tests. It might allow to detect a potential large-scale problem. Publication of the results and method participates to the transparency of the system and is part of trustworthiness building. In case of a statistical inconsistency, further in-depth investigations might be required. In this case, redundancy in the system as well as forensic readiness will help the investigation.	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate

- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
An official long-term bug bounty program, sponsored by the Swiss government, should be set in place so that reported bugs and vulnerabilities are sold to the Swiss government rather than to criminal entities. This gives an incentive for white/grey hat hackers to scrutinize and test the developed system even in the long run. This is a low-hanging fruit to increase the security of the system and its trustworthiness.	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
This might vary from one person to the other. It is a personal decision. In the scientific community, there is no consensus on the added value of Internet Voting. The scientific community may bring divergent views.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
-	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
Trust should only be promoted if the Internet Voting system is becoming trustworthy. **It is important to wait for the system to be really trustworthy before considering how to promote trust in the system. Otherwise, if this is done too early, trust can be destroyed and difficult to regain.**	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
Trust will hopefully be fueled by trustworthiness. When/if the scientific community reaches consensus on the trustworthiness of a specific Internet Voting system, then promoting trust through interviews, vulgarization articles, radio and TV emissions might be very effective.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
-	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
-	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
-	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
-	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
-	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
High education institutions with their research groups can bring valuable, state-of the-art support to the Confederation.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?

-	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
-	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
-	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
-	
7.2	What are the right events and thresholds for an activation?
-	
7.3	Who should be involved in crisis management, with which role?
-	
7.4	How should the communication be organised (internally and externally)?
-	
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
-	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

In order to efficiently investigate the Internet Voting system in case of an incident, forensic readiness makes a significant difference. Forensic readiness means that the whole system has been conceived and developed keeping in mind that problems will occur and that investigating tools must be built on top of the system itself.

Forensic readiness requires trustworthy traceability (e.g. ledger-based traceability using blockchain technology) and detailed logs in order to investigate unusual or suspected events.

In case of a (suspected or actual) security breach, it allows a rapid access to valuable information in order to understand the issues and efficiently choose adequate countermeasures when reaction time is critical. Digital forensic investigators work in close coordination with CERT teams during or just after a problem has been identified.

In a second phase, afterwards, forensic readiness also allows in-depth investigation in order to reach a more thorough understanding of the event, to assess its actual impact and to take required new preventive measures if necessary.

7.7	What are the requirements and stakeholders for digital forensics and incident response?

Forensic readiness has to be fully integrated on top of the system itself. Digital investigation tools must be available, ready to efficiently identify, authenticate, classify, analyze, integrate, interpret and evaluate digital traces in order to reconstruct the event of interest, understand its impact and take informed decisions.

7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?

On the Internet, investigation does not necessarily aim at prosecution. Internet and digital investigation might be effective and efficient even when it does not (or cannot) lead to the physical person or the entity which initiated the attack. It allows proper counter-measures to be taken, prevention measures to be adopted. Disrupting the attack or making it much more difficult to achieve in the future perturbs the attacker. Perturbing the attacker without being able to prosecute him, understanding his/her motivations, discovering the target of his/her attack can also be considered as successful results of the digital investigation of an Internet Voting system.

7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?

In case of a security breach, an attack or some malfunctioning, it is important to precisely assess the potential impact in a worst case scenario. Forensic readiness, combined with redundancy, allows in-depth investigation in order to reach a more thorough understanding of the event and to assess its actual impact.

The influence of the incident depends on the incident itself, but also on the proportion of voters that have used the Internet Voting system, as well as on how tight the voting results are.

If the investigation cannot exclude that the incident might have modified the voting result, then this voting result should not be declared valid. However, if the investigation can prove that, even in the worst case scenario, the voting result could not be impacted by the incident, then the voting result can be declared as valid.

Berner Fachhochschule (BFH), CH-2501 Biel, Switzerland

Redesign of Internet Voting Trials in Switzerland 2020

Responses to the Questionnaire

Eric Dubuis, Rolf Haenni, Reto E. Koenig, Philipp Locher

March 15, 2020

On behalf of the Federal Chancellery

Contents

1 Big Picture

Question 1.1

You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion/vote buying are not a problem.)

Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny)

Which are the most important answers you need in order to conclude that internet voting is trustworthy?

How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)?

Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting?

We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

We would first start with questions about the democratic system of that particular country and the type of Internet elections to be held. Knowing these parameters is very important for designing a cryptographic protocol. Certain protocols for example are only compatible with electoral systems of low complexity. Other questions about current voting channels and voter habits are important to understand the general context. For example, if multiple channels are offered simultaneously, it is much more challenging to guarantee the absence of duplicates votes across all channels. It is also important to know if existing technological infrastructures like electronic citizens cards are available to all voters, because this may have implications for the voter authentication process.

With regard to the voting protocol, we would ask questions about the adversary model, trust assumptions, and security goals. It is crucial for them to match as closely as possible with the real threats of the country. We would also ask questions about the design of the cryptographic protocol and the documents describing the protocol, in order to see if the protocol uses state-of-the-art techniques, if best practices in cryptographic protocol design have been applied, if the available documents are sufficiently detailed, if the designers of the protocol and authors of these documents are adequately qualified for this job, if the protocol has been gone through a rigorous reviewing process, and if the security goals have been proven formally. Then we would have similar questions about

the software design and development process, in order to see how closely and precisely the cryptographic protocol has been translated into code. If the protocol includes distributed computations on multiple independent components, it would be interesting to learn how independence has been implemented in practice.

It would also be useful to learn something about the general vision of the project and the strategy of the development process, for example with respect to collaborations with scientists, the implementation of transparency measures, or the level of mandated and public examinations. Compared to the projects in Switzerland, in which a transition from complete black-box systems to a relatively high level of transparency took place over nearly 20 years, it would be interesting to see where they are today, to verify if they learned the lessons from other places in the world, and to learn how the implemented transparency measure have been perceived by the public.

An important final block of questions addresses the implementation of individual and universal verification, for example with respect to the planned process of verifying the election results on the election day. To obtain a credible process, it is important to involve the right people—for example representatives of all major political parties—and to conduct the verification on trustworthy hardware and software. The verification software must be perfectly aligned with the cryptographic protocol and include all necessary verification steps. We would therefore ask further questions about the specification and development process of this software. And it would be interesting to learn, if external people are allowed to run the verification by themselves, possibly using their own software, and under what conditions. If this is the case, we would have follow-up questions about the awareness of possible long-term privacy problems when the election data is available to everyone.

2 Risks and Security Measures Today and Tomorrow

2.1 Verifiability

Question 2.1.1 (Crypto-Protocol)

The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks.

Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?

The likelihood of flaws in well-established cryptographic building blocks is relatively small. Security in cryptography today relies on formal definitions, precise adversary models and assumptions, and rigorous proofs based on these assumptions [13]. In other words, modern cryptography is based on sound mathematical foundations, which can be put under the umbrella term *provable security*. Relative to such provably secure cryptographic schemes, which have been studied thoroughly over many years and are well understood today, it is very unlikely for the security proofs to contain undetected flaws. It is also rather unlikely that standard intractability assumptions such as DL, DDH, or FACTOR, which are fundamental for many of these schemes, will be proven wrong in the near future by new algorithmic breakthroughs. Flaws in more recently discovered schemes are obviously more likely, because fewer people have looked at the security proofs with sufficient care. To reduce the likelihood of such undetected flaws, a design principle in cryptographic protocols restricts the building blocks to well-established methods whenever possible.

Provable security relative to some cryptographic scheme does not necessarily imply the desired security of that scheme in the real world. For example, if the security definition does not capture what is needed in a given application, or if the adversary model does not capture the adversary's true abilities in the real world, then the security proof may be irrelevant for the specific scheme. Another problem is the possibility of an inadequate implementation of a given scheme in a real-world system, which for example may violate the security proof's underlying assumptions. An example of a poorly implemented cryptographic building block is the ElGamal encryption scheme in the Moscow Internet Voting System [4]. While ElGamal encryption as such is provably IND-CPA secure under the DDH assumption, it has been implemented using an inadequate mathematical group for which solving DDH is known to be easy. Moreover, by instantiating that group using a 256-bits modulus, the resulting security is far below the security provided by current recommendations (2048-bits modulus or higher). Both problems encountered in this particular implementation of the ElGamal encryption scheme can be exploited easily

for breaking the secrecy of all submitted votes within seconds. Note that these problems have been detected only after releasing the source code to the public.

The above example shows that provable security alone is not sufficient for establishing the desired level of security of a cryptographic building block. It demonstrates that cryptographic beginner's mistakes by under-qualified developers can entirely undermine any proven security property in an actual implementation. It is therefore crucial to also involve cryptography experts in monitoring the software development process. Releasing documentation and source code to the public is another measure for increasing the likelihood of detecting even most subtle implementation flaws in cryptographic building blocks as early as possible.

Another potential problem for cryptographic building blocks based on intractability assumptions such as DL or FACTOR is the presumed availability of sufficiently powerful quantum computers in the near or distant future. The classical adversary model based on the notion of probabilistic polynomial-time algorithms implicitly prohibits adversary access to quantum computers. If this assumption no longer holds in the presence of widely available quantum computers, security proofs based on this assumption will become irrelevant and corresponding cryptographic building blocks will become insecure. For voting systems used today, this causes the so-called *long-term privacy problem* (see Question 2.1.7), which means that vote secrecy relative to an election conducted today can only be guaranteed for a (unknown) limited time period. This is one of the reasons for restricting the access to the bulletin board to the parties conducting the verification.

Question 2.1.2

> *The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model.*
>
> *Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?*

In comparison with cryptographic building blocks, defining and proving properties of a complex cryptographic protocol is far more difficult and error-prone. In the specific area of cryptographic voting protocols, where proofs are usually developed and checked only by a small number of people, the likelihood of a flaw to remain undetected in a proof is therefore considerably higher. However, the existence of flaws in a proof does not necessarily imply the falsity of the property under consideration, for example in case of an incomplete argumentation chain, which often can be closed easily. Nevertheless, the situation relative to proving security on the protocol layer is undoubtedly less robust. The best way of dealing with this problem is again to involve the best experts at every stage of the process and to share all documents with the public from the earliest possible moment.

When it comes to implement a provably secure voting protocol in a practical system, it is again crucial to ensure that the adversary model and trust assumptions coincide with reality to the best possible degree. Only then can the proven security properties be used for making meaningful statements about the security of the system. An important precondition for an implementation to withstand all sorts of cryptographic attacks is to impose a consistent minimal security strength throughout the system (112 bits or more according to current recommendations). The implementation itself must be in one-to-one correspondence with the proven protocol and the communication model used in the proof, i.e., exchanged messages must contain exactly the information as specified in the protocol and communication channels must provide exactly the required properties.

Question 2.1.3 (Printing Office)

For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the returncodes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment.

With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?

In the design of cryptographic protocols, single trusted parties are usually avoided whenever possible. The concentration of responsibility in one place creates a single point of failure, and this is where adversaries usually launch their attacks. The best countermeasure to mitigate this problem is distributing the trust to multiple independent parties (see Question 2.1.4), but currently no efficient solution exists for multiple parties to print confidential documents in a distributed manner. Defining the printing office as a single trusted party seems therefore unavoidable in the current setting (note that trusted printing offices are also needed in purely paper-based elections).

To avoid potential weak points that undermine the security of the whole system, it is crucial to design the printing process with uttermost care. Every critical step in the process must be protected by organizational measures and ideally involves multiple persons. To avoid online attacks by remote adversaries, defining the printing procedure as an offline process is highly recommended. Ideally, the printing process is entirely detached from the rest of the system, except that shares of the confidential information to be printed are received from the control components and that printed documents

are submitted to the voters. In this model, the responsibility of the printing office is reduced to printing documents based on inputs provided by external parties, which is a deterministic procedure. Limiting the responsibility to the printing office's core task is an important preconditions for keeping the necessary organizational measures as simple as possible.

Attributing responsibilities to the printing office other than printing is not recommendable, especially if the responsibilities involve cryptographically relevant tasks such as generating random numbers. Suppose a scenario in which the printing office is responsible for generating random voting, verification, confirmation, or finalization codes based on its own pseudo-random number generator (PRNG). This means that a simple attack against the PRNG (for example using a weak random seed) or a bug in its implementation could fully undermine the security of the whole system. Such an attack could be prepared long in advance of an election and would remain undetected with high probability. It is clear that such critical tasks at the printing office attract the attention of potential adversaries and should therefore be avoided.

Generally, we recommend the printing procedure to be designed as a deterministic offline process with the printed voter documents as the only output. Non-volatile memory used to temporarily store confidential information should be physically destroyed at the end the process. Any channel used for transmitting confidential information to the printing office must be protected accordingly.

Question 2.1.4 (Independence)

The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack.

Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?

Distributing trust to multiple independent parties is a standard technique in the design of cryptographic protocols. Ideally, the parties provide mutual *probabilistic independence* with respect to possible individual failure events. Then, if p_i denotes the probability of a single party i to fail in a 1-out-of-n setting, the whole system fails with probability $p = \prod_{i=1}^{n} p_i$, i.e., the overall failure probability of the system diminishes with every supplementary party added to the system. In practice, however, achieving this maximally possible degree of independence is almost impossible. If one thinks of a party as a composition of hardware, firmware, system software, and application software, it is very difficult

to design and equip multiple such parties with distinct components on every abstraction layer. Establishing independence is also difficult relative to the people involved in charge of designing, installing, and operating these systems, because these people for example can be compromised by the same external adversary. Generally, increasing the level of mutual independence between multiple parties always comes with additional costs.

Relative to the application software containing the code for cryptographically relevant computations, two types of flaws must be distinguished. In each case, if the same flaw is present at the same time across all parties, then the security of the whole distributed system is at risk. This is the worst-case scenario that needs to be avoided. The first type of flaws consists of unintended and undetected software bugs, which undermine the security of the cryptographic building blocks or the cryptographic protocol. Measures to avoid such problems have already been discussed (see Questions 2.1.1 and 2.1.2). If these measures are effective, i.e., if the application software contains no critical unintended flaw, running the same software by multiple parties does not create an additional risk. To get there, maximal efforts should be invested into checking the correctness of the software. Opening this process to the public augments public confidence.

The second type of flaws consists of intended bugs or protocol deviations, which may have been injected into the application software by malicious attackers at any point in the development process. Intentional flaws of that type can also be infiltrated over a malicious compiler or a manipulated virtual machine, in which the software is executed. The chance that attacks of that kind remain unnoticed is clearly much higher than visible manipulations in the source code. Similar attacks are also possible at other layers of abstraction, for example in linked software libraries or in the system software. A critical building block is always the random generator, which is often implemented based on primitive functions of the system software. If lack of independence makes launching a coordinated attack against all parties equally difficult to launching a single attack against an individual party, then the security of the whole distributed systems is at risk. It is therefore crucial for each party to minimize the risk of installing manipulated software components, for example by accepting them only from trustworthy sources or by checking corresponding software certificates. Adequate policies must be defined by the operators, and their application must be enforced and controlled in a strict manner.

Question 2.1.5

Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?

The question about the authorship of the verification software is not significant as long as the software has undergone a thorough public reviewing process with a positive outcome.

A precondition for both writing and reviewing the verification software is a specification document, which describes the verification input and all necessary verification steps in sufficient details. This document must be aligned with the protocol and system specification to a maximal degree. Its correctness and completeness must have been evaluated beforehand by independent cryptographic experts. Multiple implementations of the verification software based on this document may be useful for augmenting public confidence, as long as they all offer the necessary quality requirements to sustain public reviewing. Another measure for augmenting public confidence is to run the verification software on different platforms, i.e., to run the verification process by different people in different environments, which are difficult for an attacker to control simultaneously.

Question 2.1.6

The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components/auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?

Generally, facing the adversary with heterogeneous combinations of hardware, software, processes, and people increases the complexity of a coordinated simultaneous attack against multiple installations of components with identical functionality. While equally powerful hardware and operating systems are available from different providers, this is not necessarily true for commonly used libraries such as GMP, which is a de facto standard for efficient computations with large integers. At this level of abstraction, requiring fully disjoint code bases across all parties in a distributed system is unrealistic. In our answer to Question 2.1.4, we have already discussed measures to minimize the risk of installing manipulated software components. Assuming that these measures are effective are successfully applied on all layers (from the system up to the application software), then running exactly the same pile of software components on every involved machine may become an acceptable option, as long as these machines are installed and operated in different environments and by distinct people.

Question 2.1.7 (Other Forms of Verifiability)

The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, userfriendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance

voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally.

How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability?

Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?

Switching from an untrusted to a trusted voting device would create a totally different starting point for building end-to-end verifiable voting protocols. Metaphorically speaking, this would be equivalent to sending sealed ballot boxes to the voters' homes. In such a setting, cast-as-intended verification becomes meaningless, because manipulations of the voter's intention by the device are ruled out by definition. The design of the protocol could then focus on providing recorded-as-cast or even counted-as-cast verification, for example using techniques similar to the *tracking numbers* used in the Selene voting system [21]. Providing access to the election data over a public bulletin board is usually a precondition for such techniques. Access must be given to either to the general public (including the voters themselves) or to trusted third parties in charge of conducting the verification on behalf of the voters (electoral commission, preferred political party, expert groups, etc.). Note that stronger trust assumptions in one place of a cryptographic protocol may allow providing stronger security properties in another place of the protocol. The above-mentioned Selene system for example allows a certain level of coercion-resistance based on the particular construction of the tracking numbers. We see providing trusted voting devices mainly as a necessary condition for dematerializing the voting process into a fully digital process.

Generally, it will always be necessary to fine-tune a protocol for a specific application use case and a given adversary model. The most appropriate protocol is usually the one that offers the best compromise between conflicting security, efficiency, and usability objectives. A typical example of conflicting security objectives is long-term privacy vs. public verification in the presence of a public bulletin board. If unlimited public access is given to the election data via the bulletin board, which includes public access to all encrypted votes, then vote privacy may be at risk sometimes in the future, for example when powerful quantum computers will be available (see Question 2.2.1). The decision of limiting this risk by restricting access to the bulletin board to registered auditors is comprehensible, but it strongly limits the applicability of universal verification to a small number of people. Trade-offs like this can hardly be solved by technical means.

Question 2.1.8

The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?

To ensure that the protocol is implemented according to its specification, it is important to achieve correspondence between specification and code to the maximal possible degree, for example using exactly the same terms, symbols, and names for variables, functions, or algorithms. Perfect alignment between specification and code must be seen as a quality criterion of highest priority. This implies that even the smallest change in either the specification or the code needs to be updated immediately on the other side. Ideally, if the specification and the code are always perfectly aligned (in which case they can be seen as *the same thing*), then checking their correspondence becomes a diligent but routine piece of work, which does not necessarily require the involvement of cryptographic experts (their main responsibility then lies in checking the specification). To facilitate a good approximation of this ideal model and for making the code accessible to the broadest possible audience, dependencies to complex third-party libraries or software frameworks should be avoided to the greatest possible extent. Other complexity-reducing software design principles should be applied whenever possible. The software itself should be well organized and properly documented. Direct links between specification and code should be clearly visible, and possible deviations should be marked and documented. Building the code and running the tests should be straightforward.

If such a close match and software quality is achieved by following the above guidelines, making both the specification and the code available to the public (ideally without barriers such as unnecessarily restrictive NDAs) will even have a higher impact. Compared to the 2019 document and code release, the increased accessibility would attract even a higher number of potential public reviewers. This increases the likelihood of detecting even the most subtle flaw in the code at an early stage. An even broader discussion round would also be beneficial for building up a positive public perception. This is how the commitment to maximal transparency may turn into a powerful trust-establishing measure.

The question of how to ensure that the correct software as examined and authorized based on the source code is running in the deployed system has already been discussed (see Questions 2.1.4 and is 2.1.6). It lies in the nature of the matter that such a proof is notoriously difficult to establish. Imposing strict deployment policies based on known best practices seems to be an acceptably good strategy to mitigate this problem. In a

system with distributed trust, applying these policies individually to every component decreases the risk of creating identical vulnerabilities multiple times by repeating the same mistakes.

2.2 Security Related Risks Top-Down

Question 2.2.1

Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?

The effectiveness of cast-as-intended verification based on checking verification codes strongly relies on the voter's awareness and willingness to conduct corresponding checks and to react accordingly in case of a failure. If instructions are given to the voter during the online voting session, for example by displaying the number of a hotline to call in case of mismatched codes, then voters can easily be deceived into doing something else (for example calling a different number with an endless on-hold queue) by a manipulated user interface. There is a whole range of such attacks, which only recently have been analyzed systematically in experimental studies [15]. For lowering the risk of such user-interface attacks, it is important to improve the quality of the instructions given to the voters on paper to the maximal possible extent. With regard to the system offered by the Swiss Post, another recent study has demonstrated a number of eminent weaknesses in the user interface [19]. These discoveries indicate that only insufficient attention has been given to this type of attack in current implementations.

In Section 3.1 of the VEleS annex [1], the scenario of a manipulated user interface by an administrator is mentioned under 3.1.21. However, conducting such an attack directly on the voter's computer by malware or DNS-poisoning seems to be more effective for a powerful external adversary. We recommend to expand to threat model accordingly.

Question 2.2.2

Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?

In the light of the threat described in Question 2.2.1, additional measures should be taken by system providers to decrease to effectiveness of this type of attack. Conducting evaluations and reviews of the user interface by usability experts, possibly in combination with observational and experimental user studies, is such a measure. This may help

to improve the simplicity and clarity of the voting process from a voter's perspective. Particular attention must be given to the verification steps in the process, which may be difficult for voters to understand. Individual verification can only become effective if voters are fully aware of the importance of conducting these steps in exactly the prescribed order. For this, offline and online instructions given to the voter must be aligned and optimized with the help of experts.

Question 2.2.3

Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?

The negative publicity caused by releasing imperfect code and documentation to the public shortly before the planned launch of the new Swiss Post system could have been avoided by a different transparency policy. Maximal transparency is recommendable for all cryptographically relevant parts of the system (that's where the main flaws in the system have been found) at the earliest possible stage in the process. In our vision of perfectly aligned cryptographic specification and code throughout the development process (see Question 2.1.8), we see little reasons for justifying the withholding of either the documentation or the source code from the public. For cryptographic experts from the e-voting community, finding the reported flaws was relatively easy, i.e., releasing the specification at any earlier point in time would have given the system providers more room for fixing the flaws in time. We recommend public examination to become a precondition for the certification process, not vice versa.

Relative to conducting a PIT as an "ultimate" security test before launching the system, we are less convinced of the effectiveness of this measure. As the example of the Swiss Post PIT in February and March 2019 has demonstrated, conducting a PIT in combination with a bug bounty is likely to create massive public attention, but the benefit of the outcome seems to be relatively small given the fact that all major flaws have been detected based on the published documentation [2, 5–8, 16, 17].

Question 2.2.4

Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure,

etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).

A general comparison to applications in other security-critical fields is problematical, because requirements and trust assumptions diverge strongly and are often not very clear. Usually, trust assumptions are much stronger, especially those related to the central infrastructure. Protecting the central infrastructure against failures or attacks from external adversaries is therefore often the main focus in the security concepts, but general statements about the effectiveness of particular measures are not possible. In many areas, providers are rather non-transparent relative to the design and implementation of their security concepts. Public examination based on open documents and source code is almost non-existent.

In recent years, a tendency of introducing even stronger trust assumptions have been observed in some areas. In online banking, for example, monthly statements on paper have been replaced widely by electronic documents, and physical factors in two-factor authentication have been substituted by mobile phones. Such examples of complete dematerialization are possibly driven by improved usability promises, but they almost always come with additional trust assumptions. By requiring compliant systems to distribute code sheets on paper, VEleS remains more cautious in this respect.

For a completely verifiable VEleS-compliant system, which has been designed and implemented with the goal of achieving the highest possible quality level in both documentation and code (see Questions 2.1.2 and 2.1.8), and which has gone through an extensive internal and public examination process (see Question 2.2.3), it seems to be relatively safe to say that cast votes are better protected than security-critical data in other fields. However, this statement excludes the protection of the voter's privacy on the client computer, which is an untrusted party in the VEleS adversary model. And it relies on the precondition that the involved control components run in sufficiently independent environments (see Question 2.1.4). Note that problem of modified voter instructions by a manipulated user interface is unique to the electronic channel (see Question 2.2.1).

Question 2.2.5

Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels).

Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security?

Which kind of powerful organization might try to manipulate or read votes? What methods

would they most likely choose? Are there also reasons why they would not apply certain methods?

On the premise of the previous question, according to which a perfectly VEleS-compliant system is available for internet voting, it seems that circumventing security measures for powerful adversaries is more likely to succeed at other locations. A recent study of the Swiss postal voting process has given a good summary of possible attack vectors in classical paper-based systems [14]. In the light of these results, attacks against relatively unsecured equipment at electoral offices seems to a more effective way of manipulating the result of an election. Although attacks of that kind are limited by the size of the attacked counting circle, they may still be effective enough to influence the final outcome, especially in a close rally. Another promising attack strategy for a powerful adversary is influencing of voters by social engineering, particularly over social media or by filter bubbles in search engines.

2.3 Selected risks

Question 2.3.1

Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly).

Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?

In our responses to Questions 2.2.1 and 2.2.2, we have already discussed the problem of an attack against the user interface and the online instructions given to the voters. There are two recent publications on this subject [15, 19], which both come to the conclusion that current voting material on paper and online user interfaces are not optimal for guiding the user through the voting process. This reduces the voter's awareness that the verification steps are crucial elements in the system's security concept. Some voters will probably never understand the process completely, but they will understand what they have to do if clear instructions are available. To diminish the impact of user interface attacks, these instructions must be given mainly on paper (or over other secure channels). As the user experiments in [15] have shown, the number of voters conducting the verification steps can be increased by an optimized user experience of the voting process.

Question 2.3.2

> *The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server.*
>
> *What measures could be taken in order to maximize the number of voters who check the fingerprint?*

Advising voters to check fingerprints of TLS certificates in their browser is unlikely to add much to the overall security. Average voters, which are not familiar with this step, will probably not understand its meaning and consequences. Therefore, we recommend restricting the advice given to the voters in the paper instructions to entering the correct URL by hand and to checking the padlock symbol displayed by the browser after establishing a TLS connection to the server. Note that this measure only prevents the simplest cases of attacks based on URL redirection, DNS cache poisoning, or other exploits on the application layer. In the scenario of an attack against the web browser, for example by infiltrating malicious code through a poisoned browser extension, arbitrarily sophisticated forms of browser hijacking can be implemented easily (which includes displaying the correct URL together with a closed padlock symbol).

In any of the above scenarios, it is important to understand that submitting a manipulated vote can still be detected by individual verification, even if voters are redirected to a clone of the voting server that acts as a man-in-the-middle. In the DNS poisoning attack against the Geneva online voting system in 2018, this important aspect was widely misinterpreted in the press coverage of the event. The main threat in such a scenario is the user interface attack malicious instructions on the website, which aims at decreasing the percentage of voters performing the necessary verification steps (see Questions 2.2.1 and 2.3.1).

Question 2.3.3

> *The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side.*
>
> *Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?*

Under the assumption that the browser itself is not under attack, then checking that the correct client application is loaded and running is principally possible by inspecting the source code in the web browser's developer tools. But this possibility is rather

theoretical than practical. While checking a complex source code is a far too complicated procedure, which could at best be conducted by someone with sufficient background knowledge in web technologies, average voters will probably not even understand the purpose of this step. Since the consequences of an attack with malicious web client code are the same as in the scenario of Questions 2.3.2, educating the voters about individual verification appears to be the most effective counter-measure. We recommend the removal of corresponding text passages in Section 4.4 of the VEleS annex [1].

Question 2.3.4

> *How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who/which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant?*
>
> *Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.*

The development of quantum computers undermines the number-theoretic and algorithmic assumptions of today's cryptographic building blocks (see Questions 2.1.1 and 2.1.7). While it is relatively safe to assume that sufficiently powerful quantum computers will be available in the possibly not so far future, it is hard to predict the point in time when they become relevant. Note that for creating an environment that allows controlling quantum physical effects, such a machine must be able provide temperatures near absolute zero. Since this requires large and expensive technical installations, it is safe to assume that the availability of quantum computers will always be limited to large and powerful organizations.

To prevent the decryption of ciphertext votes by quantum computers, restricting access to the bulletin board is not a satisfactory solution. It is very hard to ensure that no data from the bulletin board will ever leak. Further research will be necessary to design new cryptographic voting protocols that withstand attacks by quantum computers. Quantum-resistant cryptography has become a lively research areas in recent years.

Question 2.3.5

> *The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI?*

Vote privacy attacks by malware on the voters' personal computers remains an almost unavoidable risk in remote electronic voting. By being maximally careful with respect to installing software and updates only from trustworthy sources, it is true that users can reduce this risk, but it is impossible to eliminate it completely. Powerful adversaries will always find a way of infiltrating code into computers of average users, independently of whether they follow guidelines like those by MELANI. Note that some of the MELANI guidelines, for example the advice to limit or deactivate the execution of JavaScript in the web browser, may even be counterproductive. We recommend referring to the most relevant guidelines as part of the voter education strategy, but not to expect a significant impact in reducing the risk of a large-scale vote privacy attack.

Question 2.3.6

Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?

Compared to voting in private voting booths, preventing vote buying and coercion is much more challenging in a remote voting system. The main problem is the remoteness of vote casting in an uncontrolled environment, not the type of channel used for submitting the vote. Postal and electronic voting are therefore not very different in this respect. The fact that postal voting is so widely accepted in Switzerland indicates that vote buying and coercion is not a real threat in places with strong and stable democratic traditions, even if individual cases can not be excluded (for example within families). We don't expect this threat to increase much with the introduction of an electronic voting channel.

3 Independent Examinations

Question 3.1

> *Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes.*
>
> *Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?*

The fact that several critical problems in the design and implementation of the system have been overlooked in the examinations performed during the certification process can have multiple reasons:

- The examinations were not conducted with sufficient care.
- The people conducting the examinations were not sufficiently qualified.
- The total scope of all examinations was not sufficiently comprehensive.
- The different examinations were not sufficiently well coordinated.

From today's retrospective view, it seems that the best explanation comes from a mix of the above reasons. To improve the coordination, we recommend that an independent person responsible for the big picture is hired for leading and monitoring the whole examination process.

An ideal development and examination process follows a strict bottom-up procedure, in which the next stage is only tackled once the previous stage has been fully achieved. In such a ideal process, software development only starts after finishing, publishing, and approving the cryptographic specification of the protocol. The early publication of corresponding documents invites additional independent examiners from anywhere in the world to participate. As the experience from last year shows, this seems to work quite well (multiple critical cryptographic flaws have been detected within a few weeks after publication).

Similarly, deployment and operation of a system ideally only starts after finishing, publishing, testing, and approving its source code. Here a distinction between *cryptographically relevant* and *cryptographically irrelevant* code would be helpful for doing certain tasks in parallel, but then the system should be designed to provide a clear interface between these code segments. To facilitate the examination of the cryptographically relevant code segment, we refer to our software quality vision presented in our response to Question 2.1.8. Then again, publishing the source code is likely to attract people from many different places in the world to become external code reviewers. Installing bug

bounties may be an effective additional measure for attracting an even higher number of external people.

Generally, we recommend conducting the certification process only *after* a sufficiently long public examination period (see Question 2.2.3), and only when all relevant findings of the public examination have been taken into account. During the official certification process, well-defined tasks can then be assigned to examiners within the scope of their specific qualification. The person in charge of the big picture ensures that all critical examination areas are covered, especially those related to the cryptographic protocol and its implementation. For examinations related to infrastructure and operation, ISO 27001 or other standards from the ISO 27K family seem to provide appropriate guidelines.

Question 3.2

In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.

The time period needed to fix a newly discovered vulnerability is known as the *patch gap*. Attackers may take advantage of the patch gap, if they manage to develop exploits more quickly. In regular applications, which are available to users on a 24/7 basis, this creates an attack window during which the security of the system is at risk. If an online voting system is used for political elections, which only take place a few times a year, this problem only exists if the patch gap overlaps with an election period. If this happens anyway, the extent of the problem and the resulting risks have to be evaluated from case to case. In the extreme case of an ultimately severe problem, it can happen that aborting the election becomes unavoidable. Should an ongoing election be continued during the patch gap, reporting the problem and the risks to the public is important. Crisis management and communication strategies should be prepared for such cases.

The situation is slightly different if new vulnerabilities are discovered between two election periods. If a patch can be rolled out quickly enough, the question is whether to accept the patched system for the next election without renewing the certification. Here again, decisions should be taken on a case-by-case basis according to the threat, the risks, and expected effectiveness of the patch. To obtain reliable and sufficient information in time, we recommend setting up a task force to investigate the problem and evaluate the proposed solution. If a severe problem can not be fixed within the limited time period, system providers and election administrators should be prepared to temporarily close down the electronic channel for the next election.

Question 3.3

Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

The credibility of the people and organizations appointed with the examination clearly influences the public perception of the outcome. High credibility is usually given to people that are not on the direct payroll of the system providers, for example to members of independent academic institutions or to experts from specialized associations engaged in IT security topics. Independently of who is appointed with the examination, credibility is strengthened by publishing their reports no matter what the findings are. We expect the strongest possible credibility to result from an extensive public examination process, in which experts from different areas and with different qualifications have participated voluntarily (see Question 3.1).

Question 3.4

Which adaptation/clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?

According to the requirements listed in Section 5.1 of the VEleS annex, the examination of the cryptographic protocol focuses on providing cryptographic and symbolic proofs of the desired security goals [1]. These proofs are mandatory for achieving provable security also on the protocol layer (see Question 2.1.2). The problem with these proofs is that they sometimes refer to a model, in which certain cryptographically relevant details remain unspecified. A typical example is a model in which so-called independent group generators (a central concept in mathematical group theory) are assumed to exist for proving the correctness of a mix-net. If a high-level property of the protocol is proven in this model, then the independence assumption relative to the generators becomes a precondition for the property to hold. But this precondition can only be checked, if the protocol specification includes an algorithm for finding independent generators in a publicly verifiable manner, otherwise it is possible that this check slip through the net of the conducted examinations. This is roughly what happened during the certification of Swiss Post system, in which checking the independence of the generators was overlooked by everyone. Only public examination has revealed the problem [8, 16].

To avoid such problems in the future, or at least to detect them earlier in the process, an examination of the protocol design and an evaluation of the specification documents should be conducted by experts with strong background knowledge in cryptographic protocol design. In our vision of an ideal bottom-up development and examination

process (see Question 3.1), settling the cryptographic protocol with all its subtle details is one of the first and most important steps in building a solid cryptographic foundation of the system. The cryptographic and symbolic proofs are important to strengthen this foundation.

Question 3.5

How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?

Software updates are necessary and unavoidable. Whether such an update should trigger certain re-examinations depends on the update itself. We have already proposed a software architecture, in which cryptographically relevant and cryptographically irrelevant code is strictly separated (see Question 3.1). If an update affects the cryptographically relevant part of the code, then the re-examination is mandatory. The extent of the re-examination in such a case depends on whether the update affects the protocol specification and the code or the code only. Protocol changes may even affect the cryptographic and symbolic proofs. All cryptographically relevant changes should be clearly motivated and well documented.

Minor software updates that are restricted to the cryptographically irrelevant part of the code may not automatically imply the necessity of a thorough re-examination by external examiners. We recommend conducting general software examinations periodically, or at least when a major new releases is available. We also propose periodical examinations of the cryptographic parameters and their alignment with current recommendations. Certificates related to infrastructure and operation must be renewed when they expire.

Question 3.6

How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them/to the public?

We have already stressed the importance and potential of opening the examination to the public (see Questions 2.2.3 and 3.1). In a maximally transparent system, public examination is a continuous process with sometimes unpredictable outcomes. System providers and election administrators should therefore be prepared to obtain important feedback at any inconvenient moment (see Question 3.2). An official platform for submitting feedback can help keeping this process under control. It must be clear to everyone that this platform will release any reported flaw after a certain time period and that authors will

receive corresponding credits (see Question 4.6). Periodical bug bounty programs may create an additional incentive for people to participate.

Question 3.7

How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?

Given the complexity of the subject, different and conflicting opinions are unavoidable, especially in a process in which the public is invited to participate. If such conflicts arise within the official mandates given to different experts, maximal efforts should be invested into resolving them to everyone's satisfaction, even if this is notoriously difficult. In case of an unresolved issue, final decisions must be taken on a case-by-case basis by either the person leading the examination process or the responsible authorities.

Conflicts with participants of the public examination should be treated similarly, provided that their opinions are well-founded. Unjustified opinions should be treated with respect, for example by providing material with additional background information.

4 Transparency and Building of Trust

Question 4.1

How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the security community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?

In a delicate application area such as online voting, which affects all members of a democratic society, any form of disclosed or restricted access to relevant documents and code creates annoyance and mistrust, not only in the security community, but also among the general public. Providing maximal transparency with respect to every aspect of such a system is a different mindset, which we regard as fundamental for a successful project. We have already discussed the benefits of a continuous public examination process, which involves both the cryptographic protocol and the source code (see Questions 2.2.3, 3.1, and 3.4). Well-directed incentives could possibly lead to an even higher number of voluntary participants, but the experience from 2019 shows that the delicacy of the topic itself already creates enormous world-wide interest.

Ideally, designing and implementing an online voting system is not impeded by intellectual property restrictions or more generally by commercial interests. This does not exclude organizations with commercial interests from developing a system or becoming a system provider. Appropriate non-commercial software licensing models exist, which permit publication, redistribution, or modification of the source code for personal or academic use. This gives sufficient room for the public examination process, but at the same time retains the intellectual property of the software owner.

Question 4.2

What should the scope/coverage of the published documentation be in order to achieve meaningful public scrutiny?

The documentation should be centered around the cryptographic specification of the protocol. It should include sufficiently detailed descriptions of all relevant aspects (election parameters, trust assumptions, adversary model, communication channels, workflow, messaging, computations, cryptographic parameters, security definitions, formal proofs, etc.). Ideally, third parties should be able to implement prototype implementations of the protocol in reasonable time, solely based on the publicly available documents.

In our collaboration with the State of Geneva, we were assigned to lead the development of the new CHVote protocol [10]. The level of detail that we achieved in the resulting document was sufficient for two students from our IT security bachelor program to fully implement the protocol in a single semester [11,12]. The key for them to advance quickly enough were the pseudo-code algorithms included in the CHVote documentation. Relative to computational processes, pseudo-code algorithms can be seen as the ultimate level of detail given in a paper document, which restricts the freedom of developers to the maximal possible degree.

Documents about the software architecture or the IT infrastructure may also be interesting for participants of the public scrutiny, for example for people inspecting the source code. Even if we consider these documents less useful for obtaining relevant feedback from the public, we still recommend their publication. In the mindset of maximal transparency, all aspects of the system are properly documented and nothing is withheld. This includes the reports from people conducting mandated examinations.

Question 4.3

When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?

We have already discussed our vision of an ideal development and examination process, which follows a strict bottom-up procedure (see Question 3.1). The two most important milestones in this process are the completion of the cryptographic protocol and the release of the cryptographically relevant part of the source code. We recommend including the public at every stage of this process, i.e., whenever documents or parts of the source code are ready to be given to mandated examiners, we propose releasing them also to the public. Note that conducting mandated and public examinations in parallel accelerates the whole process. Authorizations should only be given at the very end of the process.

Question 4.4

Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)

In the mindset of maximal transparency, nothing speaks against the publication of documents that go beyond the current VEleS requirements. The two given examples of test data and instructions for compiling and executing the code (ideally on regular hardware) are particularly useful for people participating in the examination of the source code. The ability to execute the code is a precondition for conducting a so-called *dynamic code*

analysis. Compared to a *static code analysis* based on only looking at the code, there are numerous benefits, for example the possibility to perform test runs or to run automated utilities. When performing comprehensive source code examinations, both static and dynamic code analysis should be included in a complementary manner. If the software building process is complex, it is essential to provide sufficient installation and configuration instructions, otherwise even experienced developers may not be able to compile and deploy the software in reasonable time. The lack of such instructions was one of the main criticisms raised against the Swiss Post system during the PIT in 2019 [3]. Our suggestion under Question 3.1 of introducing a clear separation between cryptographically relevant and irrelevant code may help to simplify corresponding installation procedures, especially for conducting a focused analysis of the cryptographic aspects of the code.

Question 4.5 and 4.6

Under what conditions should public reactions be discussed?

- *To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.)*
- *Which entities should be involved in the discussion?*

Should the system providers publish existing/fixed security breaches? Through which channels? When?

We already proposed the installation of an official platform for the submission of feedback during (or even beyond) the development and examination period, similar to common issue tracker tools in software development and version control systems (see Question 3.6). For maximal credibility of this platform, a mandate for running the platform should be given to a neutral third party. The platform acts as an interface between the participants of the public examination, the system provider, cantonal election administrations, the federal chancellery, and other involved parties.

In the mindset of maximal transparency, we recommend the publication of all reported issues after some time, such that all participants receive corresponding credits. Participant wishing to stay anonymous should be able to do so. Generally, the procedure for resolving and publishing reported issues should be as efficient and transparent as possible. The *responsible disclosure* principle should be applied in cases of vulnerabilities with high impact, which means that the involved parties agree on a time period for repairing the found issue. Disclosure deadlines of 90 or 120 days are common in practice, but depending on the number of days left until the next election, this may be too long or too short. Financial compensations should be considered in extreme cases. Situations of conflicting opinions or disputes have already been discussed under Question 3.7.

Question 4.7

Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT/bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?

To the best of our knowledge, the security benefit from the received PIT feedback was relatively modest, especially in comparison with the benefit of the feedback received form participants looking at the cryptographic protocol and the source code. The PIT as it was performed is rather an infrastructure test. In regular applications with a fully trusted central infrastructure, a PIT of that kind can be useful to detect unknown vulnerabilities, which may allow an external adversary to break into certain components of the system and then steal, destroy, or manipulate their data. In principle, this could also happen in an attack against a verifiable online voting system, but this does not automatically weaken the security provided by the cryptographic protocol.

The most important question regarding a system with distributed trust is to evaluate the probability of a simultaneous attack against all control components (see Question 2.1.4). An example of a successful attack would be the stealing of their shares of the private encryption key, in which case vote privacy could possibly be broken entirely. More focused PITs, for example one with the specific goal of stealing these keys, would therefore be more beneficial than the general PIT conducted in 2019. For that, it would be sufficient to provide a clone of the real system running in parallel, which can be tested and attacked at any time, with as little restrictions as possible. Social engineering, for example, is a very important factor in many successful attacks in practice. It is therefore not surprising that excluding it from the attack vector has been perceived mostly negatively.

Question 4.8

Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust?

Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?

We see enforcing low-scale use of Internet voting as a strategic measure for limiting the overall risk in case of a fraud, not for establishing public trust. Possibly even the

opposite is true: by artificially limiting the usage of the electronic channel to a small number of voters, electoral authorities seem to admit that large-scale electoral frauds remain possible even in a system providing individual and universal verification. Public trust in online voting mainly comes from a top-quality product, maximal transparency, public examinations, and universal verification, not from risk-limiting regulations. This said, we are not entitled to judge the strategic benefit of such regulations (for example for lessening the resistance of critics).

Question 4.9

How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission/a separate administrative body charged with running votes)?

In the light of the verification process models proposed in [9], it seems reasonable to assume that the tallying and verification process conducted by the cantons will turn out to be more complex than what one might expect. Independently of how the details of this process are specified, it is again crucial to apply the principle of maximal transparency, for example by defining clear and transparent *standard operation procedures* (SOP), or by making the process observable in the sense of a public ceremony (for instance using video broadcasting). People attending the ceremony in person should represent the whole electorate, for example by inviting representatives of all major political parties. They must receive a training, in which their understanding of the individual steps of process.

Question 4.10

Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?

Separating the electronic voting shares of election results from the shares of other voting channels is a necessary precondition for universal verification. By limiting access to the election data and restricting universal verification to cantonal authorities and auditors in an internal process, it is possible in principle not to publish the electronic voting shares, but this would imply that the public is entirely locked out from the universal verification process. Even if public participation in the verification process is not a conceivable option given the long-term privacy problem (see Questions 2.1.1 and 2.1.7), we still consider it as the ultimate tool for establishing credible election results.

Not publishing the electronic voting shares of the election results is also totally incompatible with the mindset of maximal transparency. We could imagine people to become skeptical when partial results from the electronic voting channels remain invisible. On the other hand, we could also imagine people to become skeptical in a situation in which shares from different voting channels differ from each other in a statistically significant way, even if the difference can be explained from a sociopolitical perspective (for example by observing age differences in corresponding voter groups). Nevertheless, we believe that publishing the electronic voting shares remains the better option for establishing credible election results.

Question 4.11

What additional transparency measures could promote security and/or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

Transparency measures do not necessarily increase trust, but everything that is not transparent is in a way suspicious. The question regarding the publication of documents such as the meeting minutes of an electoral commission is whether they are relevant for the public. If this is clearly not the case for a certain type of documents, we do not see any added value coming from releasing them to the public. Publishing a large amount of irrelevant documents could also be perceived negatively, for example as a sign of not having a clear view of the security-critical topics. The relevance question regarding a certain type of documents (or other transparency measures) can only be answered on a case-by-case basis after careful analysis.

Question 4.12

Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?

The problem with statistical plausibility checks based on election results only is the definition of useful threshold values, which determine the borderline for triggering an alarm. The selection of these values is a trade-off between generating false positives (values selected too loosely) and false negatives (values selected too strictly). Both cases are highly problematical, because manipulations are either not detected when they exist or suspected when they don't exist. This can create very confusing situations, for example by triggering an alarm even if universal verification has been successful. To avoid such

situations, we recommend conducting statistical plausibility test at most as an additional measure in the internal monitoring of the system.

Statistical plausibility checks based on election results should not be confounded with another type of post-election audit called *risk limiting audit* [18]. This technique helps to increase the credibility of the election result by manually checking statistical samples of paper ballots. As such, they can only be applied to an electronic voting system with a paper trail and are therefore not relevant for the Swiss case.

5 Collaboration With Science and Involvement of the Public

Question 5.1

Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must/could be taken to meet or promote these conditions and thereby participation?

1. *Participation in «public scrutiny»*
2. *Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers*
3. *Supporting the public administration in the further course of the trial phase, e.g, at implementing the measures currently being defined in the course of the redesign*

The willingness of experts from academic institutions to participate in the development or examination of an online voting system is usually relatively high, independently of whether their participation is motivated by an official (paid) mandate or takes place on a voluntary basis. Their general attitude towards a successful project is usually very positive, as long as the conditions of the project and the framework of their collaboration remain compatible with general principles of academic research. These principles include the freedom to speak publicly about all thematically relevant aspects of the project or to exploit the findings of the engagement for scientific purposes. Restrictions based on non-disclosure agreements or intellectual property concerns are usually not very welcomed in scientific communities (see Question 4.1). Most scientist live the principle of maximal transparency in their daily work.

Another form of scientific participation could be initiated by providing funding for independent e-voting research. The cryptographic building blocks of the protocols used in the second-generation systems from today have been developed a decade ago or more. Current research should therefore focus on developing new building blocks and protocols to overcome remaining problems such as coercion-resistance, everlasting privacy, or complete dematerialization. If sufficient research projects in these areas are funded today, their results will be available for the systems of the next generation.

Question 5.2

Which are the conditions to be met in order for representatives from science to participate in the political debate?

Political debates are usually conducted between different political parties and other interest groups. The purpose of such a debate is to discuss a political subject from different

perspectives and to determine the grounds for possible compromises. This process is driven by the participants' basic values, convictions, and interests, and also by the goals in the agendas of their political parties.

The role of a scientist in an ongoing political debate is not to participate in the debate itself, but to make research results and conclusions available to the broad public. Scientists try to collect evidence and provide facts in a systematic manner. In discussions, they try to argue objectively based on unbiased premises. For the case they are needed in a debate for clarifying certain questions in a dispute, it is important for them to protect their independence and freedom to speak in project collaborations with the interest groups involved in the debate.

Question 5.3

How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?

Scientific recognition is achieved by publishing new findings in peer-reviewed publications, ideally in publications with a high impact and reputation in respective fields. Most scientific publications today can be accessed freely on corresponding online platforms, but they are often not written for the general public. To better communicate state-of-the-art methods and latest discoveries to a broader audience, some sort of translation into a less technical language is necessary. Platforms for publishing such popular-science articles exist in large numbers. It is also possible to explain complex technical relationships more easily in video clips. Using video streaming platforms or social media, the broad dissemination of such video clips is not difficult to achieve today.

To explain a complex online voting system to a broader audience, we recommend deriving a demo system from the real system, which offers additional explanations about the involved cryptography and the process running behind the curtains.

Question 5.4

Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?

To address as many voters as possible, information should be provided at different levels of detail, from general educative descriptions of basic concepts such as verifiability or distribution of trust to very detailed technical descriptions of specific cryptographic

subtleties. The addressed audience should be clearly indicated in each document. For maximal clarity, the terminology used should be consistent across all documents. In documents addressing a broad audience, a simplified language may help to present complex subjects and concepts in an understandable way. To limit the total amount of information provided, these documents should focus on the most relevant topics. FAQ sections can help to efficiently address the most common concerns and objections in a systematic way.

Question 5.5

Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust?

- *Public debates on selected issues*
- *Hackathons around selected challenges*
- *Others you might think of*

The three editions of the *Swiss E-Voting Workshop* in the years of 2010, 2012, and 2014 were attempts to start fruitful discussions on questions related to online voting. The events attracted participants with different backgrounds: scientists, system providers, cantonal election administrators, journalists, and even ordinary citizens. One of the goals of the organizers was to promote verifiability as an indispensable requirement for the second-generation systems. This goal was reached with the publication of the 3rd e-voting report of the Federal Council verifiability in 2013, in which verifiability was given a central role in the security concept of the future systems [20].

Today, a similar series of events could possibly be helpful for guiding certain discussions into the right direction. It would be a platform for both critics and promoters of current systems to explain their respective viewpoints to a broad audience. Compared to discussions on Twitter and other social networks, the chance of being able to conduct a more constructive, respectful, and objective dialogue would be much higher.

6 Risk Management and Action Plan

Risk analysis is not our area of expertise. We may have one or the other opinion to some of the following questions, but we don't feel qualified enough for giving answers with substantial content. We only have one general comment regarding the publication of the produced documents. Here again, we recommend applying the mindset of maximal transparency, which means that documents containing information relevant for the public should be released as a matter of principle. By demonstrating that remaining risks have been evaluated in a systematic manner and that appropriate action plans for corresponding incidents have been defined, we believe that public trust can be strengthen even further.

Question 6.1

What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?

Question 6.2

What are the benefits and downsides of publishing the (dynamic) risk assessment?

Question 6.3

How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?

Question 6.4

Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?

Question 6.5

To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?

Question 6.6

Who can/should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?

Question 6.7

Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?

Question 6.8

Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?

Question 6.9

Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.7 Would this methodology be appropriate to handle the risks from the cantons'/system provider's point of view? Do you see any weakness/strong points in this methodology?

7 Crisis Management and Incident Response

Here again, we don't feel competent enough to respond to the following questions related to crisis management and incident response in sufficient details. In our process model presented in [9], we analyzed various scenarios of incidents related to the universal verification and proposed three different evaluation criteria for classifying the impact of the problem. We refer to the discussion in our paper without giving further comments.

Question 7.1

What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?

Question 7.2

What are the right events and thresholds for an activation?

Question 7.3

Who should be involved in crisis management, with which role?

Question 7.4

How should the communication be organised (internally and externally)?

Question 7.5

Are there already structures that should be involved in crisis management (e.g. GovCERT)?

Question 7.6

What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?

Question 7.7

What are the requirements and stakeholders for digital forensics and incident response?

Question 7.8

In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?

Question 7.9

How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?

References

[1] *Technische und administrative Anforderungen an die elektronischen Stimmabgabe*. Die Schweizerische Bundeskanzlei (BK), 2013.

[2] A. Driza Maurer. The Swiss Post/Scytl transparency exercise and its possible impact on internet voting regulation. In R. Krimmer, M. Volkamer, V. Cortier, B. Beckert, R. Küsters, U. Serdült, and D. Duenas-Cid, editors, *E-Vote-ID'19, 4th International Joint Conference on Electronic Voting*, LNCS 11759, pages 83–99, Bregenz, Austria, 2019.

[3] A. Fichter, A. Moor, and P. Recher. Postschiff Enterprise. *Republik*, 15. Februar 2019.

[4] P. Gaudry and A. Golovnev. Breaking the encryption scheme of the moscow internet voting system. In J. Bonneau and N. Heninger, editors, *FC'20, 23rd International Conference on Financial Cryptography*, Kota Kinabalu, Malaysia, 2020.

[5] R. Haenni. Attack on vote secrecy. Technical report, Bern University of Applied Sciences, Biel, Switzerland, 2019.

[6] R. Haenni. Generating random group elements (best practice). Technical report, Bern University of Applied Sciences, Biel, Switzerland, 2019.

[7] R. Haenni. Undetectable attack against vote integrity. Technical report, Bern University of Applied Sciences, Biel, Switzerland, 2019.

[8] R. Haenni. Undetectable attack against vote integrity and secrecy. Technical report, Bern University of Applied Sciences, Biel, Switzerland, 2019.

[9] R. Haenni, E. Dubuis, R. E. Koenig, and P. Locher. Process models for universally verifiable elections. In R. Krimmer, M. Volkamer, V. Cortier, R. Goré, M. Hapsara, U. Serdült, and D. Duenas-Cid, editors, *E-Vote-ID'18, 3rd International Joint Conference on Electronic Voting*, LNCS 11143, pages 84–99, Bregenz, Austria, 2018.

[10] R. Haenni, R. E. Koenig, P. Locher, and E. Dubuis. CHVote system specification. *IACR Cryptology ePrint Archive*, 2017/325, 2017.

[11] K. Häni and Y. Denzer. CHVote prototype in Python. Project report, Bern University of Applied Sciences, Biel, Switzerland, 2017.

[12] K. Häni and Y. Denzer. Visualizing Geneva's next generation e-voting system. Bachelor thesis, Bern University of Applied Sciences, Biel, Switzerland, 2018.

[13] J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. CRC Press, 2nd edition, 2015.

[14] C. Killer and B. Stiller. The Swiss postal voting process and its system and security analysis. In R. Krimmer, M. Volkamer, V. Cortier, B. Beckert, R. Küsters, U. Serdült, and D. Duenas-Cid, editors, *E-Vote-ID'19, 4th International Joint Conference on Electronic Voting*, LNCS 11759, pages 134–149, Bregenz, Austria, 2019.

[15] O. Kulyk, M. Volkamer, M. Müller, and K. Renaud. Towards improving the efficacy of code-based verification in Internet voting. In J. Bonneau and N. Heninger, editors, *FC'20, 23rd International Conference on Financial Cryptography*, Kota Kinabalu, Malaysia, 2020.

[16] S. J. Lewis, O. Pereira, and V. Teague. Ceci n'est pas une preuve: The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiabilty of the Scytl-SwissPost Internet voting system. Technical report, 2019.

[17] S. J. Lewis, O. Pereira, and V. Teague. How not to prove your election outcome. Technical report, 2019.

[18] M. Lindeman and P. Stark. A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, 10:42–49, 2012.

[19] K. Marky, V. Zimmermann, M. Funk, J. Daubert, K. Bleck, and M. Mühlhäuser. Improving the usability and UX of the Swiss Internet voting interface. In *CHI'20, 38th Annual ACM Conference on Human Factors in Computing Systems*, Honolulu, USA, 2020.

[20] U. Maurer and C. Casanova. Bericht des Bundesrates zu Vote électronique. 3. Bericht, Schweizerischer Bundesrat, 2013.

[21] P. Ryan, P. Rønne, and V. Iovino. Selene: Voting with transparent verifiability and coercion-mitigation. In J. Clark, S. Meiklejohn, P. Ryan, D. Wallach, M. Brenner, and K. Rohloff, editors, *FC'16, 20th International Conference on Financial Cryptography*, volume 9604 of *LNCS 9604*, pages 176–192, Christ Church, Barbados, 2016.

Redesign of Internet Voting Trials in Switzerland 2020

First name Oscar

Last name Nierstrasz

Organization University of Bern

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[1] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

NB: The responses to this questionnaire are given from the Software Engineering perspective, rather than strictly from the Security perspective.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

1.1 Trustworthiness in eVoting

You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.)

[1] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html
https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny)

Risk assessment: What are the biggest risks? Manipulation of votes? Disruption of service? Who stands to gain by violation of system integrity?

Players: Who are the players responsible for the components of the evoting system? What is their level of expertise? What is their track record? What stakes do they have in ensuring a safe and trustworthy solution?

Technology: What technical solutions have been chosen? Is there a continual monitoring of risks and threats? Is an auditing and certification process in place?

Which are the most important answers you need in order to conclude that internet voting is trustworthy?

The context is crucial. Everything hinges, for example, on the risk assessment. If coercion and vote buying are not issues, then which threats are important? Attacks from foreign states? Ransomware attacks? No system is perfect, so the important answers depend on which threats are important to mitigate.

How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)?

Less important than the origin is the process used to obtain the answers. In particular I would need to know how the risks have been assessed. Are they obtained through empirical and statistical data that have been objectively and systematically gathered, or are they based on "expert opinions"? Who are these experts and what are their credentials?

Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting?

The only element that appears to be missing, as far as I can tell, is a realistic assessment of the different categories of risks. There are (always) too many potential risks to realistically address them all in any technical solution. My question is, which risks are considered high priority, and what is their relative weight? For example, is the focus more on accidental risks (e.g., data loss through network or power failure, or software defects) or on deliberate, malicious attacks? These risks need to be continuously monitored and reassessed through a suitable auditing process.

We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

Quite simply, it is impossible to have a system that is perfectly safe. The best you can do is to design the system (including all players) to mitigate the most important risks, and to monitor the situation as the context changes over time.

2. Risks and security measures today and tomorrow

The Federal.Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7a, 7b and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[2] – are responsible for the following tasks:

- *Import from the electoral register*
- *Configuration of the vote (incl. generation of codes for individual verifiability)*
- *Preparation and delivery of voting material*
- *Splitting of private decryption key sand casting of test votes*
- *Support for Voters*
- *Detect double voting: Querying the internet voting system for every vote cast through postal mail*

---

[2] *The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.*

- *Decryption and counting of the electronic votes (incl. the test votes)*
- *Verification of results (by the means of universal verifiability and by comparison with the other voting channels)*
- *Transferring the results to the systems used by the canton for aggregating the votes from non-internet voting sources*

Goals

- *Risk-identification*
- *Identification of counter-measures*
- *Assess counter-measures*

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

2.1.1 Crypto-Protocol

The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?

There are two separate issues: the formal protocol vs its implementation. The protocol includes simplifying assumptions and typically ignores issues of platform. The protocol may itself be flawed. The protocol may only address some security concerns but not others. The implementation may be flawed, and incorrectly implement the protocol. The platform may be flawed and introduce vulnerabilities not addressed by the protocol.

The more the implementation depends on unspecified components (e.g., operating system functions, network features), the greater the risk will be that unknown vulnerabilities exist, and these can be exploited for attacks. By severely restricting the

number and size of needed components, the less the risk that there exist holes that can be exploited.

2.1.2 Effectiveness

The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?

If the protocol used has been custom-designed, then the risk of error is higher than if a well-known and vetted protocol is used. It is much more likely that the simplifying assumptions are problematic, i.e., that the protocol only addresses certain kinds of vulnerabilities but ignores others. (E.g., it ignores the possibility of man-in-the-middle attacks.)

2.1.3 Printing office

For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment.

With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?

The question seems strange to me. The return codes are generated by encryption. Decryption only occurs when the ballots are received and the votes tallied. There is no need for the printing office to be involved in the generation of the return codes. There should be just a single trusted entity charged with encryption and decryption of the codes. Unfortunately I could not find a complete description of the envisioned process (section 4 of the Annex only sketches the process), so perhaps (probably) I have misunderstood the question.

The need for a printing office is unclear to me in an electronic voting system.

2.1.4 Independence

The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack.

Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?

Every new interface adds new ways to attack the system. This makes it harder to verify that the end result is secure. It is better to have one system that can be analyzed. Multiple systems multiply the possible attacks. I am very sceptical about the notion that "independence" of components through multiple providers will improve security. Instead I would expect it to introduce yet more opportunities for attack.

2.1.5 Auditors' technical aid

Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?

The technical aid is not part of the technical solution, so introduces no new risk. The added benefit is that a separate implementation is used to verify, so this heightens the chance to catch additional errors. The only downside is the additional software development and verification costs.

2.1.6 Operating systems

The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?

The question is unclear to me. Is it about requiring support for multiple platforms, e.g., for users, or that the eVoting system itself must be based on multiple platforms? Neither requirement appears explicitly in the VEleS document as far as I could see.

Safety and reliability are helped by breaking the solution into small, simple, and independently verifiable components. Requiring them to be implemented on different

platforms, however, won't increase reliability. Requiring support for multiple platforms may, however, expose differences and weakness in individual platforms, but it is unclear if this is beneficial or not with respect to the targeted risks.

2.1.7 Other forms of verifiability

The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user friendliness was a strong concern. This is why voting with return codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally.

How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability?

I imagine that voters would want a simple way to verify that their votes are correctly cast and tallied. The large majority of voters would balk at the need to install a separate verification service, seeing neither the need nor the benefit. (If it is needed, it puts the trustworthiness of the evoting system itself into question.)

Considering a solution where votes are posted to a public bulletin board, how do you assess long-term privacy issues?

Average users might well be skeptical about the benefits and privacy of such a solution, even if it is technically sound.

2.1.8 Correct implementation and protection from unauthorized access

The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?

Many different kinds of flaws can arise, in the formal protocols and algorithms, the implementation, or the platforms. Standard techniques to address these threats include systematic testing and formal reviews. Others include parallel implementations and bounties offered to hackers. The fact remains that no complex software system is

completely free of defects or vulnerabilities; one can only reduce these to some "acceptable" level by a systematic application of these known techniques. The question remains, what processes were in place in the previous implementation effort?

Independent experts should focus not only on the specific development effort, but on the entire process and its quality management, as outlined in standards such as ISO 9000.

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

2.2.1 Further risks

Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?

The possibility of *software defects* either in the system itself or in the used platforms is not explicitly mentioned. On the user platform, this would be a variant of 3.1.17 (malware), leading to impossibility to vote, or sending a wrong vote. On the administrator platform, this might be seen as a variant of 3.1.1, leading to failure of the system to function, or loss of data.

The risk of a *trojan horse* or a backdoor being planted in the system or a used platform seems to be missing as well from the list of risks. (Cf. the Crypto AG affair.)

Another threat is related to *usability*. The VEleS mentions "user friendliness" as a criterion, but goes no further. Poor usability can be a serious threat. It is important to quantify the usability requirements in a well-motivated and verifiable way. This aspect has been largely ignored, it seems, at least in the available documents.

2.2.2 Security measures

Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?

The listed security measures all focus on the operation of the system. Aside from the requirement that the source code of the system be made available (Art. 7), nothing is mentioned about measures to ensure the *quality* of the security code (correct use of APIs, correct implementation of protocols, detection of common errors through software analysis). Software Quality Assurance needs to be explicitly addressed, with a focus on detecting potential security defects in the source code.

2.2.3 Critical security requirements

Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?

What I am missing is insight into the software development process. To what extent are formal reviews, exhaustive software testing, and software quality analysis tools used? Are specific tools used to detect common software flaws? What processes and techniques are used to detect and minimize software defects? These are important aspects not addressed in any of the documents.

2.2.4 Degree of data protection

Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).

The question is a bit odd since the fields are not comparable. The risks in banking differ from those in e-health and evoting. Furthermore, banking applications must deal with large legacy mainframe applications and databases, which is not the case in evoting. E-health must deal with a large number of heterogeneous data sources and medical applications. The contexts are not comparable. Nevertheless, in many ways, evoting is a much simpler context, so indeed one can assume that integrity and secrecy will be easier to ensure.

2.2.5 Threats to internet voting

Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels).

Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security?

Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?

I see two main goals for such an attack. The first might be to influence a vote, and the second would be to disrupt society or discredit the government. In the first case,

detection must be avoided. Given the difficulty, I can only imagine such an attack taking place where the outcome of the vote would have a severe economic impact for some outside players (countries or industries). It is probably much safer to try to influence votes through more legitimate (or at least legal) means, such as advertising and propaganda (eg fake news).

In the second case, detection is less of an issue, as the main goal is simply to disrupt and discredit. Such an attack on a small country like Switzerland seems unlikely, unless the broader goal is also to indirectly disrupt, say, the Swiss banking industry.

2.3 Selected risks

2.3.1 Checking return codes

Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly).

Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?

Voter awareness can be raised by highlighting the potential risks. However this may have the negative effect of lowering trust in the system. The key is to emphasize the benefits of the evoting system, keeping it as simple as possible, and lowering the perception of risk, while offering verifiability. If the return codes are provided electronically, immediately after voting, the chance is high that voters will check them. The chance seems much lower if, as proposed, the codes are sent by postal mail. (I admit I do not understand the rationale behind this approach.)

2.3.2 TLS fingerprint

The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server.

What measures could be taken in order to maximize the number of voters who check the fingerprint?

This seems unlikely in any case, as the average user will not understand what this means. Better is to give explicit instructions on how to reach the legitimate server, through a very short URL. At the same time phishing attacks need to be monitored.

2.3.3 Verification of client application

The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side.

Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?

This scenario seems to assume that the voter must download and install a (fat) client application. It is more reasonable to adopt an approach where the voter uses a (thin) client running in a web browser, as is common with e-banking and tax preparation applications. Two-factor authentication might be a reasonable way to signal voters that they are really connecting to the right application. (It's not the purpose of two-factor authentication, but it is a nice side effect.)

2.3.4 Quantum computing impact

How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant?

Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.

I believe that quantum computing is still a distant threat (or opportunity). Realistically, it will be at least ten years, probably twenty, before there are commercially viable applications. The threat to secrecy arises if the encrypted votes are physically accessible. Even if QC becomes reality earlier, the encrypted data can be kept secure by archiving it in a way that is not accessible through network means.

2.3.5 Protecting voter platforms

The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[3]?

[3] https://www.melani.admin.ch/melani/en/home/schuetzen.html

At best one can try to raise awareness about best (and worst) practices. Typical users are nevertheless challenged when trying to distinguish phishing attacks from legitimate emails.

2.3.6 Vote buying

Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?

Not really. Perhaps there will be new opportunities to tie vote-coercion to ransomware, but it seems far-fetched to me.

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- *Obtain a concept for effective and credible examinations*

3.1 Scope for examination

Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes.

Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?

The scope should not be restricted only to security issues. Experts with experience in implementing and running evoting systems are needed. Expertise in software quality assessment and software analysis, as well as expertise in software usability should be covered.

3.2 Prioritization of security requirements

In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.

As outlined above (question 1), the risk assessment should set priorities according to the severity and likelihood of individual threats. Every risk identified in the annex should be prioritized according to the importance attached to it, the perceived danger, the likelihood of an occurrence, and the cost to mitigate it. It appears that this exercise has not yet been done. (In any complex software project, requirements need to be continually re-prioritized.)

3.3 Credibility of examination output

Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

Hard to say. I think the most important credibility factor is not who does the appointing, but that the experts are perceived to be objective, and without conflicts of interest.

3.4 Scope and depth of examination

Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?

I do not understand the question.

3.5 Frequency of examinations

How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?

Hard to say, but I expect that every major version should require an examination. Possible criteria for triggering a new examination should be a partial outcome of a first examination.

3.6 Presentation of results

How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?

It's not clear what role the independent experts play. Will they be nominated by some party, or are they self-identifying? To me it seems uncontroversial how the results are published (web site + press conference).

3.7 Differing opinions

How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?

As in any project, there must be a stakeholder who plays the part of the "project owner". This stakeholder must ultimately take any business decisions on what actions to take (e.g., project termination or revision).

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7a and 7b have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use. A few weeks later, the PIT was running under a separate set of terms and conditions [5]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[4]

Goals

- *Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog*
- *Setting out the conditions related to source code publication*
- *Setting out the requirements related to public scrutiny*

[4] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

4.1 Source code access terms

How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the security community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?

The goal of a PIT should be clearly and only to identify security breaches for a bounty. Nevertheless, the code should be of an adequate quality to escape further criticisms. Documentation and test cases need to also be provided. The terms and conditions must make clear that the source code is only provided for the purpose of the PIT, and other uses are excluded. In any case, the risk that the source code could be used for other purposes are minimal.

4.2 Scope of documentation

What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?

The same documentation should be provided as would normally be available to developers and maintainers, i.e., API documentation, installation documentation, tests etc.

4.3 Publication workflow

When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?

Clearly all major and minor versions with patches should be published after all integration tests are complete, the software is ready for deployment, and the product owner signs off. If a mandated examination is planned, then publication must follow afterwards.

4.4 Extent of documentation

Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)

Yes, clearly whatever documentation and information that would normally be provided to developers and maintainers, including test cases and test data, should be made available.

4.5 Assessing public reaction

Under what conditions should public reactions be discussed?

1. *To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.)*
2. *Which entities should be involved in the discussion?*

It depends on the nature and extent of the feedback. In case only minor technical flaws are detected, these can be addressed in a revision of the software. If fundamental flaws are discovered, the project stakeholders may need to take strategic decisions.

4.6 Publishing security breaches

Should the system providers publish existing / fixed security breaches? Through which channels? When?

Normal practice is to publish information about such breaches once they have been patched. In the case of evoting software, if the software is not currently deployed or in use (i.e., no vote is taking place), then such information might be published before a patch is in place.

4.7 Public intrusion tests

Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?

Clearly security can benefit from PIT bounties; the question is rather how to manage the public perception, so that detected security flaws are seen in a positive rather than a negative light.

4.8 Low-scale internet voting to promote trust

Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust?

Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?

This is clearly a successful strategy that has worked well to gradually introduce both e-banking and electronic submission of tax statements. It is unclear what kind of additional federal regulations would help to "enforce" low-scale evoting use.

4.9 Tallying and verifying

How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?

Such processes should mirror as closely as possible existing manual processes to ensure credibility.

4.10 Publication of relative shares of eVotes

Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?

In principle this should increase trust. There is a risk that for certain votes, the electronic and physical results may differ significantly, since it is likely that the voter demographics will differ. Significantly different voting results may raise questions of credibility. (Imagine a vote on digital rights; it is likely that the demographic that makes use of evoting will have a different general opinion than the one that doesn't.)

4.11 Additional transparency measures

What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

None come to mind.

4.12 Statistical plausibility

Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?

See my comment above under 4.10.

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- *Identifying the conditions necessary for institutions from science to participate*
- *Identifying measures aiming at a stronger involvement of the public*

5.1 Participation of independent experts

Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation?

1. *Participation in «public scrutiny»*
2. *Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers*
3. *Supporting the public administration in the further course of the trial phase, e.g, at implementing the measures currently being defined in the course of the redesign*

The key danger I see is that such experts may be tied to vested interests. How to ensure that experts do not have conflicts of interest?

5.2 Conditions for participation

Which are the conditions to be met in order for representatives from science to participate in the political debate?

Established and relevant expertise, and truly objective independence (no conflicts of interest).

5.3 Presentation of facts to public

How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?

This is the job of a communications expert.

5.4 Level of detail for public consumption

Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?

Same answer as above. Information has to be layered, so those who need more detail can access it.

5.5 Measure to engage scientists and the public

Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust?

- *Public debates on selected issues*
- *Hackathons around selected challenges*
- *Others you might think of*

No comment.

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to create a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- *Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier*
- *Drafts for risk assessments and action plan*

6.1 Continuous risk assessment process

What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?

Very simply, one output of the risk assessment process should be to identify the conditions to trigger a fresh risk assessment. On a regular basis (for example biannually) a check should be performed to determine whether the risk analysis should be updated. Triggers could include occurrences of major security attacks on other public systems inside or outside the country, major releases of new versions of software platforms (e.g., operating systems) used by the evoting system, or major advances in relevant technology (e.g., quantum computing).

6.2 Publishing risk assessment

What are the benefits and downsides of publishing the (dynamic) risk assessment?

Obviously, benefits include public transparency and building of trust, while the downside is that attackers may be able to identify new threats not foreseen.

6.3 Supply chain risks

How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?

As we have seen with the Crypto AG scandal, these threats are very hard to mitigate.

6.4 Prioritizing measures

Which criteria for prioritizing action plan measures are relevant and in what order

As mentioned above (3.2), all risks need to be classified and prioritized. This information can then be used to prioritize suitable measures.

6.5 Standard methodologies

To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?

Well, agile software development methodologies include a lifecycle in which requirements are continuously reassessed and prioritized to deliver the features of most value early in the process. This is certainly needed. Systematic testing and reviews are also essential components of any serious software development methodology that values software quality.

6.6 Support for risk assessment

Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?

Not just specialized security firms but also usability experts, and software analysis experts can be of help. Such experts exist both in industry and academia.

6.7 Outsourcing risk analysis

Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?

See above.

6.8 Separate process analysis for Canton and system provider

Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this setup?

Possibly. No easy answer springs to mind.

6.9

Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[5] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?

Octave is designed to assess information security risks within a large organization. It identifies information assets and how they are managed. The scope is rather different from that of an evoting platform. Although some useful ideas might be reused from

[5] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Octave, in general it is not adapted to the evoting context. (Octave would be more useful to assess information security risks of the internal software and information systems used *within* a federal or cantonal administration.)

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- *Establishing a concept for crisis management*
- *Identifying the elements that are necessary for incident response*

7.1 Key elements of crisis management

What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?

The most important elements are (i) timely detection of an attack, (ii) if possible, termination of the attack, (iii) assessment of the damage, (iv) determination of any impact on the end result, (v) assessment of possibility to repair damage, (vi) communication of the results, (vii) steps to prevent repeat attacks.

7.2 Activation of crisis management

What are the right events and thresholds for an activation?

This will depend on the details of the implementation and the risk analysis.

7.3 Players in crisis management

Who should be involved in crisis management, with which role?

Similar answer. Different actors may also be involved in case of different kinds of crises.

7.4 Communication in case of crisis

How should the communication be organised (internally and externally)?

Clearly technical communication must be distinguished from public communication. There is no simple answer. It will depend on the scope and the nature of the crisis.

7.5 Established crisis management structures

Are there already structures that should be involved in crisis management (e.g. GovCERT[6])?

I am not aware of any.

7.6 Crisis management process

What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?

Again, this will depend on the nature of the incident. See also the answer to 7.1 above.

7.7 Requirements for digital forensics

What are the requirements and stakeholders for digital forensics and incident response?

Same answer. Many different incidents are possible, and need to be addressed in different ways.

7.8 Effective response measures

In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?

One must distinguish between known and unknown threats. In case of known threats, it should be possible to identify effective monitoring and mitigation measures. (Detecting intrusion, DDoS attacks, unusual traffic etc.) A careful analysis of risks, likelihood and priority will help to identify suitable measures. The difficulty is in the case of unknown threats missed in the risk analysis. Though the likelihood of a completely new and unknown type of incident is low, one must be prepared to react quickly. Experts in crisis management must be involved and available at any time, particularly during a voting period.

[6] https://www.govcert.admin.ch

7.9 Validity of outcome in case of an incident

How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?

See answer to 7.1 above. Clearly if the damage cannot be repaired, and it is not possible to assess whether the outcome of the vote has been impacted by the incident, then the vote may need to be declared invalid.

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name: Olivier Last name: Pereira

Background: I am professor of cryptography at UCLouvain (Belgium). I have been working and publishing on the technical aspects of voting systems for close to 15 years, including the design of verifiable voting systems and research on their provable security. I am a designer of the Helios end-to-end verifiable Internet voting system, which has been used for more than 10 years in numerous elections in universities, associations and private companies, including the International Association for Cryptologic Research (IACR). I am also a designer of the STAR-Vote end-to-end verifiable voting system, which was designed for US government elections, and a contributor to the BeVoting study that specified the electronic voting system currently in-use in Belgium. I did study the cryptographic protocols proposed by Swiss Post/Scytl for use in Internet elections in Switzerland.

The following answers result from a best effort within a limited amount of time. I flagged each of the answers with a perception of my level of expertise in the associated area: ($\star\star$) indicates an answer based on a direct expertise in my research domain (and may also reflect that I would consider some questions as open research questions), ($\star$) indicates an answer based on a general expertise in computer science, and non flagged answers are only opinions, possibly less informed than those of others given that I am not living in Switzerland.

1 Big picture

1.1 Question 1.1

You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examibations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

($\star\star$) In an imaginary country... I would definitely be intrigued by this imaginary country. Internet voting has been for a long time a central open technical challenge in the scientific community, with numerous proposals being set on the table and being all recognized as inadequate for deployment in government elections (most often by the authors themselves). As of today, there is a fairly broad

consensus among academic election technology experts that we still do not know how to do Internet voting for government elections in a secure way.[1] The availability of such a trustworthy system would definitely spark my scientific curiosity, and I would like to know if and how that country solved all these problems that my colleagues and I haven't been able to solve until now.

I would ask the following questions:

Integrity How does this system guarantee election integrity? How does the system offer evidence to the people that their vote intent has been properly captured on their electronic ballot? How does the system convince the people that all and only the ballots cast by legitimate voters are included in the tally? How does the system convince the people that this tally is computed properly?

If integrity relies on trusting some people or system components, I will wonder which minimal subsets of them, if failing, would become able to undermine the integrity of an election. If such subsets exist, I will wonder why it is believed that those people or components can be trusted. If none of them needs to be trusted individually, I will wonder what level of independence is guaranteed in order to limit the risks of joint failures.

I will care about the origin of the answers differently depending on the content of these answers. If the system is claimed to offer traditional end-to-end verifiability [BRR+15], that is, a form of verifiability that does not require to trust anyone, I would not care about the origin of the answer. (I may still be happy to see that a community of experts have been able to assert if the system is really end-to-end verifiable, that is, if the verification process is sound. This should only require assessing public documentation.)

If the system is claimed to offer weaker forms of verifiability, I will wonder what components or people need to be trusted for the verification to be sound. I will wonder how those components or people can be assessed to be trustworthy, and who is put in a position to evaluate this trustworthiness (delegates from candidates/parties? experts hired by the country? experts hired by the solution provider?). I would also expect to find official reports from all of these experts after each election, explaining why they believe that the result is correct, and I would be willing to assess if the evidence that they claim to have seen can be considered to be sound.

Confidentiality Confidentiaty will always be low for remote voting systems: there is no way to make sure that people vote in isolation or while not being recorded on a camera. Also, if there is no concern regarding coercion and vote selling, then the main motivations for confidentiality disappear.

I would still ask: how much confidentiality failures can scale in this system, compared to vote-by-mail or in-person voting?

Since elections need to be tallied, a group of people and components will always need to be trusted for the confidentiality of the votes. I will then ask: which subset of these people and components, if failing, would become able to undermine the confidentiality of the votes? What level of independence is guaranteed in order to limit the risks of such joint failures?

As confidentiality is something that can only be assessed by monitoring the election process continuously (contrary to integrity, which can be assessed at any time and by anyone if the system

[1] See, e.g., the 2015 E2E-VIV report by the U.S. Vote foundation, which reads, on p. 3 of its executive summary: "Internet voting systems currently exist, but independent auditing has shown that these systems do not have the level of security and transparency needed for mainstream elections." (`https://www.usvotefoundation.org/E2E-VIV/`), or the 2018 report by the US National Academies "Securing the Vote: Protecting American Democracy" that reads (p.122) "We do not, at present, have the technology to offer a secure method to support Internet voting." (`https://www.nap.edu/read/25120/`).

is designed properly), I would be looking for answers from the system designers (how do they intend to keep the votes secret?), but also for answers, after each election, under the form of reports by all the entities that play a role in keeping the votes secret. I would expect those entities to be chosen in a way that makes extremely unlikely to agree on jointly cheating.

Availability Internet voting makes it potentially much more difficult to assess whether the system is equally available to voters. We might for instance be concerned by any network operator who would randomly crash Internet connections, in order to discourage a fraction of the voters in well-chosen constituencies from submitting their vote.
I would then ask: what mechanisms are deployed to detect such issues, and who needs to be trusted in this detection process?

As for confidentiality, I would be interested in seeing which measures are taken in the system in order to guarantee availability (these can be described by anyone), but I would also be looking for reports, after each election, from the people who are in charge of assessing the availability, and wonder how effective, trustworthy and independent these people are.

Usability Security often comes at the expense of usability, and may increase the level of competence that the voters would need to vote. Typically, the requirements will be much broader: Internet voting systems typically rely on voters to report failures (wrong ballot, wrong confirmation codes, ...). Apart from from technical skills, this requires proper communication channels, and also self-confidence and communication/language skills from the voters.

Besides, Internet voting puts some parts of the system out of the hands of their providers: voters will use devices with very different screen sizes and resolutions, use different software stacks, including some that cannot be tested in advance (e.g., we may have browser updates deployed in the middle of an election). This non-uniformity my may influence the votes as well.

Usability will also be very important for the system operator. Contrary to voters, system operators may be picked for their expertise, and probably rely on more support, but their tasks may also be considerably more sophisticated: handle cryptographic keys, verify digital certificates and signatures, check huge vote registers, ability to properly report errors when they happen, ...

I will then ask: how much systematic experience has been gained in order to assess the usability of the system, in the elements described above? How it is documented? How is usability testing kept up-to-date given the quick and often unpredicatable evolution of software environments?

Again, apart from evaluation processes that can be defined by anyone and should be independently assessed, the execution of the evaluation process would need to be re-assessed for each election, by enough trustworthy and independent people.

The Swiss case I am now relating the questions above to the Swiss case, and to the Swiss Post experiment in particular, as it is understood to be the starting point of this discussion. I do not know how some of these questions would be answered, as I could not find related documentation.

Integrity The Swiss Fch Electronic Voting Ordinance 161.116 requires a form of individual and universal verifiability, which are key ingredients for integrity. Complete verifiability is distinct from (and apparently weaker than) end-to-end verifiability, in that it is compatible with the requirement to trust specific system components. These trust requirements may actually be quite strong, even for the >50% case: Art. 5 para. 6 of the Ordinance defines the notion of trustworthy part of the

system, and it appears that this definition could be satisfied even by a system that would define all of its components as "trustworthy parts" without any level of redundancy. Based on the discussion above, I would expect a system in which trustworthy components would be required to be made of several sub-components, operated by different independent entities using different software and hardware stacks, and such that a single honest sub-component would detect any failure of the others.

Ordinance 161.116 also requires the publication of the code of the system, but I do not see any requirement to publish a specification of the audit process, in particular for universal verifiability. It would appear to be important to have such a description explaining how proofs need to be verified and what they guarantee, under a form that would be similar to the specifications offered by standardization bodies for cryptographic protocols (IETF, FIPS, NIST...), so that a link can easily be made between a cryptographic protocol specification suitable for security proofs (including proofs of the soundness of the audit process), and implementations that could be made independently based on different software stacks.[2]

Confidentiality Votes are entered in clear in the voter device. This means that a voting devices can leak votes, which could happen by active corruption by external parties (malwares, ...), but also possibly through things as common as bugs in browser plug-ins.[3] This also practically puts a lot of trust in the voting server, which has the possibility to submit to the voters a corrupted voting app that would leak the votes (possibly through covert channels), and also trust in the network infrastructure, including DNS servers and certification authorities, which could be the cause of MITM attacks. These risks seem much higher than for in-person voting. A fair comparison with vote-by-mail seems more difficult to perform (depending of the security of the mailboxes and postal services, among other factors).

In terms of internal security measures, and based on the decision to ask voters to enter their vote in clear on their device, it seems complicated to avoid the need to trust the server distributing the voting client. On the other hand, distributing corrupted voting clients might leave evidences if, at some point, the voting client is saved by a voter and audited. Assuming that honest voting client software is distributed, one would still be interested in making sure that no server-side component would be able to violate the confidentiality of the vote, and whether this would leave any evidence. Here, despite the presence of multiple cryptographic keys, it is unclear from the requirements on the system that these keys need to be operated by independent parties at all time, in order to prevent a single corrupted hardware component to collect them all for instance.

Availability I did not find documentation explaining which measures would be taken to offer protection, or just detect, the kind of threats described above.

Usability I am not aware of specific usability issue with the Swiss system. The choice of entering the vote in clear in the browser and then asking voters to check their return codes seems to be a challenging one. On the one hand, it is clearly more comfortable for the voter to enter their vote

[2] Independent implementations have been made for systems like Helios, Scantegrity or Verificatum, including as programming projects in classes. Independent implementations, in various languages, have regularly been the source of the detection of missing or imprecise specification of verification steps.

[3] For instance, some writing improvement browser plugins record and transmit every content typed in a browser, which could at the same time reveal votes to the company editing the plugin, and possibly to external parties in case of extra security issue – see, as an example, (`https://www.cyberscoop.com/bug-in-grammarly-browser-extension-exposes-virtually-everything-a-user-ever-writes/`).

just by a few clicks that mimick the behavior of a paper ballot, than using an alternative in which, for instance, the voter would have to enter codes in order to express their choices. But, on the other hand, the cost in terms of security seems important since the browser now sees the votes in plaintext. This has a clear cost on the confidentiality side, as described above. There is a less clear cost in integrity: do we know how effective voters are at actually comparing the return codes provided by the system with those on their paper ballot, and reporting if there is an issue? Do we know that a malicious voting server would be unable to identify specific categories of voters who are very unlikely to check their codes and report errors?[4]

Based on my current knowledge of the system, I would say that the main points would be:

- Switzerland chose an intriguing direction regarding integrity with its notion of complete verifiability. This appears to be a weaker requirement than the usual end-to-end verifiability requirement that is standard in the academic literature, as it admits that certain components may need to be trusted. It is appealing because it makes the problem more manageable, at least from a conceptual point of view. However, it also creates a setting that is less studied.

- I find little evidence for the moment that the proposed system would achieve the expected individual/complete verifiability notions: security proofs have been shown to be lacking, attacks have been found after limited inspection, and I see little evidence that the components used for distributing trust are indeed operated and audited independently. I also do not know how effective voters are, in practice, at identifying and reporting issues related to their return codes (individual verifiability), and did not see any independent code that could be reviewed and used for auditing universal verifiability.

- Confidentiality seems difficult to assess as well: security proofs are also incomplete, the code assessment that would be needed has been limited for the moment, implementation issues have been identified, and I see little evidence that the components used for distributing trust are indeed operated and audited independently.

- Independently of this, it appears that there are various differences between the system that is analyzed from a cryptographic point of view and the system that is implemented, and that those differences are often not described. As such, it is really hard to assess the extent to which the reviews of the specification would offer sound conclusions regarding the deployed system.

- Switzerland took very interesting and promising steps, by requiring some forms of verifiability and distributed trust that are stronger than any other country I know, and much better aligned to address the general security concerns regarding Internet voting. Given the originality of this process, it is natural to expect it to be a long journey, and that iterations and further adjustments are needed. The current review process seems to be the right approach now.

[4] On a related task in which voters are asked to enter their vote on a ballot marking device, receive a printed version of their ballot, and to report if the printed ballot is correct, a recent study obtained mixed results [BMM+20].

2 Risks and security measures today and tomorrow

2.1 Verifiability

2.1.1 Crypto-Protocol

The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?

($\star\star$) There are two types of cryptographic protocols used in a modern Internet voting system: protocols that are specific to voting, and protocols that are in general use for the security of Internet applications. I discuss these two types of protocols below.

Voting specific protocols There is unfortunately no standard available for most of the cryptographic protocols proposed for use in the Swiss Post voting system. For instance, no mix-net has been standardized, there is also no standard for the various non-interactive zero-knowledge protocols that are used in the system, ...

As a result, the main source used for these protocols is academic papers. However, this brings at least three important limitations:

1. Academic papers focus on the novelty of the protocol that they propose, and often do not provide any precise description of many of the surrounding components (set-up assumptions, ...), if only because of page-limit constraints.

2. The cryptographic protocols available in the literature can hardly offer full solutions suitable for a system as complex and specific as the Swiss one. As a result, these protocols need to be adapted, often in apparently very minor ways. It is unfortunately well-known that tiny adaptations and optimizations can have dramatic effects on the security of such protocols.

3. Papers in the academic community often focus primarily on bringing a new algorithm or design approach, and there is very little level of review of the details of technical proofs.[5]

The first two limitations have been the source of all the issues found in the cryptographic protocols proposed in the disclosed versions of the Swiss Post/Scytl system.

General purpose protocols Internet voting systems also make use of very standard cryptographic protocols, like TLS for instance. Here, precise specifications are available, as well as various implementations, and these protocols are often subject to intense scrutiny.

[5] This has been identified as a controversial situation in the cryptographic community for at least 15 years [BR04]. One of the reasons is that the rate at which security proofs are produced exceeds, by far, the rate at which the community can hope to review these proofs. Besides, there are relatively low incentives to check the details of the security proofs of schemes that are only proposed as steps in an ongoing research effort: a thorough security assessment is expected to happen as part of a further standardization step.

However, since the stakes are much broader than an election in one country,[6] various security agencies and criminal organizations have strong incentives to find flaws in these protocols or in their implementations, and to keep these secret.

Besides, thanks to the intense ongoing public scrutiny, it is relatively common that vulnerabilities are found at any time. This may result in new vulnerabilities in the voting system that are essentially independent of the quality of the implementation of the voting system provider, which always needs to rely on external components. Such a difficulty has been demonstrated on an Internet voting system deployed in New South Wales (Australia) in 2015 by Scytl [HT15]: as an election was running, a TLS vulnerability was found by researchers, which was completely independent of the voting system (TLS is a standard Internet protocol used to secure most web communications), and it turned out that this vulnerability could be used to completely undermine the security of this Australian election.

How likely does it seem to you that such a flaw could be used for an undetected attack? This may depend on a lot of factors:

Impact Some vulnerabilities may only make it possible to de-anonymize a handful of votes, while some others may make it possible completely change the result of an election.

Convenience Some exploits may require internal access to a network infrastructure, while others may only require external access to the computer of a voter.

Visibility Some exploits may be easy to detect after the fact (which may not be an issue if, for instance, the goal is to publish a de-anonymized list of votes), while others may be stealth (which would be needed if the goal is to silently change an election result, for instance).

All these factors may influence the decision of pirates to exploit these vulnerabilities, and face criminal charges. In general, I find it difficult to run a system under the assumptions that people won't exploit its weaknesses: the news show on a daily basis that weaknesses are exploited, and often silently for long periods of time.

2.1.2 Security proofs

The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?

($\star\star$) Security proofs are a most useful tool to understand what a protocol would achieve (they require security definitions), under which assumptions (they require to make these assumptions explicit), and why the protocol would be secure (by inspecting the proof strategy).

Security proofs are known to be very tricky to write, and even trickier to verify.[7]

[6] Together with undermining elections, these could be used to undermine the banking industry, government and trade secrets all over the worlds, . . .)

[7] A recent and prominent example of this can be found in the proceedings of the CRYPTO 2019 conference, in which attacks are demonstrated against the OCB2 mode of encryption, which is an ISO standard since 2009 [IIMP19]. The authors of the attacks report: "That OCB2 might be flawed was first identified by the authors [...] when they re-examined the proofs of OCB2 for educational purposes and searched for potential improvements. Instead they came to find a seemingly tiny crack in the proof that they first tried to fix as they strongly believed OCB2 was a secure design, but after several tries they ended up with existential and (near-)universal forgeries."

I would then consider it very likely that flaws would be present in the security proofs of protocols as exotic and complex as those found in a full Internet voting system, unless a tremendous amount of scrutiny, possibly in conjunction with formal verification, has been obtained.

These mixed comments should not in any way dismiss the importance of security proofs. I believe that they are the best and most tested way towards the specification of secure cryptographic protocols. But this is a long and arduous way.

The moment at which proofs are produced may be of importance as well: it is considerably easier to design a protocol together with its proof, than to design a protocol and analyze it later.[8] The first strategy is therefore much more likely to lead to proofs that are more accurate, and easier to verify.

2.1.3 Printing office

For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment.
With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office).
How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?

($\star\star$) It seems, indeed, very hard to avoid the need to trust the printing office to print the return codes correctly and to keep them confidential.[9]

However, I do not see how to justify extending that trust beyond what can be argued to be necessary – and such arguments would need to be provided. It adds new vectors of attacks, may make it more complicated to run an investigation if an attack happens (because there would be more possible origins to the attack), and is harder to justify to the public.

For instance, I would not understand why a printing office would need to be trusted for generating public parameters (e.g., group generators) for a verifiable mix-net, since this task could be performed publicly in a verifiable way. Assigning this task to be performed in a non-verifiable way by a trusted printing office raises various issues: it requires to track more code and processes as part of the secure printing office, it requires investigating both the printing office and the mix-net operators if there is any issue detected with the results of the mix-net, and it may bring more suspicion on the printing office operators since the public may question why they are asked to trust these operators despite the fact that the parameters in question could easily be generated in a publicly verifiable way.

[8] It is known since the 1980's that the problem of proving the security of a given protocol is in general undecidable, while the problem of building a provably secure protocol for any task can be done efficiently (that is, in polynomial time).

[9] Various solutions that do not require this have been proposed in the literature, but they all seem to carry important usability or operational challenges. This might change in the future!

2.1.4 Independence (control components)

The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?

($\star\star$) I believe that using several providers has tremendous added values. The obvious first is that it reduces the risks of having a vulnerability shared by all components.

Independently of this, the various providers should produce their software from the system specification, and without having access to the software from the original provider. This would be a very good tool to detect gaps and inconsistencies in the specification (such as those that have been found in the reviews that were made last summer), because it forces independent groups of people to have a full examination of the protocol specification, and possible ambiguities in the specification would show up: in order to build code, the specification must be interpreted, and differences of interpretation will become quite visible when the software will be tested with actual data. This, in turn, can be most valuable to improve the overall security of the system.

2.1.5 Independence (auditor's technical aid)

Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?

($\star\star$) The arguments mentioned above also apply here.

In particular, I see a very strong added value in having the verification software being built from a protocol specification rather than by people who are familiar with the code that produces the proofs and other data that need to be verified: this will avoid reproducing the same mistakes.

2.1.6 Independence (OS and hardware)

The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?

($\star\star$) Running the control components on various software and hardware stacks can protect from 0-day attacks on standard libraries incorporated in operating systems, or Trojans/bugs embedded in the hardware (servers, networking equipment, HSM's, . . .), provided that the voting protocol is designed to be secure as long as a single component remains honest.

The separation of duties, apart from making corruption harder, offers strong opportunities to detect human mistakes and forces improving the quality of the system documentation.

2.1.7 Other forms of verifiability

The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?

($\star\star$) I agree that such mechanisms, if introduced, should come in addition to the existing ones that can be expected to offer stronger usability. I would see such extra solutions as being an interesting way to offer a solution to tech-savvy people who would like to challenge the trust that they are required to put in the printing office (for instance).

I would not advise posting encrypted votes on a public bulletin board, due to the long-term privacy issues and the risks that a computational assumption gets broken. Other approaches exist in which perfectly hiding commitments could be posted instead. Here, instead of relying on the hardness of computational problems, the trust assumption would be placed on the quality of the PRG used to compute the commitments. Multiple sources of randomness could be combined for that purpose.

2.1.8 Correct implementation and protection from unauthorized access

The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?

($\star\star$) Requiring independent implementations of the various components is likely to help in having software that complies with its specification: any extra or missing field of information, change or tweak of algorithm, ... would be very likely to create incompatibilities between the components. This would however not help spotting some types of flaws (e.g., related to confidentiality, like the use of poor randomness, or applying random permutations, ...).

Secure boot technologies and attestation could also possibly help an operator who would like to verify that a machine is running the expected software. This is still a very active area of research and development [Fra20], which could possibly be simplified and improved with the development of the RISC-V architecture. But this would in turn bring strong constraints on hardware choices. Offering attestation to a third party auditor that the right software and hardware was used to produce a physical result, e.g., to print a pile of paper ballots, appears to be an even more complicated issue.

Regarding the role of independent experts: the questions raised here are long-standing research questions. As such, I would think that their primary role should be to keep inventing better solutions to

these issues.

2.2 Security related risks top-down

2.2.1 Chapter 3.1 of the VEleS annex

Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?

($\star\star$) It looks like this list covers the basic threats, indeed.

I wonder why the threat related to ballot paper (3.1.4) is only discussed from the point of view of MITM and regarding accuracy.

- Would it not be the case that altering the ballot paper could be made by a (malicious) administrator?
- Could this also have an impact on vote secrecy (e.g., an attacker could add instructions to connect to a malicious website, which would have the same effect as DNS spoofing – 3.1.11).

Regarding the security objectives, I suspect that "availability of functionalities" should also be considered as a potential problem with the "accuracy of the results" (I do not know if it is the case already): if an attacker manages to make the system (or voting client, or network connection, ...) unavailable (maybe in a random way so that it is hard to detect and reproduce) to some chosen categories of voters, this can be expected to influence the result as well (in the sense that it will make some categories of voters less likely to submit a ballot).

2.2.2 Missing security measures

Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?

($\star\star$) I do not know, and it would probably take weeks to determine this. It would be useful to have a documentation explaining how these sets of requirements have been derived.

I am also not sure that I understand what all these measures cover: I do not see what could be missing when, for instance, 3.4.2. states that "the system must be protected against attack (irrespective of the nature of the attack or of its origin)".

Just some random aspects, by sections:

3.3 This section seems to be the only one explicitly focusing on the confidentiality of the votes. In particular, 3.3.4 explains when votes should be encrypted. Encryption may however not be sufficient, as shown by Locher et al. [LHK19]: the order in which ciphertexts are stored, and other external data, may also be a source of confidentiality failure. It might be sound to add an extra requirement, or to broaden 3.3.4, in order to express that any information related to cleartext votes should be infeasible to derive from the information that is transmitted or stored, before the tally.

3.3.6 Standards often make several recommendations for key lengths, depending on which security level is aimed for and duration. Requirement 3.3.6 does not state what duration or security level should be taken into account: this should be added.

4 The verifiability sections talk about proofs that should be substantive (4.2.4, 4.4.7). I wonder if it is explicit enough that proofs come with a proof verification process. It may be the case, and it

has been the case, that some maliciously crafted proofs would pass the prescribed verification process, even though it might be possible to detect that something went wrong by performing other types of verification (possibly completely non-trivial). Would such a possibility be enough to say that a proof is substantive, in the sense of the Annex? I believe that it should be clear that the prescribed proof verification process should be sufficient to detect any malfeasance.

4 The analyzes performed in 2019 showed a number of discrepancies between the system specification and the code. This is obviously a source of security issues. As indicated above, I suspect that at least some of the discrepancies would have been detected if the auditing code had been written by independent parties directly from the specification, and without access with the code used to produce proofs. This could be an extra security measure.

2.2.3 Unmet requirements

Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?

($\star\star$) The requirements that are listed here are mostly operational, and I do not know whether they have been met.

Regarding cryptographic aspects:

4.2.4 I believe that this requirement was not satisfied: it was shown [LPT19a] how a malicious voting client would be able to cast an invalid vote despite the voter having received all the proofs (valid codes) from the system.

4.4.2 I believe that this requirement was not satisfied: it was shown [LPT19b, LPT19c] that a single untrustworthy CCM would be able to provide a proof of correct mixing and partial decryption that would not be substantive.

4.4.14 I am curious as of why the CCM4 gathers, in a single device, multiple decryption keys. Formally speaking, it is defined as one out of 4 components. But, if one is willing to rely on the additional security of having multiple keys (the EB_{sk_i}), and on the associated burden in key generation, then this process does not follow the (sound) idea of keeping minimal the impact of unauthorized access: it would be safer to have one decryption component per key.

2.2.4 Integrity

Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).

($\star\star$) I do not think that it would offer better protections compared to other security critical data.

In terms of verifiability, my bank offers me detailed account statements, which I can use to verify, without the need of any technical knowledge, or special data access, that all my transactions have been properly recorded, and gives me evidence of the amount of money that the bank has on my account. If money disappears, I will be able to see it and complain – and this is the case even if the whole banking industry were malicious. In the context of voting, I cannot receive such statements, due to the secrecy of the vote. Complete verifiability, as expressed in the VEleS, only partially compensates for that: I only receive evidence under the assumption that trusted components are trustworthy. And there is essentially no way for me to detect if they are not.

Besides, even if the level of verifiability required in the VEleS matched the one I have in my bank, there still are important differences that make voting more complicated: the scope of verifiability is broader, and the secrecy of the votes makes verification more complicated, and out of any current standard. For instance:

- What I need to verify for banking is much simpler than what I would like to verify for voting. In banking I only need to care about my own bank account: the number of other accounts, and the number of transactions on these accounts have no impact on me, and I do not have any legitimate ground to be willing to verify anything about it. In voting however, I also need to care about what the others are doing: I want my vote to be included in the tally, but I also want to make sure that the other votes included in the tally come from legitimate voters, and that nobody can push more than one vote. So, the scope for verification in voting is much larger than for banking.
- Evidences are much harder to collect in voting than in banking. In banking, transactions are only secret to external parties, but not to the bank, which makes it possible to do numerous internal checks and balance controls on cleartext data. In the context of voting, the vote is secret even for the system operators, which makes it considerably more difficult to track information, and requires sophisticated cryptographic protocols that are not part of any standard as of today (there is no need of a verifiable cryptographic mix-net in a bank, for instance).

So, even if the technical solutions could be considered to be much more advanced than in other applications (and I do not know how these applications are handled in Switzerland), the requirements on voting are much more challenging too.

2.2.5 Internet vs. postal voting

Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?

($\star\star$) I would see two types of powerful actors: external parties (foreign governments, mafias, ...) and internal parties (voting system operators, ...). I would also make a difference between local and federal elections.

External parties would probably find it more attractive to attack an Internet voting system: this can be done from foreign countries where prosecution in case of detection would be quite unlikely, and anonymous communication technologies can also be used. Actively corrupting mailboxes or local election officers would typically require being on-site, and therefore more easily subject to prosecution.

An Internet voting system also offers a single infrastructure to target in order to potentially undermine dozens of elections. This would be considerably more complicated for in-person voting.

Regarding internal attackers, this could go differently depending on the context:

- In local elections, the parties with the highest interest in cheating would probably be local (e.g., the party in power), and having a system operated externally (by mail or by Internet) could potentially make cheating more complicated (depending on the security safe-guards in place for in-person voting).
- In federal elections, cheating with an in-person voting system would probably require to cheat in many municipalities. This can in turn be considered to be more complicated than corrupting the single entity operating the central infrastructure for Internet voting or vote-by-mail.

In all cases, I believe that attackers would have strong incentives to use attack strategies that leave no or little evidence: being unnoticed offers the possibility to cheat multiple times. Besides, given the cost of an election and the political impact of canceling one, it will always be tempting, as long as there is no overwhelming evidence, to minimize the impact of any incident.

This is also why verifiability is so important: it offers a way to detect malfeasance (external or internal), and to collect evidence about it.

2.3 Selected risks

2.3.1 Code verification

Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?

($\star\star$) I believe that most voters would be *able* to check their codes. Based on past studies, I would see the following difficulties:

- Voters will check their first few codes, or their codes in their first few elections, then stop and just trust the system. Cheating happening after a few years would then become much more unlikely to be detected.
- Voters who receive invalid codes may be concerned that they did something wrong, or did not understand something, and not dare to inform the administration (being afraid of looking stupid, for instance). Or they could just be unwilling to spend time to notify the administration (assuming a busy hot-line, . . .).

One possible option for making sure that voters check their code would be to have 5 digit codes on the paper ballot, have the voting server return only 4 digits, and ask the voter to type the fifth digit, which would be sent back to the voting server for verification. This extra measure would offer little protection against a cheating server, but could possibly be helpful against a cheating voting client, and it would guarantee that the voters take a look at each single return-code. It would also increase the effort required from the voters to vote, and may discourage some.

In a honest server setting, returning wrong digits would also be an indication that there is something wrong, even if the voter does not report anything by himself/herself. If this happens a lot, voters could be contacted in order to understand what happened.

2.3.2 TLS-Fingerprint

The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?

($\star$) Do you mean the SHA-256 hash of the certificate?

I would think that it is quite hard to do, and browser dependent. Even with proper instructions, it may still be possible that a major browser developer changes its interfaces a week before the election and makes the instructions obsolete.

It also seems to be a risk if, for any reason, there is a need to renew a certificate just before an election (e.g., due to a vulnerability found in TLS just the day before an election, that would require generating new keys).

If it is really decided that voters should check a fingerprint, then one way to push them to do it would be to ask them to type the last two digits of the fingerprint as part of the instructions on the paper ballot. Of course, a malicious website would accept any last two digits, but finding them would force the voter to take a look and give him a chance to detect if there is something wrong.

2.3.3 Client integrity

The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?

($\star\star$) I do not have in mind any good solution to this important problem.

In the context of the Helios Internet voting system, which faces the same difficulty, we suggested that various voting clients should be offered. If I want to vote for party A, I could pick a voting client endorsed by party A, and hope that this client will at least vote for A. Of course, this raises new confidentiality issues (party A might be willing to learn who uses their voting client), and authenticity issues (I now need to trust that I am really using the client endorsed by party A). We had numerous independent implementations of voting clients (including as class projects), but we did not see any of them being used more than marginally in elections.

2.3.4 Quantum computing

How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.

($\star\star$) I do not think that quantum computers are a unique threat to election integrity for the moment: they would need to be already there, and I do not see any reason to believe that someone holding a big quantum computer today is more likely to exist than someone being able to break the computational assumptions on which the protocol depends in a different way. The people who could exploit such a computer would be external parties distributing a malicious voting client, and forging the ZK proofs of ballot correctness, or the voting system operator, which could then cheat during the ballot tracking and tallying process.

Quantum computers could be a threat for confidentiality: someone monitoring Internet traffic, or having internal access to the encrypted votes, would become able to decrypt them and break the secrecy of the vote, assuming that there is a way to make a link between the ciphertexts and the voters (which would require extra logistics and would not always lead to a successful re-identification).

Besides, the requirements of the current system are already very challenging to meet while using "traditional" cryptographic techniques (based on the discrete log in finite groups), and moving to post-quantum cryptography would add an important extra challenge and probably lower our understanding of the solution even more.

2.3.5 Trustworthiness of voter platform

The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI?

($\star$) These guidelines really good to distribute and share.

I would be surprised if a significant influence could be gained if voters only receive this kind of instructions as part of a voting process: most of the good practices need to be part of an every day concern (unless the voter can use a brand new computer at every election).

I would therefore think that this should be part of general public information campaigns on cybersecurity rather than something election-related.

2.3.6 Vote buying

Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?

($\star$) I suspect that the primary influence on vote-buying and coercion will come from the social context in Switzerland rather than from technical aspects.

From a technical point of view, it also this depends on the specifics of the protocol that is used. In the current system, it seems that vote-buying could scale quite easily, which may make it more effective

than before. For instance, a vote-buyer (or a coercer) could offer a browser plug-in to voters, which would record all the vote choices and the signed receipt transmitted by the voting server. All of this can work remotely, without any contact between the voter and the buyer/coercer.

This looks more challenging than asking voters to make a movie of themselves voting and collecting that movie, or collecting the ballots in vote-by-mail.

3 Independent examinations

3.1 Criteria

Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?

($\star\star$) This is a complicated question, and there is very little experience on this in the context of verifiable Internet voting systems. In general, one should maximize the incentives of the people running the examination to find and report issues, and make sure that these issues will be appreciated to their full extent (or dismissed if deemed unreasonable).

A specific challenge is that the system makes use of various cryptographic technologies that are highly non-standard. This means that developers have little wisdom on which they can rely, and that there is a very small number of people who have the expertise to spot issues. And that these issues will often be of the level of original research findings than of the level of spotting a gap with respect to a good standard practice. (As such, it is quite common in the academic literature that errors in security proofs remain unnoticed for decades, or that security definitions remain misinterpreted and do not offer as much practical security as expected.)

I also see very different areas in the verification, with very few people being able to perform verification within more than a single area. People able to check security definitions and proofs for cryptographic protocols often do not know anything about software and system architecture. Experts in high-quality software development often know very little about cryptography and system architecture. And the same typically applies to system experts. This means that there is a significant challenge in ensuring the consistency of the base documents used by the various verification teams.

Eventually, verification should be considered as an ongoing process aiming at continuous improvement, rather than a process at the end of which a certification stamp is obtained: this is way too close to research, and the target keeps moving with the evolution of the Internet landscape.

3.2 Delaying fixes

In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.

($\star\star$) I would be very cautious with the idea of delaying the resolution of known weaknesses. It is often very difficult to appreciate the full impact of a weakness: in systems with that level of complexity, any

weakness may violate an assumption made (possibly implicitly) in a completely different component of the system, and result in damages that could be very different of those initially envisioned.

Besides, it seems to be a public relation nightmare to justify, if something goes wrong, that a known deficiency was exploited.

3.3 Origin of the examination

Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

($\star\star$) I see a different perception between an examination ordered by an external judge asking whether a design is faulty, and an examination ordered by a designer willing to obtain evidence that his design is good. The judge would be perceived as looking for the truth, while the designer would be perceived as looking for validation. As a result:

- The judge is likely to offer a more neutral view on the design, and not do anything that would hide defects.
- Examiners would feel more comfortable to report defects openly to a judge than to the designer who spent years on his design.

3.4 Scope and depth of examinations

Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?

($\star\star$) The current requirements are mostly expressed in a “stamping” spirit: all the parts of the system need certification stamps, at regular intervals.

This is definitely important, but it should also be accompanied with a permanent review process, with associated incentives. For instance, an ongoing bug bounty program could be organized on the cryptographic protocol specification and proofs, on the system description documents, on the code, and a copy of the system could be run in parallel of the real one and offered for public intrusion tests. Rewards in this bounty program could be monetary, but also in terms of recognition: students can often come with very unusual and effective ideas, and being listed as having spotted an issue in a national voting system can be a welcome line in a CV.

Many companies have a very documented bug bounty program, in terms of rules and effectiveness.

3.5 Refreshing the examination

How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?

($\star\star$) Any “important” change should prompt a new mandated examination. Any important finding, as part of a bug bounty program, should also prompt a new expert examination in order to make sure that the full scope of the issue has been properly understood. It seems important here to have a rolling pool of experts, or different sets of them: some should be there for quite some time, in order to have people who are most aware of the intricacies of the system, but fresh eyes are also very important.

3.6 Independent examination

How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?

($\star\star$) I think there is very little experience on this, and Switzerland is likely to be the country with the most experience.

I would suggest to involve the public as soon as the certification bodies and mandated experts have completed the first round of their job. The expectation would be that the low-hanging fruits would have been removed already, limiting the risks of public relation challenges if too many issues are found at the same time.

If the system is not in use, I do not see any reason to delay the publication of analysis results that have been validated (which should be done quickly, especially if one is willing to benefit from students and researchers who are interested in completing their classes or publishing a paper).

If the system is in use, then the publication should be made as early as possible while not offering new ways of exploiting a vulnerability (it could be immediately if the vulnerability can only be exploited from the inside, and insiders already know about it, it could be just after the election, or just after a fix is put in place, whichever comes first). A maximum delay should also be determined: the possibility of unlimited extensions can be badly received.[10]

3.7 Handling differing opinions

How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?

I am not sure. Maybe look at how health departments in various countries are making policy decisions regarding COVID-19?

4 Transparency and building trust

4.1 Terms

How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the security community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?

($\star\star$) The goal seems to be to offer more incentives to the people who are willing to help improving the system security, than to the people who are willing to undermine elections.

The goal would be to attract external volunteer experts and make them as effective as possible, which could include:

- Explaining why this is good and important for democracy, in Switzerland, and also elsewhere;
- Low barriers to the access to the code;
- High-quality documentation of the code, but also on how to compile it, run it, and use it with a debugger;
- Various types of rewards, aligned with the various incentives of the experts/researchers.

[10] `https://www.hackerone.com/` offers various discussions on these topics.

In particular, I think that people might be interested in helping for very different reasons, and it would be good to cover as many of them as possible. For instance, I can think of public recognition (publicly acknowledge people's contribution, which can be helpful for students to get a job for instance), rewarding interactions at the technical and at the personal level (people like to feel that their contribution is valued) and also money.

Asking people to register in order to be able to help reviewing the system (code review or intrusion test) is an unusual demand, from what I see in typical bug bounty programs, especially for a code that is required to be public. It also opens concerns that this registration would be used to convey an incorrect message: many people will access the code or the system just to have a quick look, and may be frustrated if they see that this is used to claim that the system is secure just because many people registered (even though they did not review anything). It may also put wrong incentives for publishing code of low quality or poorly documented, in order to discourage reviewers immediately after their registration.

It is also quite important that reviewers have the freedom to discuss their findings openly and in a timely manner (especially in the academic sector, where there is a need to get a job/make a publication). Of course, it is reasonable to ask that the system operators should be informed first, so that a proper analysis can be made, and that problems could be fixed if needed. If the system is not running, this could be just a few days in order to acknowledge the problem – there is no need to fix the problem before talking about it. For systems in which vulnerabilities could be exploited, a 30-90 days range (with no extension) is common.

The context of voting seems a bit specific in this respect, since the primary goal of the system is to offer valid elections to a country, and not to increase the profits of the company operating the system. As such, I do not see any reason to keep confidential an issue related to universal verifiability (for instance), including if the system is running: universal verifiability is also there to protect from the system operator, and it therefore makes little sense to let the system operator delay the publication of a vulnerability which it could exploit: it is the public that needs to be protected first, here. The story could be different if we are talking, for instance, about a client-side vulnerability that could be exploited by external parties to modify votes in an undetected way.

As for the IP concerns, I believe that it should be addressed as part of the eligibility of the system (as it is now): the owner should agree to make it available for broad public review, and an owner disagreeing with this should simply not offer his system for public elections.

4.2 Scope of documentation

What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?

($\star\star$) I believe it should be very broad, and possibly redundant: some experts will target cryptographic protocols, others will target bugs in the code, others will think about the operational measures, . . . These will very likely be different experts, using different documentation formats.

Of course, there are components that will remain out of scrutiny: for instance, people won't be able to check if operational measures have been properly implemented during a specific election, or they are unlikely to be able to test some offline trusted hardware component for vulnerabilities (because of lack of access). These issues will need to be addressed differently.

4.3 Timeline

When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?

($\star\star$) I would suggest to involve the public as soon as the certification bodies and mandated experts have completed the first round of their job. The expectation would be that the low-hanging fruits would have been removed already, limiting the risks of public relation challenges if too many issues are found at the same time.

The code and documentation should then remain available permanently: it will offer very little extra information to malicious parties (who will make sure to access it as soon as it is there), and offers more possibilities to attract helping parties who can become available at any time.

4.4 Extra content

Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)

($\star\star$) This a large and complex system, and it would make sense to support the community as much as possible if one is willing to receive help in return. In this spirit, and given the past experience, I would suggest to also offer detailed instructions on how to compile the code, run and test the system, and use it with some standard debugging tools. Various projects also make it possible to download a virtual machine (or set of virtual machines) on which the full system would be running, so that there is no need to set-up a complete testing environment with all its dependencies.

4.5 Who to report to?

Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?

If this is a system recommended by the Confederation and offered by the Cantons to their citizens, I believe that the Confederation and the Cantons using the system should be informed of any public reaction (assuming that they are in the right position to be judges here–I do not know their public mandates well enough). They should be hearing the public concerns, and the system provider's responses, and make decisions based on these. I do not see any reason why the system provider should have a possibility to interfere with this process, or to delay it. (But, of course, the system provider should have chance to respond to the concerns that are raised by the public.)

It is also quite common that an external reviewer identifies a vulnerability, but does not understand the full implications of it. As such, it seems quite important that any identified vulnerability should also be reviewed by external mandated experts, that would be in a position to evaluate whether a vulnerability has been properly addressed – the reviewer alone is not in a good position to do so, and the provider has incentives to minimize things.

Eventually, I also believe that many people will be more interested in helping the Confederation and the Cantons to have secure elections, than in helping a company improve their product.

4.6 Publication of security breaches

Should the system providers publish existing / fixed security breaches? Through which channels? When?

($\star\star$) Vulnerabilities should not be made public as long as the primary way of exploiting them would be by external third parties. But the Confederation and the Cantons should be made aware of their existence and potential impact.

On the other hand, since the system is expected to have its source code and documentation published, explanations should be provided for any change: this is necessary in order to have an effective public review process – reviewers should not have to guess the reasons of a change in the code or in the documentation of an audit process. As a result, it would seem to be more effective to just be straightforward about it, and clearly explain the vulnerability and the way it is fixed.

4.7 PIT organization

Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?

($\star\star$) I believe that the PIT offers one channel, among many others, to improve security. It would probably have been more effective by not requiring registration (many companies let people search for vulnerabilities in their system without asking for registration).

The PIT can be expected to improve public trust: claiming that a system is secure and then making it illegal to try to disprove that claim does not seem to be a good strategy to obtain trust.

Restrictions regarding social engineering and DDOS seem reasonable, especially if the PIT is a permanently running process (which it probably should be, possibly apart from during elections): social engineering, if allowed, can just become unbearable for the system provider and lead to forms of harassment. DDOS are very expensive to prevent (in a secure way), and are easy to notice at election time.

Still, I believe that social engineering and DDOS are important concerns – I rather believe that a PIT is not the best way of challenging these concerns. Mandated random tests could be useful to address social engineering issues, and emergency plans are needed when facing a DDOS (on top of technical measures).

Besides, code, system documentation, and security proof inspection should also be part of a bug bounty program. See answer to 4.1 regarding incentives.

4.8 Low-scale use of Internet voting

Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally pro- mote trust?

($\star\star$) The low-scale use appears to be a sound choice for a system that is far from being fully tested and understood, and operates within a model that puts a lot of trust in the system operator.

But I am not sure that it will be perceived as a way to promote trust: it is rather an appropriate way to act given the limited trust that can be put in the system in the first place.

A security oriented agenda may raise concerns from non-experts (who may be concerned that security is not given for granted). But it may also eventually lead to approval and support by experts from the general public, or at least make it possible to address their concerns. I believe that, in the long term, it is more effective to address these concerns, and have an informed public debate: the common reaction to avoiding the security discussion is that activists/hackers/experts/. . . will raise an emergency security alert in the context of a real election (maybe because they did not have a chance to look at the system before), which seems to be far more damaging. The other risk of avoiding the security debate is of course that security vulnerabilities will actually be exploited in order to rig an election.

4.9 Tallying and verification

How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?

($\star\star$) There is very little experience with this.

I think that every candidate/party should have a right to take part to the verification task. They should be able to mandate their own expert (as they would typically have the right to mandate observers in paper elections), which should have a right to run its own audit software, written based on the specifications of the system provider.

I can imagine that open-source audit software would be written by concerned citizens, but could also be included in student projects in high schools and universities, and that parties and candidate would then have the possibility to pick the software that they trust the most–or to mandate someone to make their own.

4.10 Publication of partial results

Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?

($\star\star$) I imagine that the assumption here would be that, if the electronic results “look like” the results of the votes collected by other means (paper, mail), then those electronic results would be trustworthy.

If this is the assumption, I would not be convinced: I may imagine that it is a specific part of the population that is mostly interested in electronic voting, and I do not see why that part of the population would vote in the same way as the rest of the voters (this may or may not be the case, but I do not see why we should trust that it is the case). Besides, if the criterion is: “if the results are consistent across voting methods, then we will trust them”, then an attacker who knows that his party receives a lower support from the electronic voters might be even more tempted to try to cheat in a way that would balance this difference, and have better chances of not being caught.

As another downside, I can imagine that the publication of partial results may raise privacy concerns in some cases.

Still, I believe that an internal comparison (by the Cantons or the Confederation) of the results across different voting methods is an important security safeguard, and a good way to obtain hints at possible

security failures (e.g., a candidate receiving a very low share of the votes because his name was not properly displayed on some devices).

4.11 Additional measures

What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

($\star$) I suspect that having a real public bulletin board, including all the information needed for end-to-end verifiability, could increase trust in the outcome by the public. As discussed before, this has to be put in balance with the associated risks for privacy.

Publication of the content and results of system inspections by independent experts at election time would probably help as well.

4.12 Statistical plausibility checks

Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?

($\star\star$) As discussed above (4.10), these could be good for detecting honest mistakes, but would not be effective for the detection of attacks.

5 Collaboration with science and involvement of the public

5.1 Conditions of participation

Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g, at implementing the measures currently being defined in the course of the redesign

($\star$) A crucial condition for the participation of scientific experts seems that they should be able to make academic publications from their results: this is what they need to be funded and maintain their expertise.

As a result, I see different options and limitations:

- Academic experts could take part to the public scrutiny. This may or may not happen, and may be quite out of the control of the organizers (it would depend on the many other projects running at the same time). Top quality documentation and easy access can certainly help, here.
- Academic experts can be mandated to specify or review a system. This seems to be workable for short-term missions, and possible for medium-term missions when the content of the mandate has a scientific interest (technical novelty, . . .), as it makes it possible to also attract the interest of

younger researchers without delaying them too much in their other tasks (since they are gaining scientific expertise at the same time).

- I suspect that it will be much more complicated to involve academic experts in implementing measures (even though this may depend on the academic institutions and rules). This is typically a much more long-term effort (so, it would typically have to be pushed on younger students who just graduated), and it is usually not part of the university culture to prepare code of production quality: universities typically focus on research prototypes. An exception to this could be in auditing code, which could be a self-contained effort.

In any case, it is likely that it will be much easier to benefit from academic expertise when there is a new system, or a new process, or anything that can be connected to research, than in the routine inspection of small (but possibly critical) changes in a system that has been running for several years.

A possible solution to this would be to seek for the creation of European research networks of e-voting experts, which could focus on the novelties and questions that come in all participating European countries. This could create a critical mass of experts who could rely on longer-term funding rather than on the short-term availability of some persons who do this as a side-job, and would maintain a strong expertise across various countries at a controlled cost.

5.2 Participation to political debate

Which are the conditions to be met in order for representatives from science to participate in the political debate?

($\star$) In the case of technology experts, I would say that it is very challenging: the political debate uses very different codes and languages compared to the technical community, and participation to the political debate seldom gives positive side-effects on the "traditional" research activities. So, direct participation will often hinge on the (not very common) capacity of some strong researchers to effectively learn how to have a political discourse and on their decision to spend the time that it requires to convey this discourse in a debate.

Quite often, it is most helpful and effective to have experts from public administrations who have the ability and the mandate to make a bridge between the scientific experts and the public debate. This offers the possibility to specialize the task of the scientific experts on the topic of their expertise: it makes it possible for them to focus on framing the debate from a factual point of view, on expressing what technology can achieve and its limitations, on opening doors, while not necessarily being direct proponents of the policy debate.

5.3 Fact presentation

How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?

($\star\star$) There is relatively little knowledge on this.

I believe that several modes of communications are needed: my experience is that the general public and scientific experts tend to focus on very different things and to be willing to trust very different things.

In the context of verifiability, my experience would be that the simplest possible explanations are quite effective with the general public, and that there is little demand to understand why the proposed verification steps are effective.

For instance, in the Helios voting system, the voting client displays to the voter a ballot tracker before sending any ballot (this tracker is just a sequence of letters and numbers), and the voter is asked to later check that this ballot tracker is correctly displayed on the Helios public bulletin board. This makes it possible for voters to track their ballot and make sure that it is properly included in the tally. Voters are active at performing this verification, even if they do not have any understanding of why this really does something (which would require to understand that the ballot tracker actually is a cryptographic hash of the encrypted vote and associated zero-knowledge proofs). They still have a pretty clear intuition that this ballot tracker makes it possible to track their ballot and to be sure that it is properly handled. And, if these voters have been using that system with the ballot tracker more than 2-3 times, many will start to complain if they have to use a system with no ballot tracker, claiming that this other system cannot be secure, because it does not make it possible to verify that their vote is received and properly stored.

Of course, apart from the basic instructions saying something like: “please keep a copy of your ballot tracker and check that it shows on the bulletin board”, there is additional technical documentation that is available for anyone with a basic background in cryptography who would like to understand why it works. But the huge majority does not care, and having that technical documentation readily available offers peace of mind to many potential auditors.

5.4 What information should be given to voters?

Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?

I am not sure, and would probably poll people in order to understand what they would like to know.

I would like to see basically what the VEIeS asks for: cryptographic protocols, security proofs, specification of audit procedures for verifiability. The source code also helps, mostly for privacy.

The more complicated part is about the trusted, or partially trusted components: even if I see their specification and code, I have no idea whether they are actually used or not, and it will be really hard for me to decide whether any of the components can be trusted or not. Here, what would probably help would be to see reports by independent observers (probably mandated by the parties) explaining what they could verify and what they could not after each election.

5.5 How to have the public involved?

Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of

All of these events seem to be useful! And I imagine that the having these organized by the Cantons, the Confederacy, and possibly also by political parties willing to build an audit expertise (for instance) would attract more attention than a vendor.

6 Risk management and action plan

6.1 Risk analysis

What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?

($\star$) The Internet context is always changing, and the system depends, to a large extent, on many pieces of software (browsers, operating systems, ...) that keep being attacked and updated. Besides, countries around the world are constantly trialing new voting systems, testing new review processes, observing new types of public reactions, and new research comes that make new threats become more (or less) plausible.

As a result, risk analyses should be continuously updated. The inputs can be obtained by monitoring the technical conferences in the domain, the experiences run by other countries, the security updates of the various components of the system (software and hardware), ...

The depth might be in part dictated by the speed at which actions plans could be executed: it seems particularly useful to have a well defined action plan when it makes it possible to complete the election and have results on time for publication. For instance, if there is a DDoS on the system that makes it unavailable for some time, it might be useful to have a well defined investigation and decision process that would make it possible to conclude, within the time frame of the election, whether the e-voting process can still be considered valid, or whether a longer investigation will be needed.

6.2 Benefits and downsides

What are the benefits and downsides of publishing the (dynamic) risk assessment?

As usual: the benefits is that they offer the possibility of public review and of obtaining inputs from helping people. The downside is that people spotting missing elements could obtain new hints that they could use to attack the system.

6.3 Supply chain

How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?

Elections need to take place in any case. I imagine that cantons should always have a backup plan (including vote by mail?) and that failing suppliers might need to bare the costs of activating this backup plan?

6.4 Priorities

Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?

These all seem relevant.

6.5 Standard methodologies

To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?

I do not know.

6.6 Support

Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?

Anyone willing to help should be involved! This risk assessment process looks like a relevant subject for PhD theses, that could be run in collaboration with the Confederation.

6.7 Responsibility

Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?

E-voting remains quite an experimental process, with much research still involved. As such, it seems hard to move away from a “best effort” expectation.

6.8 Modularity

Would it be meaningful to have a risk analysis from the canton focusing on the canton’s processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?

This sounds really hard to do: security usually does not compose well, and there are countless cases where two secure component put together result in a completely insecure system.

I would then try to identify if there are some components or processes that can be reasonably treated in isolation, and make sure to have a solid documentation justifying why it is believed that they be treated in isolation (this would help reconsidering if anything changes in the system at a later point). But it is likely that several critical components will need to be assessed jointly.

6.9 Octave Allegro methodology

Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology. Would this methodology be appropriate to handle the risks from the cantons’ / system provider’s point of view? Do you see any weakness / strong points in this methodology?

I do not have personal experience with this or other risk management methodologies.

7 Crisis management and incident response

7.1 Key elements

What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?

I am not sure of what is specific to Internet voting here.

7.2 Activation criteria

What are the right events and thresholds for an activation?

Evidence of errors or malfeasance, or evidence of significant public concerns.

7.3 Actors

Who should be involved in crisis management, with which role?

I do not know the possible actors well enough.

7.4 Communication organisation

How should the communication be organised (internally and externally)?

I do not know the possible actors well enough.

7.5 Existing structures

Are there already structures that should be involved in crisis management (e.g., GovCERT)?

I do not know the Swiss context well enough.

7.6 Investigation process

What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?

I imagine that it would look like any investigation by police units specialized in cybercrime.

7.7 Incident response

What are the requirements and stakeholders for digital forensics and incident response?

Probably the same as those of any case of cybercrime.

7.8 Prosecution

In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?

Probably in the same way as any case of cybercrime.

7.9 Election invalidation

How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?

I would tally the rest of the election (i.e., the votes that were not collected through e-voting), compute the election margin, and assess whether the impact of the incident could be large enough to change the election results given the election margin.

References

[BMM+20] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. Can voters detect malicious manipulation of ballot marking devices? In *Proc. 41st IEEE Symposium on Security and Privacy*, 2020.

[BR04] Mihir Bellare and Phillip Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive, Report 2004/331, 2004. `https://eprint.iacr.org/2004/331`.

[BRR+15] Josh Benaloh, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, and Poorvi L. Vora. End-to-end verifiability. *CoRR*, abs/1504.03778, 2015.

[Fra20] Jessie Frazelle. Securing the boot process. *Communications of the ACM*, 63(3):38–42, March 2020.

[HT15] J. Alex Halderman and Vanessa Teague. The new south wales ivote system: Security failures and verification flaws in a live online election. In *E-Voting and Identity - 5th International Conference, VoteID 2015*, volume 9269 of *Lecture Notes in Computer Science*, pages 35–53. Springer, 2015.

[IIMP19] Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, and Bertram Poettering. Cryptanalysis of OCB2: attacks on authenticity and confidentiality. In *Advances in Cryptology - CRYPTO 2019*, volume 11692 of *Lecture Notes in Computer Science*, pages 3–31. Springer, 2019.

[LHK19] Philipp Locher, Rolf Haenni, and Reto E. Koenig. Analysis of the cryptographic implementation of the swiss post voting protocol. `https://www.bk.admin.ch/dam/bk/de/dokumente/pore/E-Voting_Report_Locher_Haenni_Koenig_Juli%202019.pdf`, July 2019.

[LPT19a] Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. Addendum to how not to prove your election outcome, 2019. `https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcomeAddendum.pdf`.

[LPT19b] Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. Ceci n'est pas une preuve, 2019. `https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf`.

[LPT19c] Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. How not to prove your election outcome, 2019. https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf.

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Adrian	**Last name**	Perrig
Organization	ETHZ		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

As is well known, good security hygene utilizes several approaches, that are partially overlapping to cover the case of one approach failing. This is also referred to as "defense in depth". Approaches can in general be attributed to one of the following classes: prevention, detection / recovery, resilience. In my experience, a sound security system utilizes approaches from each of these three classes. The majority of attacks are covered by prevention approaches. But in case new attacks are being discovered or in the case a defense approach is circumvented, detection of attacks with subsequent recovery represents a second line of defense. Finally, systems can be constructed such that even in the case that an attack is not discovered, the final property is still preserved: resilience approaches can ensure this. In the context of voting, however, resilience approaches are challenging to establish.

Another dimension to answer this question are the properties that a secure voting system needs to provide. The general security properties include: confidentiality / privacy / anonymity, integrity, availability, auditability, which are all important for voting. Specific properties that are important in the voting context are: vote verifiability, correct vote count, etc. The requirements are very thoroughly laid out in these documents: Federal Chancellery Ordinance on Electronic Voting (VEleS) [2] and Annex of the Federal Chancellery Ordinance on Electronic Voting VEleS [3].

The most important answers I would need to conclude that Internet voting is trustworthy are the following.

E-voting system aspects

- What system is being used? Which algorithms / cryptographic methods are used? How was the system verified for correctness? How are the many properties, such as vote verifiability, achieved? How is the security of the software implementation achieved and verified?

- How are network security aspects covered, such as DNS or routing attacks. For instance, BGP prefix hijacking can be used to re-direct network traffic for analysis or alteration.

- PKI aspects represent a tremendous security challenge. Sovereignty is a core aspect here. If the standard TLS PKI is used, then a very large number (> 1000) cryptographic keys are being trusted to authenticate the web site, the vast majority of which are outside of Switzerland. A malicious entity can create a MITM attack using a malicious certificate.

- Supply chain attacks. What are the processes for the management of the system machines? How is it ensured that the hardware of the machines cannot be maliciously altered once deployed? (For instance by adding equipment to eavesdrop on the memory bus.)

- How are split-world attacks prevented? In these attacks, the adversary creates a "virtual world" around the voter, providing it with a fake application, fake certificates, etc. This way, the voter believes that it has correctly voted, that its vote was correctly counted, etc. But instead, all these operations occurred in a virtual world environment, so the vote was not effectively counted in the real election. In this context, even for points such as 2.3.3 of the annex document [3] stating "Tips and rules on vote casting are given on the internet [...]", it is unclear how one can ensure that voters are looking at the correct document, given TLS certificate vulnerabilities. If this process can be attacked, then voters can be given incorrect instructions.

- How are malicious administrators prevented? In particular, storage, backups, etc. how are they managed? A particular danger is the registration and deletion of administrators, as any threshold-based approach (which may require a certain number of administrators) can possibly be circumvented through the registration of fake administrators with subsequent deletion. Thus, such creation / deletion events have to be logged in a way that cannot be erased, and periodically reviewed by all administrators.

Voter aspects:

- How are voters registered / enrolled?

- How is voter identification accomplished?

- What processes are in place in case a voter loses its materials or forgets a secret code?

- How is secret information sent to the voter? In case information is sent by paper, how can one be sure that the information was not observed during the printing or transmission process?

- How can it be ensured that no fake voters are being registered, which could then be used to cast additional votes?

- How was population educated on mechanism? Users need to understand risks and perform some operations for verification / validation.

Client security

- How can user ensure correctness of voting software? Or web site that is visited?

Result interpretation, attack detection

- Are statistical measures in place to assess correctness of result?

Finally, how can the system ensure that no framing attacks are possible? In Framing, an adversary behaves in a way such that a legitimate entity appears to behave maliciously. In such attacks, the adversary wants to create a reputation risk.

To achieve high confidence for the answers obtained, a full formal verification of the critical components is necessary. Given the high complexity of such a system, it is infeasible for a human to manually verify the security (given the exponential increase in possible states with the increase in complexity of the system, the verification will

also encounter scalability limits even for fully automated approaches).

The human aspects surrounding printing and administrators is very challenging. Very detailed "ceremonies" need to be specified for each and every possible case. Typically, it is not the cryptography that breaks in these systems, but the human processes. Wherever possible, formal verification methods also need to be used in here to ascertain correctness and completeness of the specification.

In addition to the points laid out in documents [2] and [3], I would like to emphasize the following aspects:

- split world attacks are serious,

- network-based attacks (preventing availability),

- PKI aspects,

- human aspects of printing and system administrators (especially also the formal verification of their processes),

- ensuring that voter has correct information or software obtained on-line (in case of OS vulnerability, TLS PKI vulnerability enabling MITM attack).

To prevent network-based attacks, and to fix the PKI vulnerabilities in today's TLS PKI infrastructure, the SCION secure internet architecture has specific solutions. These systems can support a voting application with a small amount of effort. (I can provide additional information here if desired.)

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks.

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

	Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
Indeed, the possibility of a cryptographic attack is always there. However, vulnerabilities typically stem from implementation errors or human error (in the administration of the systems). Moreover, even though numerous cryptographic weaknesses have been uncovered in the past 20 years (in particular of cryptographic hash functions), the attacks were very challenging and could not easily be used against deployed systems. Thus, with the progress of cryptographic methods over the past decades, it is unlikely that a cryptographic vulnerability will be the culprit of a vulnerability of the entire system. Another aspect are quantum computers, which can disrupt most currently used asymmetric cryptographic systems. Although the risk exists, my assessment is that in practice the risk is very small, as a working quantum computer that can actually pose a threat to a currently used cyrptographic system is at least 15 years away. The main risk, however, is vote privacy, as one could record network traffic and determine 30 years later with the use of a quantum computer, how someone voted. There are two approaches for handling this threat: the use of quantum-resilient cryptographic mechanisms, or the use of symmetric cryptographic mechanisms to achieve communication secrecy (symmetric-key techniques are more resilient to quantum computers, and generally not at risk even once quantum computers exist).	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
Proofs done by hand can definitely be flawed. Machine-checkable proofs, however, are much more likely to be correct. One has to very carefully consider the security model and assumptions that underlie the proof, as an adversary may be able to conduct an attack by violating the assumptions or step outside the verified model. Generally speaking, the system is trustworthy if the assumptions are model are sound, and if the security proofs are conducted with a tool-based approach (model checker or theorem prover), such that they are machine-checkable or machine-checked.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
This is a very important point, and I would need to see and analyze the details to make a strong statement in this regard. In fact, this is one of my core concerns: how can the printing system ensure that no camera is mounted that observes the printed papers? Or how can it be ensured that the instructions sent to the printing machine cannot be recorded, enabling reconstruction of the printed sequences? Here, I would suggest that printing happens at a national level, as the overhead of creating a secure printing facility will likely surpass the effort that each canton can expend.	
2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are

	distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
Control components from different vendors is definitely advisable. The economic realities for software development make it very challenging to create truly distinct verification components by a single vendor. Given that only 1 out of 4 components needs to be trustworthy, it makes perfect sense to obtain them from 4 different vendors. In this context, I cannot see how the different vendors introduces additional attack vectors.	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
This software should also be written by a different vendor, for the same reasons as stated above. The larger the heterogeneity of verification software, the stronger the overall security of the system. In homogeneous systems, an adversary can target the specific implementations, but if the actions of some verification components cannot be predicted, the adversary is faced with a high probability of detection.	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
Indeed, heterogeneity at the OS and HW levels is also essential. For the same reasons as mentioned above, an attacker's task becomes much simpler if only a specific OS and HW needs to be targeted. The downside is the increased cost and complexity for maintenance, which requires continuous updating and following vulnerabilities of all involved systems. From a personnel perspective, multiple administrators may need to be hired, which administer different OSes, or it becomes more difficult and expensive to hire administrators that are versed across a diversity of systems.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to

	transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
This is a good model, especially if some fraction of users can engage in additional verification and potentially purchase additional equipment. Challenges here include framing attacks, where a user claims that its vote was incorrectly counted, even though is was correctly counted; and cryptographic algorithms that are vulnerable to quantum computers, which would permit to violate vote privacy guarantees once such computers become available and powerful enough.	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
Formal verification needs to be performed to achieve a high level of assurance for software. Given the very high overhead of performing such verification (it is about 5 times the amount of work of writing the code), the system should partition the code into security-relevant and security-irrelevant parts, such that only the relevant parts need to be formally verified. The research group of Prof. Peter Müller at ETH has been working on code verification systems and has developed the Viper framework. A challenge is to connect such code verification with protocol verification, which Prof. Müller's group has recently accomplished in collaboration with Prof. David Basin's group also at ETH. However, these systems still require a high effort to verify large systems, a cautious estimate for the verification of a voting system would likely be above 10 person years. Here, academia could assist industry in deploying these mechanisms to achieve a fully verified system.	

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
In the consideration of these points, the following risks should receive stronger consideration: **- split world attacks (although assuming the printing and postal deliver are secure, these are perhaps not serious),** **- network-based attacks (preventing availability),**	

- PKI aspects,

- human aspects of printing and system administrators (especially also the formal verification of their processes),

- ensuring that voter has correct information or software obtained on-line (in case of OS vulnerability, TLS PKI vulnerability enabling MITM attack).

While network-based attacks can result in a denial-of-service (DoS) attack which prevents people from voting, they can also be used to violate user privacy or facilitate MITM attacks in conjunction with a PKI-level attack. As Prateek Mittal's research groups recent results show, routing-level attacks could be abused to obtain fraudulent TLS certificates, de-anonymize users using Tor, etc.

PKI aspects are also very serious, where an entity can obtain relatively easily fake certificates for web sites to perform a MITM attack or outright forge the content. For instance, if voting training web sites could be attacked in this way, the voter could be taught erroneous information on how to vote, could be instructed to download malware, etc.

2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?

I am not intimately familiar with all the provisions of the standards mentioned, but I believe that the requirements with respect to administrator enrollment and deletion are important (which I mentioned in detail in the answer to question 1).

2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?

Network security was not considered, which opens up numerous potential avenues of attack given the insecurity of today's systems. The SCION secure Internet architecture can be used today in Switzerland (several Swiss ISPs support the system) and would absolutely prevent such attack vectors.

2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).

Given the relatively limited application space of e-voting, the integrity and secrecy of votes is easier to guarantee than for general customer data. However, the public verifiability and numerous other requirements do obviously add significant complexity. Since the privacy requirements of voting are more stringent, the resulting protection is likely superior than for other systems.

2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
The advantage and curse of e-voting is the all-or-nothing aspect: a significant vulnerability may result in the ability to completely change the outcome of an election, but in the absence of a vulnerability the system will be highly secure. It is rare that computer vulnerabilities result in a system that will enable some limited number of forgeries. **Violation of vote privacy enables an organization to determine the active voters, and attempt to influence them at the next election. Well funded individuals or entities could possibly afford such an attack. Since it is my research area, I can see possible Internet-level attacks that make use of traffic analysis to violate vote privacy. In such an attack, the recording of Internet traffic does not leak information, thus it would be very challenging to detect. A more invasive attack, such as BGP prefix hijacking, would be easier to detect, but could be conducted remotely.**	

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or dis-played incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
Even if a small number of voters performs such checks, a large-scale attack would likely be detected. Based on anecdotal evidence, Switzerland has a substantial number of individuals who are concerned about e-voting fraud, and would thus perform active verification.	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
This is definitely an excellent method, and prevents the PKI-level attacks I mentioned above. The challenge is that users need to indeed obtain the correct values, and a malicious training web site could provide incorrect information to users (which would	

be easily detectable if some users would report deviations). If voters are given the opportunity to report incorrect values, I believe that a sufficient number of voters would perform the validation, thus enabling detection of large-scale fraud.	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
This is very challenging, as malicious software could possibly also tamper with the checksum computation or display. An independent device would need to use remote attestation and trusted execution environment computation to obtain strong properties in this space. Given the availability of SGX or TrustZone on ARM devices, this is actually a possible avenue, but would require substantial effort for SW development.	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
Over the coming 15 years (at least), I do not envision any issues for traditional cryptography with respect to vote integrity. However, vote privacy is at risk, and thus mechanisms need to be in place to ensure that vote privacy is secure even in the presence of powerful quantum computers. If no personal data is revealed in the communication, then this may be achieved, however, this would need to be checked in detail to ensure that no master secret could be determined that would then violate privacy properties.	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
Yes, MELANI and related guidelines to keep a computer system secure should absolutely be recommended. These guidelines definitely reduce the possibility for malware. For voting, however, a more stringent system environment could be considered, such as making use of trusted execution environments such as SGX, which would offer security even in the presence of malware.	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
Although vote buying is relatively simple to perform with postal voting, the sending of physical envelopes with the signature, the exchange of money, and the posting of large number of envelopes in an non-concerning manner, all make large-scale attacks	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

highly challenging. In e-voting, however, such attacks can be much easier scaled up, where a voter could simply take a picture of the relevant information and send it to the entity. With digital currencies, the payment can also occur in a secret fashion.

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
An attack / vulnerability risk analysis should result in identification of security-critical protocols / implementation / processes. All security-critical aspects should undergo formal validation. Such formal verification can be performed by the vendors, and is only validated / checked by the certification bodies. With the use of public verification tools, anyone can in fact perform the validation.	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
In security, it is a dangerous approach to leave open known issues, as attacks only get better over time and weaknesses can combine to form serious issues. Numerous examples make this point, where several seemingly inocuous weaknesses in combination result in a serious vulnerability.	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).
Indeed, one needs to be careful to ensure that no seeming conflict-of-interest situation can be construed against any of the entities driving the technology forward. Thus, a recommendation would be to draw input from several entities on which entities can perform the examinations.	

3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
If examinations are indeed based on formally verifiable statements, then the validation of those statements is relatively straightforward, where the examiner needs to verify mainly the model and assumptions made. If examinations are heuristic in nature, for instance based on packet fuzzing, then a certain quality metric or level of certainty (e.g., through code coverage) needs to be defined, in which case it gets complicated on how such levels need to be set. The reliance on existing standards could be helpful, although I am not familiar with them.	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
If the protocol or code is changed, the examination needs to be updated. An advantage of formal verification is that such re-examination could possibly be fully automated, ensuring that the properties are still satisfied after the changes. If serious vulnerabilities appear that affect the operation of any system component, the system would need to be re-examined – for instance, the discovery of the Meltdown or related vulnerabilities of SGX would need to have prompted re-evaluation if SGX technology was used for any security-critical component of the system.	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
For a highly critical system such as e-voting, a wide range of experts should provide recommendations and help guide or at least initiate directions of examinations. Such experts would need to be familiar with the operations of the system, and provide inputs about newly appearing risks and vulnerabilities. Early and proactive anticipation of risks ensures the maintenance of a high level of trust by the society in the e-voting system.	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
As with almost every complex decision process, expert opinions will likely diverge widely on many topics. Whom should one pay attention to? A good example is quantum computing, where some experts predict doomsday scenarios for current cryptographic systems, while other experts predict that useful quantum computers are impossible to build. Often, the truth lies somewhere in between the extremes, but hopefully over time, it will crystallize out which experts have a good track record for pointing out which issues are important to pay attention to. A learning process will be required to guide the administrative and operative structures of e-voting.	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code

was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
This is a very challenging space to navigate. Clearly the software vendor would like protection of the source code, while the open hacker community needs open access to perform validation. In many settings, NDAs and review contracts stifle open verification. In the nature of this technology, the software vendor should be willing to publicly disclose the software, and to build the business model around that premise.	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
The full system specification and documentation should be available to enable in-depth public scrutiny.	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
Ideally, much examination and scrutiny can occur before a wide-ranging public validation. In typical systems, the number of discovered issues diminishes with increasing maturity of the system, which can be measured and used as an indication when the system is ready for publication.	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
Ideally, yes. The better the documentation and transparency of the system, the higher the level of trust that can be derived.	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

This certainly will depend on how the oversight and operation structures are implemented. The BK certainly takes on a central role, which should be supported by a scientific committee, interacting and interfacing with the broader stakeholders.	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
Following ethical disclosure (which needs to be specified for the e-voting system), vulnerabilities need to be communicated and publicly disclosed based on a clear schedule. Numerous issues arise. What if a severe vulnerability is disclosed a few days before an election? What if it is disclosed after a close election, whose results may have been influenced? In any case, it is important to have a clear rule on when ethically disclosed vulnerabilities (or internally discovered vulnerabilities) will be publicly published. Otherwise, it may often appear advantageous to wait with public disclosure, which will likely erode confidence in the long term.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
PIT / bug bounties are definitely useful to create confidence in the system (assuming that no severe vulnerabilities were identified). Before engaging the broader public, however, professional pen testing and researchers (academia and industry) should be involved to verify the systems. Thus, a staged evaluation is advised.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
That is a good approach, enabling the gathering of experience in a relatively low-stake environment.	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
Given the high complexity of e-voting systems, the federation and industry should support the cantons as much as possible, to reduce replication of effort by the cantons to a minimum.	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
If they are consistent, then trust in e-voting will be increased. However, given the likely different constituencies using e-voting, the results may diverge. For transparency's sake, the detailed results should be revealed, with the downside that such publication may indicate a potential for weakness in e-voting.	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

Based on past security systems, the presence some undisclosed verification / intrusion detection system has the potential to be a strong deterrent. Adversaries dislike uncertainties. If they know that some intrusion detection system is running, which may potentially catch an attack or discover the presence of a potential bias, they may shy away from attacking. Thus, my suggestion is to invest in a team that creates additional security measures to catch attackers. **Additionally, statistical plausibility checks should be in place, and the divergence of the expected result could be published. With a good statistical model, a low divergence can create trust in the e-voting system.**

4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
Statistical plausibility checks can offer many advantages. As stated in the previous response, trust in the system can be enhanced. In case of an actual attack, there should be a strong indication of divergence, which would trigger a closer investigation, again creating more trust in the system.	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
Many experts will help based on voluntary work to support our democracy. Additional help from academia, however, can be achieved through distribution of research funding to support research projects that are aligned with the e-voting agenda. This will bring exposure of the problems to PhD students working on those projects, and in turn to MS and bachelor students through thesis work and projects. To further raise awareness, a summer school and a seminar series can be established revolving around e-voting topics. Most of these programs can be achieved through existing	

resources (e.g., SNF, Innosuisse) or through modes additional funds. Since these efforts will be open, the broader public is also invited to participate. The establishment of an expert science panel is advised, which can be based on voluntary pariticipation or modest remuneration.	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
Some individuals in the science community are also well-versed in the political space. Such «bridge people» have an important role to bring together the two communities by speaking their respective languages and translating between each other. Given the importance of the e-voting effort, such individuals will naturally step up to their calling.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
It is often a challenge to translate scientific results to be understood and appreciated by the broader public. Our media take an important role in this context, in that they write popular articles and translate research results into easily understandable articles.	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
Indeed, demonstrating the power of verifiability, formal verification, etc. will be very helpful to establish trust in the entire system. An entire class can be taught on this subject, with a lecture on each major component, which can be presented online and enable anyone to follow along and explore the different systems.	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
As mentioned above, summer schools, public lecture series, online courses, etc. Public debates and hackathons are also good ideas.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
A scientific expert panel should meet regularly (perhaps twice a year) and collect potential risk factors. New emerging vulnerabilities can be discussed in online discussions to enable rapid reaction. The public can also submit potential risk factors, and an ethical disclosure process can also funnel potential vulnerabilities to the right people. **A suggestion would be to establish a web page with the known risk factors, along with an assessment of their severity. This will help to reduce the number of submitted risks, as people can first navigate the known risk factors before they submit their perceived-to-be novel risks.**	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
Assuming that all the risks are properly addressed or managed, a dynamic risk assessment enhances transparency and trust.	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
This is a known challening problem, even at goverment-scale or large multi-national corporate scale. It is doubtful if each canton can resolve this by itself. A recent breakthrough is the «chip-x-ray» system developed at PSI, to ensure that a computer chip contains the correct transistors (and in particular, does not contain any superfluous connections or transistors that may implement a back-door operation).	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
Perhaps the level of trust in the system is the most critical metric to optimize, thus the action plan measures that maximise public trust are the most important.	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
This is not my core area of expertise, I assume that other experts will be better versed in this area.	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
The scientific expert panel should advise the administration on these points. Some university research groups specialize on these aspects, for instance the Risk Center at ETH.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here.

	How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?
Click or press here to enter text.	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
Click or press here to enter text.	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
Click or press here to enter text.	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
Click or press here to enter text.	
7.2	What are the right events and thresholds for an activation?
Click or press here to enter text.	
7.3	Who should be involved in crisis management, with which role?
Click or press here to enter text.	
7.4	How should the communication be organised (internally and externally)?
Click or press here to enter text.	
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
Click or press here to enter text.	

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
Click or press here to enter text.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
Click or press here to enter text.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
Click or press here to enter text.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
Click or press here to enter text.	

FCh1

DemTech Group

DEMTECHGROUP
DEMOCRACY, TECHNOLOGY & TRUST

Ribegade 19 st th
2100 Copenhagen
Denmark
CVR: 35527052

Redesign of Internet Voting Trials in Switzerland 2020

Answers to the Questionnaire for Workshop 1

Carsten Schürmann

March 2020

Preliminary Report

Table of Contents

1 Big picture

1.1 Imaginary country, the ideal voting system

The central and arguably most important objective of any voting system is to strengthen public confidence in the election outcome.

If the electorate loses trust in the election, voters no longer accept the legitimacy of government, which can have disastrous consequences, including civil unrest, political polarization of the electorate, etc. The history books are full of examples. To my knowledge, there is only one reliable mechanism to strengthen public confidence and this is generating *evidence* during an election to be *audited* post-election to verify that the election outcome is correct.

For elections that take place in controlled environments, such evidence is relatively easy to come by, for example, hand- or machine-marked paper ballots or voter-verifiable paper trails and it can easily be audited, for example by recounting, conducting secondary counts, or risk-limiting audits (RLAs) that self-correct the election outcome with high probability in the case of error.

When voting from uncontrolled environments, however, as it is typically done when using an Internet Voting systems, a succinct definition of evidence is much harder to come by and often consist often of collections of cryptographic constructions, such as zero knowledge proofs of knowledge, digital signatures, return codes, and threshold keys. There is also no broadly agreed methodology on how to audit this evidence. There is no clear definition of what constitutes a post-election audit or what has to be done to settle an electoral dispute. To my knowledge every EMB using Internet Voting has designed their own more or less convincing ceremony of decrypting internet votes and checking their validity. As the nature of evidence is cryptographic, its definition is in general not self-contained, but relies on assumptions about the system generating it. This constitutes a substantial trust base, which is also the reason why many academics recommend caution with offering Internet Voting even if only as an alternative voting channel.

To assess if the voting system is good in the imaginary country, we'll have to go ahead and convince ourselves first that the notion of evidence proposed is compatible with the electorate's expectations and will be accepted as such.

Second, we need convince ourselves that the auditing procedure is complete and independent from the counting process. Let's look more closely at what constitutes evidence and how to define auditing.

1. *Evidence:* Evidence refers to the artifacts used to determine/audit the election outcome. The definition of evidence should be completely independent from the crypto-protocol and the technology used, and furthermore it should not depend on being kept secret to be valid. We need to assume that the evidence may be leaked to the public, as no computer systems is 100% secure. The evidence needs to be voter-verified to ensure that it really represents the intent of the voter and not the intent of some malware running on the voter's laptop.[1] The evidence must be immutable and it must guarantee vote-privacy. Ideally, it should guarantee everlasting privacy of the vote, which means that no matter if the underlying crypto is ever broken, the connection between voter and vote remains private. Furthermore, it must be possible to check the eligibility of each and every vote. The evidence should be consistent with local culture, which means that the proposed chain of custody is socially accepted to protect evidence from the time it is generated to the time when it is audited. Vote coercion resistance is intentionally excluded from this list.

   If the imaginary country's society is based on the Rule of Law and the Rule of Order, paper is a nearly perfect evidence because we can rely on the chain of custody. But if the imaginary country were to use Internet Voting, we would insist that digital evidence is defined independently from any crypto-protocol and technology. The evidence needs to speak for itself and needs to be understood (at least in principle) by the electorate.

2. *Auditing:* The auditing process must be defined independently from the technology used to collect the evidence. In Internet Voting, the auditing procedure is an algorithm that checks all parts of the evidence. Ideally, the auditing framework is defined and implemented before the voting system is procured. Taking all parts together, the audit should paint a complete picture of why the election result is correct.

3. *Technology:* Only if it is clear and accepted what kind evidence is required to create confidence in the imaginary country and how to audit it, only then can we assess feasibility and the suitability of a particular voting technology.

[1] The Voatz system used in the 2018 midterm election in the State of West Virginia, printed votes submitted by a mobile phone, which should not be considered evidence, as it is not voter-verifiable.

In many countries, it is the case that the legal framework has to be changed to allow internet voting. Some countries, including Denmark, have been reformulating laws with the goal to be able to procure a particular technology. This, however, in my opinion, is the wrong way of going about it. The legal framework needs to protect the values of a society, and should therefore aim to rule out what is deemed an unacceptable voting technology. We will have to look at the legal framework of the imaginary country and convince ourselves that the principles for evidence production and auditing are required in the clearest terms.

Next to Switzerland. We observe that the requirements for individual and universal verifiability are part of the legal framework, but that the legal framework does not define in further detail what kind of evidence is acceptable and how it is defined. The legal framework appears to lack provisions on how to audit evidence as well. This in turns means that critical decisions are left to the vendor, which then has to be trusted.

2 Risks and security measures today and tomorrow

2.1 Verifiability

Verifiability is a property that can guarantee integrity of the election result, but it cannot guarantee vote privacy and availability. Verifiability by itself does not define evidence as we described in the previous section, but evidence can be used to check verifiability.

2.1.1 Crypto-protocol

Of course it is possible that cryptographic building blocks can be flawed despite the fact that they adhere to a standard, and it is also possible that the use of several otherwise correct cryptographic building blocks in combination is flawed.

Cryptographic building blocks can be broken from one minute to the other, for example, when someone identifies a collision in a cryptographically secure hash function (which means to identify two messages m_1 and m_2 that map to the same hash). Hash functions typically map elements of a large domain onto elements of a much smaller domain, therefore collisions necessarily exist. When hash functions are used, for example, to compute message authorization codes (MACs), the MAC is only secure as long as collisions are difficult find. A recently broken hash function is SHA1, and it is most likely a question of time until collisions for other hash functions are found as well.

Crypto-protocols usually rely on many cryptographic building blocks, such as one-way functions, HMACS, encryption and decryption primitives, signing, blinding etc. If two cryptographic building blocks are used with the same cryptographic key, then things can go terribly wrong. Related, if randomness is reused in cryptographic protocols, the security can often be broken.

Therefore, it is not sufficient to just consider and rely on the security of the cryptographic building blocks.

2.1.2 Security goals

First things first. A security proof always abstracts away from the real and implemented crypto-protocol. Proving a crypto-protocol secure in the abstract guarantees that no attacker will be able to break the protocol in the abstract. But it does not imply that the implementation is also secure. If we picture abstraction as a line, the adversary will not be able to attack above the line, but it does not preclude an attack below the line.

Once the crypto-protocol is abstracted, the security argument goes as follows. Assume, there is an attacker who can break the security of the crypto-protocol then one can turn this attacker into an attacker that breaks a generally believed hard problem, for example computing the discrete logarithm of an element in a cyclic group, or another, which is called the decisional Diffie-Hellman assumption. Therefore, security arguments are in general reduced to the hardness of such a basic problem and it is a generally accepted method to reason about security. However, quantum computers challenge this view, because they will be able to solve hard problems in no time. Google, for example, has recently claimed quantum supremacy, claiming that they could solve a hard problem in only 200 seconds, which would take otherwise 10000 years computation time on a modern super computer. When quantum computers become more available, the security arguments of much of our infrastructure will have to be revisited.

The security proof is pure mathematics. The only way to break the security of a crypto-protocol that has a security proof is either by breaking the problem assumed to be hard, or by attacking below the abstraction line.

2.1.3 Printing office

The underlying question here is what constitutes evidence of a successful individual verification of the vote. Clearly, it should be easy to do the checking otherwise not many will check, but the return code system should be accountable as well. Mechanisms should be in place to disprove allegations that the Internet Voting system was not working correctly, a desirable property of the return-code mechanism that is often overlooked.

Alternatives to the printing of return codes include the following: The now discontinued Geneva system uses an oblivious transfer protocol to establish an on demand return-code mechanism. The NSW system and the Estonian system displays a barcode in the voting app to allow the voter to decrypt the encrypted ballot in a verification app. I am not suggesting that any of these techniques is better, but I am suggesting that there might be other return code mechanisms that may render the Printing office obsolete.

Ideally the mechanism for individual verifiability must should produce evidence that can be checked independently after the election by auditors or even in the court of law. In my view, such evidence would make Internet Voting system more credible.

2.1.4 Independence

If the control components run the same software, there is no independence. In the case, however, that the vendor provides two independent implementations of the software stack that runs in parallel in each control component, then both requirements of the VEIeS are satisfied. In comparison, to my admitted rather limited knowledge, flight control computers in an Airbus 320 are triply redundant, where each flight computer consists of two different hardware and software stacks. I think it is worth pointing out, that the required redundancy only helps with availability of the system, but this redundancy does not necessarily improve public confidence in the integrity of the election outcome.

2.1.5 Verifier

As we have described in the introduction, ideally, the auditing framework should come first, i.e. before the Internet Voting system is procured. This means, it is natural to expect that the software for the verifier should be implemented from scratch by a different organization, perhaps even by the EMB itself. Preferably, the verifier should also use different libraries to guarantee as little code overlap with the software produced by the vendor, as possible. If not, bugs that may be contained within the vendor's verifier will not be caught.

2.1.6 Operating systems and hardware shall differ

Redundant control components in the system are beneficial for availability and integrity: They make sure that while running the system (including computing evidence), issues are kept to a minimum and the likelihood of a fatal crash is reduced, while at the the same time the likelihood is increased that the post-election audit of the evidence will be successful; and they also make sure that software bugs and hardware failures do not disrupt the operations of the voting system. In terms of vote privacy, not much is gained using multiple systems, in fact, the opposite may be true. Using redundant control components is a good idea, especially when the underlying operating systems are updated in between elections, for example, to patch vulner-

abilities (see the CVE database[2]). If all of the control components were to run the same software, a bug in the underlying operating system might be replicated on all control systems, which might lead to a collective failure of all control components if they were to run, for example, the same operating system. Therefore, to make sure that the system remains functional after broke updates, it would be a good to use different hardware and operating systems. Of course, there are also other mechanisms to ensure that security updates are successful, for example, extensive testing or re-certification, but this relies on external operational controls, whereas using different software/hardware will improve reliability, even if no testing has been done.

2.1.7 Other forms of verifiability

The critical part of any voting system providing individual verifiability is that the evidence used to determine the election outcome captures the voter's intent correctly. The question should not be if the device is trusted. All systems can be hacked and voters know it. Many laptop users block the camera in their laptops for privacy reasons. Also with information that is going to appear in the media (2020 is US election year), voters will be constantly reminded about the security of their devices. Individual verifiability does not only defend against an attacker, but also against software bugs that might be present in the voting client, either a custom-made stand alone program (like in Estonia) or a Javascript client that is loaded into the browser on demand. Transferring and evaluating cryptographic values appears to have a negative impact on usability, which will lead to less people checking the information. A bulletin board of encrypted votes is also not desirable, because most common encryption techniques will be broken in a few decades (yes key sizes matter), even earlier, if quantum computers become more ubiquitous. To my knowledge, there is no good technique to construct bulletin with everlasting privacy, so more research is needed. The Estonian system displays the randomness used to encrypt a vote, and gives the voter 30 minutes access to encrypted vote using an app, that accesses the ciphertext in the database and then decrypts it. The drawback is, that anyone with access to the vote database who gets to see the barcode, can also decrypt the vote.

2.1.8 Correct implementation and protection from unauthorized access

Internet Voting systems are highly complex systems. Cryptographic mixnets, even more though. One slight misuse of randomness can have disastrous consequences and break the security of the entire system. There are stan-

[2] See `https://cve.mitre.org/`

dards, but it is not clear if any of those would have caught the vulnerabilities exposed in the Swiss Post system. These include, OWASP Application Security Verification standard, FIPS, or Common Criteria with the right protection profile. But there are also other ways to increase code quality. (1) The choice of programming language: F* was used to generate and verified implementation of TLS 1.3[3], and it is conceivable to do this also for a mixnet implementation, such as the one used in the Swiss Post voting system. (2) Formal methods supported by ready-made tools, such as ProVerif, Tamarin, or EasyCrypt, to prove an abstract version of the implementation of the voting protocol, but these so called models are not executable programs. (3) Software verification tools. If the implementation is in Java, one could also use tools such as KeY to verify correctness, but it is not clear, how difficult it is to derive the correct specification or if such tools are good enough to verify larger developments, such as an Internet Voting system. To summarize, exact specifications of the security properties, plus formal methods, can help identify implementation issues already at development time.

2.2 Security related risks top-down

2.2.1 Threats

One threat that is not considered is that of an alleged malfunction of the system, be it due to a cyberattack, a programming bug, a human error, or bad configuration. Actually, this is the most serious threat against public confidence, especially, if the Chancellery has no evidence to prove or disprove the allegation. One comment to the table 3.1, is that the attribution who executes the attack is unnecessarily limiting. The adversary model should include eavesdroppers, criminals, activists, insiders, parties, nation states, among others The table also lacks threats against the printing office, for example, producing wrong return codes, or sending the return codes to the wrong address. There should be requirements regarding which source of randomness to use and how to use it.

2.2.2 Security measures

Not to my knowledge.

2.2.3 Unmet requirements

[3] https://github.com/project-everest/mitls-fstar

One additional requirement could be that the source code should be minimal, not contain any dead-code, and include all necessary libraries to build the system. 3.3.4. This requirement apparently allows the transmission of unencrypted votes over TLS, which does not protect from inside eavesdroppers and insider attackers. 3.3.5. It is a good habit to get into to sign all data, and check the digital signature before data is accessed and used. 3.15.2. is weak. How is the eligibility of voters guaranteed? Regarding 4, it appears that the recommendations are very prescriptive with respect to the voting system that is to be procured. I would like to suggest to consider requirements more in terms of evidence production and auditing, that would allow the Chancellery to reject unsuitable solutions, instead of formulating the requirements with the intention to accept a suitable solutions.

2.2.4 Degrees of security for critical data

I am not entirely clear how to answer this question. “Far better” is a strong word. I don’t know how other fields guarantee integrity and the privacy of data, but it is pretty clear that a good voting system could be used to store data, and the threshold crypto schemed required by 4.4.10 would govern access. It is not clear how key materials a managed in other fields, there are many different ways how this could be done. It is conceivable that components under certain circumstances also use threshold schemes. In the end, the vote is encrypted with a key of certain size, and it possible that the database storing all health records is encrypted using the same size key. What is different of course, is that the voter does not receive a receipt to check the vote later in the process. There are no mechanisms in place to contest a vote. A completely verifiable system will guarantee the existence of an auditing mechanism that inspects the digital evidence produced by the voting system.

2.2.5 Internet voting and postal voting

As I said in the introduction, the difficulty of designing an Internet Voting system is not to make it secure, but too make it trusted. The more complex a process the more difficult it is to build trust that everything works well. I don’t believe, that the biggest problem of (a well-engineered and secure) Internet Voting is that someone alters the vote. The biggest problem is to defend against allegations that the election outcome is correct and worthy of trust. Polling station voting and to a lesser extend postal voting, are much simpler than Internet Voting. In postal voting, the eligibility of voters can be checked and it can be ensured that every voter on voted once. Of course, it is possible to attack the postal voting system, by invalidating ballots with a pencil,

and other attacks, however, it is always possible for those concerned to join the opening and counting effort, strengthening public confidence in the election outcome. This is not so easy with an Internet Voting system. An alleged attack against the voting database, for example, by claiming that all ballots were replaced altering the election outcome has a much more profound impact on public trust than accusations that a few letter votes in a particular precinct were tampered with. Internet Voting, if not done right, i.e. without a clear definition of evidence and auditing, threatens public confidence in the electoral process. Security and public confidence, are surprisingly unrelated notions. A secure system does not necessarily enjoy public confidence (see elections in Egypt, that are protected by the military and still people don't trust it), and voting systems that may not be secure can very well be trusted.

As an election security expert, living outside Switzerland, I cannot say, which organization may try to manipulate or read votes. If the organization is as powerful as described in the questions, then most likely by social engineering. In some countries, key shares to reconstruct the private election key are stored on smartcards that are then sealed by the external auditor. Social engineering can give access to the smartcards distributed to the election committee members or simply to the computer program generating the smartcards (an adversary only needs to control the source of randomness, to be able to reconstruct all key shares independently). Having seen the movie Icarus[4] recently, it has become very clear to me, that there is no such thing as a temper-resistant seal especially when dealing with powerful organizations. Internet Voting comes with so many implicit assumptions, that are impossible to quantify. If any of those assumptions is broken (for example adversary controlling the source of randomness for mixing), the Internet Voting system is rendered insecure.

2.3 Selected risks

2.3.1 Individual verifiability

Studies have shown, that the more usable a system is, the more people check the return codes. In Norway, for example, the fact that an SMS was sent to the voter, right after the vote was cast, prompted relatively many to check their return codes. It must have been the beep announcing the arrival of an SMS that must have caught their attention. In Estonia, where QR code was used to allow the voter to decrypt the ballot and provided sufficiently many checks. The system in Estonia, was much less usable, in part because

[4] https://en.wikipedia.org/wiki/Icarus_(2017_film)

the voter had to install the voting program on their computer and an app on their mobile phone, which was then used to scan the barcode from the computer the voter used for voting, accessed and downloaded the vote associated with the voterID from the digital ballot box, decrypted it and showed the voting preferences in the clear. Therefore, in order to make sure that voter check, the return code system has to be simple. I am not aware, if there are any return code systems that would *force* a voter to check, for example, before their ballot is recorded. I suspect that such a system could be designed and built, but more research and user studies are necessary.

2.3.2 TLS fingerprints

I think is doubtful that a voter would ever check the TLS fingerprint. I personally have never checked the certificate/fingerprint myself. Even if they would check, it is not clear how this activity would contribute to increasing public confidence. To make voter's check the fingerprint, it must be made easier to locate the fingerprint information in the browser, which would entail improving the browser design.

2.3.3 Client application

I don't understand this question. A well-defined individual verifiability system must at least satisfy the following properties.

1. [Correctness] If the vote was recorded as cast, the information (aka return code) returned to voter must be verifiable.
2. [Accountability] The probability to claim successfully that a correctly recorded vote was incorrectly recorded must be negligible.
3. [Tamper-resistance] The probability of a malicious client application to fake a correct return code should be negligible.

A malicious client application will be able to break vote privacy, but it will not be able to break integrity undetected. The question that is asked here is for people to check the right client application being run — checking the return codes is the only way to check that this is the right app. It is important to make sure voters check the return codes and not the client application. To ensure that more voters check, see above.

2.3.4 Quantum-computing

Of course. Maybe, it is a bit premature to talk about the quantum apocalypse, but recently there has been great progress in quantum computing. Lots of progress during the past two/three years has been reported. The number of quantum bits are steadily increasing, while algorithms are being optimized for this new way of programming. There is no question that once quantum computers become available, there will be web interfaces to submit jobs, not the least to corner the market. There are many companies currently developing quantum computers, including Google, Honeywell, IBM etc. But these are only the ones we hear about. We don't know what other governmental organizations including other Nation States are doing about it. I personally think that we will see quantum computers factorization numbers into primes within the next ten years. This would break many of the crypto assumptions that are used in current Internet Voting systems.

One way to handle the quantum computing challenge is to think of the crypto-protocol in terms of the Universal Composability (UC) framework. Then components, that are no longer secure enough, can be replaced by quantum secure counterparts, without having to do the security proof again. The proofs are very difficult, however.

2.3.5 Voter platform security

MELANI appears to be a common-sense approach to application security and cyber hygiene. This is good. The mechanisms of individual verifiability, described in Section 2.3.3, guarantee integrity of the vote submitted. Vote privacy, however is not guaranteed by individual verifiability and can only be guaranteed by the software itself. Therefore, the insecure platform problem is a real problem. MELANI helps, but it is not perfect. In 2014, Halderman demonstrated how a third-party server that was incorrectly configured could be high-jacked by an attacker to install vote modifying code (or vote privacy breaking code) in the browser. On way to remedy the problem is to use code voting, where votes are not submitted in clear text, but voter-specific numbers, that cannot be directly linked to a candidate or party. It is needless to say, that code voting is more cumbersome and less usable. It has not been used in Internet Voting systems to date.

2.3.6 Coercion-resistance

Yes, absolutely. Studies in Estonia have shown that there is a correlation between votes by male and female voters in Internet Voting. Even if not intended, I think it is very likely that people do not cast their votes in secret. This is maybe a mild form of voter coercion, but it still is. The more frequently

Internet Voting systems are used, the clearer it will become to and adversary, that this can be an effective way to influence someone's vote. It might take a few elections before systematic misuse, but I believe that the argument is flawed that simply because voter coercion is *currently* not a problem, this does not mean that it won't be a problem in the future.

3 Independent examinations

3.1 Mandate

How to best organize an independent examination can be a very difficult questions. First, one has to decide on objective, a certification according to a standard, a commissioned review of requirements, design, or implementation, or a penetration test? Second one has consider what to do with the results of the reviews, for example, make them public, react on them and follow-up. Third, one has to decide who will do the actual work for the examination, for example a consult companies, or a group of experts with different competences, or even individual academics. Fourth, how many resources (for example, time, people, money) are left for implementing the possible recommendations. Fifth, the style of review, ranging from informal to formal.

In combination, these different dimensions define possible scopes for EMBs to consider. There is no clear answer to understand which scope fits best for Switzerland. From my observations related to other countries are the following: penetration testing is a popular form of examination of somewhat limited utility: insider threats, zero-day attacks, and general design flaws in the crypto-protocol are out of scope for such an examination. Certification is often considered the gold standard of quality assurance, but it has certain draw backs: the standard must be good enough to check a system against, it is expensive, and one usually does it only once in the life-time of a system. Certifications are often carried out by organizations that themselves have to be certified, and therefore only larger organizations offer this service. Underlying changes to the certified systems often require a recertification. Expert reviews are a very good way to learn about problems of a system, they go into the nitty gritty and often identify implicit assumptions that an EMB either has to accept or order changes and updates from the vendor. I believe it is important to include experts from the very beginning of the process, already while drafting requirements. Broken requirements will lead to a broken system. The expert team should review drafts of requirements and design documents in due time, because it is at this time when problems can still be fixed. Finally the source code should be reviewed – to simplify this task, which can be extremely resource intense — the requirements should define what are acceptable code drops and which aren't. In computer science, we have now developed frameworks that will allow the extraction of executable code from

formally verified models, a technique which will probably take a few more years to mature, but it is in essence here and all critical infrastructure system developments should consider using such frameworks. In the Swiss setting, this includes, for example, all components that are on the critical path to create public confidence, and those that need to be trusted to ensure vote privacy. Finally, there must be enough time allotted for quality assurance activities. Aim to start reviewing the source code at least one year before the election being held — to state the obvious, an election date is a fixed deadline that cannot be postponed.

Certification authorities should not be tasks with deriving the formal proofs, but they should check formal proofs others have done (note, that finding a proof is hard, checking it is easy). Certification authorities should, however, check carefully that the statement that is claimed to be proven, is correctly formulated. Otherwise one checks a proof of something that might be true, but unfortunately not what is needed.

3.2 Non-compliance

An EMB should never get into a situation, that an issue identified by a review, cannot be fixed (and vetted) in time for the election. Time management is absolutely critical here. There are no circumstances under which deficiencies in the software could be accepted without putting public confidence at risk.

3.3 Credibility

I believe the answer is yes. The credibility of the examination critically depends on who does it. If the consulting company that conducts the examination is involved in scandals, this does not bode well for strengthening public confidence. A consulting company that doesn't have the right expertise cannot deliver a credible quality review either. The right team for the job must consists of independent specialists for example, in cryptography, security proofs, operational security, and network security. By analogy: Not everyone can provide advice on Google's quantum computer: for recommendations to be credible the team better consists of trusted and trustworthy experts.

3.4 Scope and depth

There are no good standards for critical infrastructure systems that so directly affect public confidence. There are some, but they don't go really far

enough when be applied in the setting of Internet Voting, for example, the verifiable voting system guidelines (VVSG) by the US Election Assistance Commission (EAC) and the Council of Europe recommendation on E-Voting. There are many standards for securing ICT systems in general, for example, Common Criteria, or OWASP standard, but keep in mind, that provisions for cybersecurity do not imply trust. Therefore, although Internet Voting has been offered since 2004, there are still no widely accepted standards available. As they are not set, expert reviews are the next best choice.

By the way, a superficial software analysis, for example, only using code scanning tools, is not sufficient to make any final statements about the quality of a software system, as Pereira, Teague, et al. have shown in 2019 for the Swiss Post system.

3.5 Expiration date on examinations

The result of a penetration test is no longer meaningful from they time the test is completed. (Penetration tests talk about the past, and not about the future). A design review, perhaps even including formal methods and verification, is valid as long as the basic hardness assumptions underlying the security proof are not broken. Once they are, design reviews expire. Certifications expire more quickly, in particular when the underlying operating system is patched. Many US voting machines are certified, however, the underlying operating systems are not updated and security patches never applied in order to keep certification. I am not aware of any continuous certification model that would allow patching election technologies while keeping certification.

The examination should take place with every change to the system. A robust and mature system will need fewer examinations, but they still need to happen at least once before every election to determine whether the assumptions under which the system operates are still valid.

3.6 Independence of experts

I believe that openness and transparency is key to creating trust, and this means also to give independent experts willing to engage should the opportunity to be involved. Share the source code, invite the experts to review, and offer a hot-line to collect community comments, suggestions, and criticisms, evaluate them, and take further action if necessary. Keep in mind that non-mandated independent experts represent the public's interests.

3.7 Effects on authorization procedure

I don't know the details of the Confederation's authorization procedure, but I believe, that it is the Federal Chancellery's responsibility to conduct and organize all examinations. The cantons can suggest a voting system solution, and provide evidence (for example a formal proof in the symbolic or the computational model), but it is the Chancellery's prerogative to determine if it is acceptable. Therefore all examination activities should be organized on the federal level. By the way, constructing a security proof should not be part of the examination, it is part of the implementation.

4 Transparency and building of trust

4.1 Source code access

First things first. Transparency should be a central part of any electoral process. In some countries, for example, Germany, it is even enshrined in the constitution. Reverting from the principle of transparency in elections would be counter productive and wrong.[5] Therefore it is good to be transparent and it is good to publish the source code. But the source code shouldn't just be published as a snapshot a few days before the election or even worse as an out of date version of the source code actually used (as it happened in Norway in 2013). We argue that that the software should be published and maintained on an open platform, such as github or bitbucket, and all pull requests should be visible and observable to everyone.

Many EMBs don't want to release the source code because of security concerns. Why one should give the adversary inside knowledge about weaknesses in the source by publishing it? We always have to assume that a well-prepared adversary can get access to the source code, through whatever cyberattacks he or she chooses. Therefore, security by obscurity is not a good defense mechanism. We must always remember, that it is not the public release that makes software insecure, it is the software itself. Therefore the vendor will have to think about techniques to identify vulnerabilities in the source code and remove them. Secure software systems do not rely on keeping parts of the code secret, instead they rely on true randomness and extremely difficult to solve problems.

Vendors are of course against publishing their source code because it is not in their interest to release their intellectual property into the public domain: some might steal, modify, and resell their software. There is of course some truth to this. However, the situation is not as bleak. The vendor can initiate legal proceedings in the case of misuse. There are large and successful companies (for example Redhat) with interesting business models for building and selling with open-source software, that may serve as good examples for the voting industry.

[5] On these grounds, the German Supreme ruled in 2009 the election law from 2005 unconstitutional.

I am sure, that there are plenty of experts, who would be interested in identifying problems within the source code of an Internet Voting system. Invite them in and the system will become more and more secure with every pair of eyes inspecting it. To avoid an adversarial relationship, invite experts in and share every pull request.

I am not recommending that a the Internet Voting should be released under an open-source license. I am recommending that the source code should be made public in the interest of transparency.

No review is meaningful without proper design documentation. Before the implementation commences, ideally, the design documentation should be completed and reviewed. If problems are found in the design of a system while it is being implemented, it could be, hypothetically speaking, that the entire system needs to be redesigned and reimplemented from scratch. Analyzing the system documentation is therefore a necessary and effective quality control.

4.2 Scope/coverage of published documentation

The scope and coverage of the published documentation should be complete and cover the entire system. Every functionality should be described. The best way to think about design documentation is in form of contracts (or invariants): What are the input to a particular procedure, and what are the outputs. A very good example, I think, of a comprehensive design document is the one provided for the Geneva system.[6] Design documentation at this level of detail makes it easy to check if the source code implements the right thing, and it is also possible to evaluate if the mathematics adheres to the requirements.

4.3 Timing for publication

The system and its documentation should be continuously updated. Every change to the source code should be documented and recorded (pull requests). The authorized system should then be build from the sources before needed in the election.

[6] See `https://eprint.iacr.org/2017/325.pdf`

4.4 Coverage of requirements

The test reports are not sufficient (actually, testing should never be confused with a proof of correctness). One thing that often happens while testing an election system, which I believe is unwanted, is that during the test the system is used with a set of keys that are then also used for the real election. This is not good practice, as the private election key may have been reconstructed during testing, compromising vote privacy for the real election. I believe that a review of the design documents and how well they match the requirements should be included with the publication of the design documents, especially, for the purpose of authorization.

4.5 Public reaction

Although all cantons are responsible for providing a secure voting solution, it is the Federal Chancellery who should responsible for deeming the respective voting solution secure enough. My suggestion would be to create a contact point (hot-line) on the level of the Chancellery that receives of comments regarding to the voting system. If the autonomy of the cantons allows it, the Chancellery should then also be responsible for evaluating the comments, and take appropriate action, in the worst case, deauthorizing the use of a particular Internet Voting system. Most importantly, the Chancellery must be able to provide convincing answers to people crying wolf that the system doesn't work. This means that the Chancellery should also be able to defend against unfounded accusations. Once the Chancellery has determined the right course of action, it will take next steps and involve the vendor, police, or academics.

4.6 Publication of security breaches

Yes, it should. Only transparency can create trust. The best solution is to publish all the source code, pull requests etc. from one of the open platforms, such as github, bitbucket etc. Github integrates now code scanning tools that can help identify patterns of common security problem.

4.7 Penetration test

In principle the public penetration test was and is a good idea. So absolutely, the security of a system will benefit from a PIT. One idea is that the test should not be arbitrarily limited in scope. During the PIT, certain forms of attacks were ruled out, and one had to sign not conduct these. I believe, gain-

ing experience with Denial of Service attacks or Social Engineering attacks can only be useful for the Chancellery. But as already mentioned above, a PIT cannot replace a thorough security analysis. For example, if the server runs a protocol that is secure today, it may no longer be secure tomorrow. A bug bounty program could be useful, maybe it would be worth considering running it all the time, and not be time limited to a one month event? For example, there could be public testing side that runs all the time. It could also be possible to turn the PIT into a “capture the flag” (CTF) contest, a competition, where the best will try to break into a system. And if there is a reward, even better. All bugs and vulnerabilities identified could then go directly to the Chancellery who then will, for example in conjunction with experts, determine the best course of action. Perhaps it is good to remember at this point that there is no secure system. All systems are hackable. The reason to have a PIT, is not to make the system secure, or demonstrate that the vendor can secure it system appropriately, it is simply there to increase the security of the system incrementally. Short of program verification, I am not aware of any other alternatives.

4.8 Low-scale use of Internet Voting

By limiting the electorate, the Chancellery signals an understanding of the concerns related to public trust. Also using the words individual verifiability and universal verifiability in the legal framework is pretty unique among EMBs around the world. But in my opinion, this is not enough.

I am convinced, that sustainable public trust can only be built through a clear and accepted definition of evidence and procedures for auditing this evidence. This should be a part of federal regulation. As I already argued above: Security does not imply trust, and trust does not imply security. Both are very different concepts. Therefore, I don’t think that the proposed low-scale use of internet voting alone would promote trust.

4.9 Credible process of tallying and verifying

This is absolutely the correct question to ask. Again, define evidence and auditing. *Evidence* should refer to the encrypted votes, the public signing keys, the proofs of knowledge produced by a mix-net (for universal verifiability), evidence that voters checked the correctness of their votes recorded as cast, proofs of correct decryption. It must be clear from this definition that the evidence is immutable, and that collectively, all pieces of evidence form the picture of a credible election. Evidence must also be vote privacy preserving. *Auditing* This is the process for checking the evidence. It should be

evident that the auditing (or verification) process is completely independent from the counting process. Ideally for every step, there will be evidence witnessing correct execution, including individual verifiability, cleansing, mixing and decryption.

Some products rely on an independent auditor to rerun processes to deduce that the results are the same. This is also a possibility, but inherently weaker: There is no evidence that the auditor uses an independent hardware software system. If not, it is not an audit and has only limited utility.

The *independence* of the counting process and the auditing process are absolutely critical to convince voters to trust, and defend the system against voters crying wolf.

In summary, every canton must define evidence and auditing. Both concept should be defined in terms that are completely independent of the particular voting system to be used, and ideally checkers for both should be created, before the voting system is procured.

4.10 Publication of electronic voting share and popular vote results

Only evidence should be published. The evidence can be used to hold the system and the final election result accountable, and at the same time it can be published because it is vote-privacy preserving. I would recommend against publishing vote shares, because most of the votes are encrypted in a way that may be considered insecure in 30 years. Ideally, the evidence should yield everlasting privacy, but how exactly a scheme could look like is still under ongoing research. There are no other downsides to publishing evidence.

4.11 Additional transparency measures

Everything should be made transparent. There cannot be trust if there is no transparency. Even meetings/minutes about the voting system should be made publically accessible. By hiding things, scoping trials, excluding experts, etc, an EMB risks to weaken public confidence in the electoral process.

4.12 Statistical plausibility checks

In 2018, I co-authored a Council of Europe publication, which discussed the identification of electoral irregularities by statistical methods.[7] The main findings were, the statistical methods can at best suggest where to look for election fraud and electoral problems, but it can never be used as evidence to identify election fraud and electoral problems. The same finding holds here as well. It is the evidence generated during an election that needs to be inspected. With the right auditing framework this will be automatically done, rendering statistical plausibility checks unnecessary.

[7] https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2018)009-e

5 Collaboration with science and involvement of the public

5.1 Conditions to ensure that independent experts participate

To understand academic experts, one has to understand what drives them: In one part, it is the pursuit of knowledge, in other to relay information back to the actors directly effected, in this case EMBs. Some of the scientists see themselves as activists: Just as when the atomic bomb was developed when some physicists were in opposition for it to be used, some academics warn of the use of Internet Voting technologies. To engage independent experts, it is often enough to make all artifacts available for scrutiny, to offer a trustworthy channel of communication that gives the experts the confidence that their concerns will be heard and reacted upon. Academics love to write papers about their findings, and this should be possible and most academics subscribe to responsible disclosure rules. It is actually quite important that findings are documented for the public record, and also for other cantons/-countries, to learn about common problems. As the PIT has shown, only limited promotion of the event excited a huge group of people. Of course, the Chancellery will have to be prepared to respond to any input, and live with the consequences. (Allow for enough time!) The past has shown that the Switzerland has the ability to take serious and long-reaching remedial actions after serious vulnerabilities in the Swiss Post system have been identified.

There is a difference between research and consulting. An researcher is driven by the pursuit of knowledge and personal curiosity, and intends to be free and unconstrained in terms of the research questions asked, the methodology used, the time it will take, and how to publish the final results. In this setting, an academic will not want to sign a non-disclosure agreement or commit to a particular time table. In contrast, a consultant is ready to sign non-disclosure agreement, commit to time tables etc., but also wants to be paid for services rendered. Participation in examination always requires a consultant, ideally an academic with deep knowledge about the field, who is willing to serve as a consultant.

5.2 Participation in the political debate?

I don't think there are any conditions to be met. Most scientists in the role of a researcher would be willing to participate in the political debate if asked, arguing a point either for or against. Consultants are usually excluded from political debate by the contracts that they have signed.

5.3 Dissemination of Internet Voting facts

I don't quite get this question. There are many scientists that will argue with determination against the use of Internet Voting. They will stick to the facts as they view them. There is no way to present facts in any other way that would make them more palatable to the scientists. Facts are facts, and alternative facts don't exist. To convince a scientist, the Chancellery will have to define precisely what evidence is, argue why the evidence satisfies all of the defining properties, and that the auditing process is well-defined and independent from the counting process. It would also have to make explicit all assumptions. It would be sufficient for the Chancellery to compose a document, the internet voting rationale, and publish it on github, and invite the community to comment (which they will do, I am quite sure about that).

5.4 Promotion of trust through dissemination of information

As mentioned above, for integrity, the information must include what is evidence and how is the evidence audited, independently from any vendor's technology or product. For availability and vote privacy, an explanation of the examinations conducted, their results, the rebuttals, and the fixes, including an open invitation to download the source code and inspect it. The details of the presentation for integrity has to be at a level that even the layman understands.

5.5 Reasonable measures to involve representatives from science and public

Representatives from science will speak their mind, and they will most likely say so, if they do not find that an Internet Voting system is trustworthy. The Chancellery should not rely on scientists to build public confidence, it should be the way the system is constructed that makes the system worthy of trust. The best way to include the public and other stakeholders is complete transparency. I don't believe that it matters, who organizes the event to involve science and public. I think, that it is very important that the public is invited

to the auditing event of the evidence, or invited to audit the evidence themselves if possible. Don't forget, the goal is not to build confidence in a few participants of a hackathon, but to build confidence among *all* voters. This is a long process that may have to be sustained for decades.

It is also important to consider other events that are happening in the world. Election security and the difficulty to build secure Internet Voting systems is most likely a hot topic, also in the Swiss media, in the time leading up to the 2020 US presidential election.

6 Risk management and action plan

Organizations with limited budgets use risk analysis to determine how best invest resources to strengthen the security. Elections are slightly different. If a Internet Voting system exposes a vulnerability, then it should always be expected that the vulnerability will eventually exploited. This means, that the number of residual assumptions for an Internet Voting system to work reliably even in an adversarial environment which is controlled by a foreign Nation State, or an EMB that was infiltrated by foreign agents, should be kept as small as possible. The Internet Voting system should be designed in such a way, that the security of the result and the privacy of the vote is independent of any underlying technology, servers, operating etc.

6.1 Continuous risk assessment

A continuous risk analysis should evaluate, if the assumptions still hold that are necessary for the Internet Voting system to work correctly. It should be organized before each election, long enough in advance, that if some assumptions are no longer valid, remedial steps can be taken.

6.2 Benefits and downsides of publishing risk assessments

The benefits are clearly that the Chancellery is attentive and therefore trustworthy. In the electoral domain, there are no benefits of being secret about those things. The adversary knows anyway. Therefore it is always a good idea publish risk assessments. If for example, the risk assessment says that because of a quantum computer vote privacy can no longer be guaranteed, it is probably better not to use the system then to hide the fact that the people responsible for Internet Voting knew.

6.3 Supply chain risks

I believe that a separation of duties is the first step to handle supply chain risks. The EMB should be responsible for building and operating the technology to audit evidence. A vendor can be chosen to design and develop the technology to run the election. To become more resilient towards vote privacy, it could be an idea to modularize the Internet Voting system in such a way that there are different implementations for different components.

There is also a trade-off between who should own and run the hardware. Out-sourcing the running of the infrastructure to a third party service provider, such as Amazon AWS would bring certain benefits, namely an infrastructure that is redundant, engineered for availability and security, etc. but if things go wrong, the cantons might not have any access to data logs, etc. This could prove extremely problematic. On the other side, rebuilding infrastructure from scratch is very costly and requires many resources. A good trade-off is to reuse national datacenters to run the application, and then inherit the supply-chain risks from them. Some vendors are planning to offer voting as a service, but this comes at the price that one has to accept the supply-chain risks from the vendor, and it is unclear, if the infrastructure that they use lives up to the EMB's expectation.

I would advise against allowing the system provider to use contractors. To minimize supply chain problems, allow for enough time to conduct examinations on the completed system, and have a backup plan ready. The source code should be made public, and even if the vendor goes out of business or no longer wants to maintain the code, the EMB should have the capacity to take over maintenance of the code base. In the worst case when there are supply-chain problems, do not offer Internet Voting as an alternative voting channel.

6.4 Action plan measures

The criteria for prioritizing action plan measures should be ordered in such a way to minimize the negative effects on public confidence 1) scope: What is effected, integrity, vote privacy, availability, 2) urgency: because during a running election, time is of the essence, and 3) feasibility: can it actually be fixed, and what are the remedial actions to be taken.

6.5 Alignment of risk analysis with standard methodology

I am not an expert in risk-assessment and alignment with standard methodologies. I would however consult international recommendations for risk analysis in critical infrastructure protection.[8][9]

[8] See `https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf`

[9] See `https://fas.org/sgp/crs/homesec/RL32561.pdf`

6.6 Staffing of risk assessment activities

In general, risk assessment requires a deep understanding of existing infrastructure for handling risks, including cyber, military, natural catastrophes, etc. In the US, sector specific information Information Sharing and Analysis Center (ISACs). For elections, since 2017 deemed critical infrastructure, an Election Infrastructure ISAC has been created, and to my knowledge this works very well. ISACs don't really work with scientists, but I believe that academia should be represented in an ISAC, to anticipate future challenges and to research possible solutions to handle current challenges. Hence I would follow a construction similar to the the EI-ISAC,[10] but include academics as well.

6.7 Risk assessments requiring inside knowledge

See my answer to the question above. An Swiss EI-ISAC composed out of the right people should be able to define and respond to risks effectively and credibly.

6.8 Risk analysis on the canton level

Again, a Swiss EI-ISAC should also represent the cantons. In the EI-ISAC forum, the risks should be discussed freely, and it is critical, that if Switzerland should be the victim of a cyberattack, that the risks for each canton are considered in one forum. I would recommend to leave defining the modalities to the EI-ISAC.

6.9 Octave Allegro methodology

It is not clear to me, which of the risk assessment frameworks is best suited here. Besides Octave Allegro, there are also other options, for example, the FAIR framework. Octave Allegro appears to aim to be light weight and easy to use. It treats technology as well as people, which seems to be a good fit for assessing the risks of using an Internet Voting system. However, I would leave a final decision of which framework to use to the Swiss EI-ISAC who will actually use it in practice.

[10] See `https://www.cisecurity.org/ei-isac/`

7 Crisis management and incident response

7.1 Key elements

I am not an expert in crisis management, but it is central to have a team responsible for dealing with the crisis. (This could also be a part of the proposed Swiss EI-ISAC). The roles of the team and their respective responsibilities must be clearly identified. Their whereabouts must be known and they should be easy to reach. The crisis management team must be prepared for the things that could go wrong, and they should have a solid communication plan in place. For each election risks and crisis management options should be reevaluated, and an effective incident action plan should be available.

An important part of the crisis management tasks is to identify when a problem has occurred as early as possible. Sometimes it is difficult to do. The randomness bug in the Norway 2013 voting client was only detected by accident. Nobody in the EMB noticed that the 2010 Washington DC Internet Voting systems was under complete control of hackers until it was revealed to them, and the possible code injection vulnerability in New South Wales 2014 election was detected only while the election was in progress. Early detection is critical for crisis management planning. There should be direct communication lines established between the multiple actors and the crisis management team.

7.2 Events and thresholds

Here a few events and thresholds.

1. Incoming information on the Internet Voting hot-line. Every claim should be analyzed.
2. Notification by a secret service or cybersecurity firm on unusual attacks
3. Suspicious activities reported in log files.
4. Suspicious behavior of employees at the vender/EMB.
5. Tripwire (a software system that reports changes in the underlying file system).

6. Unauthorized access to a server room.

7.3 People involved in crisis management

There should be a dedicated office dealing with crisis management. The head of the office is the main contact point for the EMB. There should be a technical contact, who knows the system inside out, there should be a communications expert to interact with media, and their should be a national voting expert, who can frame and explain a voter's reactions. Then their should be liaisons people, for example to the Swiss telecommunication service, GovCert, and the cybersecurity office of the government/military, etc.

One of the challenges when processing claims from the hot-line is to decide quickly and reliably, if a claim is valid or not. In Norway 2011, many of the voters received the wrong return codes, a good crisis management team should be able to pinpoint the problem, initiate remedial actions, and communicate them clearly and effectively to the public.

7.4 Communication

For external communication, it is recommended to employ a communication expert, who can explain the problems that occurred in a greater political context. A prompt official response addressing public concerns is critical for building public confidence in the election, even if things go wrong. For internal communication, it might be a good idea to have the crisis management team assembled while the election is ongoing.

7.5 Existing structures

Yes, it is important that all organizations that can contribute to a swift resolve of a crisis situation meet, or even better work in one room. See my answer to 7.3. Governments often have intrusion detection systems integrated into the national network. The US, for example, uses a Suricata based Albert sensor system [11] If such an infrastructure exists, the crisis management should be able to take advantage of it.

7.6 Incident investigation

As mentioned above, public confidence is created through auditing. If the audit fails, then, incident investigation will become an important part of the

[11] See `https://www.cisecurity.org/services/albert-network-monitoring/`

election. In this situation, incident investigation should be left to those how have the best background to resolve the incident. I assume, that the police will lead such an investigation, especially, when the incident that occurred is in violation with national law. Experts will be pulled into the investigation on a by need basis. However, the audit will tell us, if the election result is correct. I suspect that one possible outcome of a failed audit is, that the election will have to be annulled and repeated.

7.7 Digital forensics and incident response

The main requirement is that all artifacts that can go into an incident investigation and digital forensics, are immutable. This means that all log files should be cryptographically secured, for example using Merkle trees. If log files are not cryptographically secure, the forensics will be much more difficult, and the conclusions likely not as trustworthy. If the servers are located out of the jurisdictions of the Swiss police it may be very difficult to collect the information necessary to investigate an incident. Such a situation has arisen in Kenya, 2018, which prompted the Supreme Court to call a fresh election.[12]

7.8 Prosecution

Investigation and prosecution rely on evidence. Define what evidence means, and you will be able to investigate and prosecute. Ensure that all log files are cryptographically secured and that they are accessible in the case of a dispute or incident. Require that each file generated, ballot boxes, log files etc, are digitally signed by a person responsible for it (this requires that Switzerland has access to a national ID infrastructure).

7.9 Validation of an election result in the case of an incident

If auditing the evidence succeeds, then the result is valid. If the audit does not succeed, then an incident investigation becomes necessary, which, in the worst case, will lead to an annulment of the election. A failed audit, can be due to mistakes in the key generation procedure, a platform running malware, programming errors, cyberattacks, etc. etc. There are many reasons. If an incident occurs, then it is really important that the reason of the failure/-for the incident is correctly understood, and then a determination has to be made on how to respond. Ideally, the VEIeS should state exactly what has

[12] See `https://www.nytimes.com/2017/09/01/world/africa/kenya-election-kenyatta-odinga.html`

to happen in each case. This is not just a technical question, but also a political one. If one person complains about a failed return code check, does this mean, that only one ballot was incorrectly recorded, or does it mean that there were many, but most of the voters didn't check their return code in the first place? I would recommend to create a catalogue of possible auditing failures, and possible incident reports, and then determine for each the appropriate course of action.

The advantage of such a catalogue is that the decision on how to react is already agreed upon before it is taken. One therefore circumvent a paralyzed government that relies on the courts to determine the election result in the case of an incident.

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Uwe	**Last name**	Serdült
Organization	Zentrum für Demokratie Aarau (ZDA) an der Universität Zürich		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.
Click or press here to enter text.	

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
Unlikely if crypto-protocols are properly implemented. State of the art technology is sufficient. In the first place a way to guarantee proper implementation of the crypto building-blocks needs to be found. This is one of the take home messages from the Swiss Post evoting system PIT (correction of individual verifiability was not properly implemented). (my opinion)	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
See above.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
Not in a position to comment	
2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are

	distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
As a general principle, control components from different providers would be preferable, however, the complexity of the software is such that currently one has to and can compromise on such a feature. (my opinion)	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
Without externally developed verifiers the work of the auditors will not be taken for granted, will not be trusted by the public. (my opinion)	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
Not in a position to comment.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
Mid-term the use of a different tool providing a verifiability service could also be used for other applications, not only for internet voting. People are getting used to such a third device or app in principle, in some domains it is becoming the norm. It could even be expected these days. (my opinion)	

Votes posted on a public bulleting board is a feature I would very much welcome. They are more « tangible » for lay people and allow to open the black box of internet voting in general and verifiability in particular a bit. Long-term privacy issues in the Swiss political culture should not be the main concern. In case there was a technology allowing to decrypt all voting codes we would live in a completely different world hard to imagine. Many other things would also change completely. It does not make much sense to limit ourselves today by technology which might or might not be available in the long run. (my opinion)	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
A sub-group of a yet to establish extra-parliamentary expert committee could be responsible for such a task and publicly declare what was checked and that according to these checks to their best knowledge the software was properly deployed. Similar to the statement a revisor is reading out in annual meetings of voluntary associations (Vereinsversammlung) with subsequent publication thereof. (my opinion)	

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
Not in a position to answer.	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
Not in a position to answer.	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
Not in a position to answer.	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in

	banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
Not in a position to answer.	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
I can not answer the questions directly but would like to add here that we should aim at fully decentralized internet voting systems which can be managed in such a user friendly way that they can be operated by local authorities themselves. This might seem far fetched but researchers should aim for such a system especially for Switzerland where trust in voting procedures is generated on the local level. **In addition to being decentralized future internet voting system could include trust-building features such as a re-materialization of the vote. This research strand is slowly developing but still embryonic. The question is what the analogy to a paper trail from an e-voting machine can be for internet voting.** **Decentralization and re-materialization seem far fetched now. However, I think with universal verifiability only the general public will not be able to build up enough trust in internet voting and a large part will shun away from it.** **The advantage of internet voting vis-à-vis postal voting is in my view not so much a gain in security but rather a more transparent (assuming universal verifiability with bulletin boards) and trustworthy tallying process. The user knows a vote arrived and will be counted correctly which is completely lacking for postal or ballot box voting.** **I am mentioning these points here because out of the box thinking is necessary to make progress and because such features (as much decentralisation as possible and re-materialisation) make potential attacks much more costly.** **(my opinions)**	

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or

	dis-played incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
See point 2.2.5 : any measure leading to a by product of the vote which can be experienced in a more natural way such as bulletin boards, paper trail, 3D-printed objects stored in a blockchain etc. would be an incentive for the general public to go and check for the return-codes. Human-Computer-Interaction research by Karola Marky partly supports such arguments. (partly research based)	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
The percentage of people checking anything during a vote will always still fairly low. Besides kindly asking them to check there is not much else one can do (and one does not need to spend too much energy on that). (my opinion)	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
See 2.3.2	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
Not in a position to comment	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
Not in a position to comment	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
Indeed, vote-buying or vote-selling or coercion do not seem to be a major issue in Switzerland. However, this is just an assumption we generally tend to make in Switzerland.	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

There are no studies to my knowledge providing evidence for such behavior in Switzerland. Implementing such studies is of course not easy. However, widows could be asked in face-to-face interviews whether family voting was practiced when their husbands were still alive. Forensic studies looking into finger prints on voting cards and ballots would be another option (I think there are studies but not sure).

Lately, I am having some doubts whether family voting in Switzerland not eventually underestimated. Especially for the older generation (an assumption again) it could have been a problem.

Coming back to the actual question : If there was coercion in Switzerland it would actually rather decrease with internet voting because the electronic channel does leave more traces than a postal vote (which is not good for the coercer) and is more time as well as location independent (which is good for the coerced).

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
Not really in a position to comment but we need to be careful not to overburden the whole process. Experts need to define which components one absolutely needs to certify, the key components to internet voting. (my opinion)	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
Not in a position to comment. Explain and declare in a very clear and transparent way what can be checkend and what not. (my opinion)	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).

In my view the necessary examinations should be defined by the extra-parliamentary expert committee yet to establish. Practically, this body would – within the legal framework – be responsible for the governance of certain elements of the whole internet voting process in Switzerland. (my opinion)	
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
Not in a position to answer.	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
Mandates for examinations would be given by the extra-parliamentary expert committee on a needs bases but at least for every update of existing internet voting systems. (my opinion)	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
Independent experts would most probably only participate in such an endeavour if they are free to publish results (as the Swiss Post PIT has shown). (my opinion)	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
In case of disagreement – equivalent to other domains – the Federal Council within its competencies can come to a final decision. (my opinion)	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
All of the questions here are good questions. However, they should be tackled in a bottom-up approach, involving an open dialogue among all stake-holders. In addition, all elements mentioned further can change rather quickly over time. I would therefore suggest to create a permanent body in the form of an extra-parliamentary committee. The new body should comprise diverse expertise and once or twice a year hold open meetings inviting constructive criticism from academics and civil society activists rathere against internet voting. The body would also have certain competencies regarding certification, audits etc. (my opinion)	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
The new body can develop such guidelines and a needs basis.	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
See above	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
See above	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
Discussion mainly within the new body.	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
Establishment of guidelines by the new body.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
The Swiss Post PIT proved to be a very effective way to check security issues. The quarrels about publication of the results are in fact a non-issue and can be resolved. (my opinion)	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low

	fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
Limitation in the form of user rate restrictions do not make much sense and were de facto never a problem due to the low scale actual use of internet voting. Internet voting use will go up slowly over time such as in Estonia once the channel is available in a stable way. In Estonia it also took a considerable amount of time to reach user rates of 45%. (partly fact based)	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
As a part of decentralization and first on a voluntary basis members of already existing local oversight bodies, the election board members in municipalities, could be trained to perform some of the verification tasks. The role of local election board members needs to be re-assessed anyway. Hence, long term internet voting should even be possible to be performed on the local level (see above). (my opinion)	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
Publication of such data should be standard. It is needed as a basis for public debate. (my opinion)	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)
Up to the newly created body and discussion therein with an extended circle of experts and stakeholders, again on a needs basis. (my opinion).	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
Academics with a sound mathematical or statistical background can perform electoral forensic studies. It should be possible to find an academic in Switzerland interested in the topic. (my opinion)	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
Click or press here to enter text.	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
For scientists it is more important to do research, publish, teach and get cited by others. Participating in the political debate is not very gratifying and a distraction from their actual job although it can indirectly help to achieve their primary goals. Some of the best academics do therefore not want to participate actively in a political debate. In the time of anonymous social media they quite frequently also get attacked or are being ridiculed. They are more likely to contribute if they can leave communication and political debate to a body such as the suggested extra-parliamentary committee. The new body gives them an oppurtinty to be heard but not having to get involved into political matters. (my opinion)	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
This can be left to the academics. Academics who are members of the new extra-parliamentary committee can play a supportive role by involving them in an open dialogue. (my opinion)	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
Current information including video material is already existant and sufficient. More of the same is not going to make much of a difference. (my opinion)	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
Such events would again be organized by an extra-parliamentary committee. They are important but one can not expect them to directly generate trust. For a topic such as internet voting it is very difficult to generate trust among the general public (and scientists the like). Even with a lot and perfectly acurate information it is easy to cast a shadow of doubt, bring in conspiracy theories, or come up with recent examples such as the case of the company Crypto who shared their secrets with Western secret services and somehow link that to internet voting. There is not way to avoid such	

behavior to some extent. Not too much energy needs to go into fighting that. (my opinion)

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
Periodical statements by the newly created body and MELANI for example.	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
Click or press here to enter text.	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
Not in a position to comment.	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
Not in a position to comment.	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
Not in a position to comment.	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
Implement that in working group of the newly created body.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here.

	How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?
Not in a position to comment.	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
Not in a position to comment.	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
Not in a position to comment.	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
Under the current legal regime cantonal authorities are directly in charge and need to take responsibility internally and externally. It is crucial to provide information on how many votes potentially were affected by irregularities. (my opinion)	
7.2	What are the right events and thresholds for an activation?
All irregularities should be communicated.	
7.3	Who should be involved in crisis management, with which role?
Only one body should communicate externally.	
7.4	How should the communication be organised (internally and externally)?
The cantonal authority in charge needs to inform the public as well as higher authorities such as the Federal Chancellery. (my opinion)	

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
Not in a position to comment.	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
Not in a position to comment.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
Not in a position to comment.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
Not in a position to comment.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
Not in a position to comment.	

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Matthias	**Last name**	Stürmer
Organization	Click or press here to enter text.		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	be improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.

In my view trust in the digital world builds upon «ubiquitous transparency». Just publishing the source code of an e-voting system on the Internet is not enough. It is necessary that all involved stakeholders are knowledgeable about the inner workings of the software. The source code is a necessary but not a sufficient precondition for this. It is also necessary that experienced software developers have time to work on and continously improve the details of the source code. Therefore there needs to be a business model for IT providers to have highly skilled software developers working permanently with the source code.

Thus in the ideal world there exists a single, standardized, user-friendly but highly secured and transparent e-voting system. Its source code is published on the Internet without any restrictions (e.g. no requirement to register and accept certain conditions) under the terms of an open source license. Technical experts and computer scientists continuously review new releases of the code and publicly claim it is secure and reliable. There exists a community of government agencies, IT companies and civic hackers that know the source code and the processes of voting.

The federal government was paying the initial software development because the cantons are not capable of handling such a large and complex software development project. The procurement followed a multi-vendor tendering strategy. Thus the knowhow about the source code resides with several national and international IT companies that continue providing services for the Swiss open source e-voting system. Many employees of these IT providers know the source code very well because they continuously adapt it for their customers - the federal government, the cantons and the municipalities.

The open source of the e-voting system is controlled by a non-profit organization (association or foundation) that is in charge of maintaining the open source software as a sustainable digital artifact. The non-profit organization is in charge of controlling the development process, the knowledge diffusion, events, and communications. The non-profit organization’s ecosystem of governments, IT companies and civil society follows the principles of digital sustainable community regarding software licensing, tacit knowledge distribution, participation, governance, and distributed funding (see Stuermer, Abu-Tayeh and Myrach 2017 «Digital sustainability: basic conditions for sustainable digital artifacts and their ecosystems» https://link.springer.com/article/10.1007/s11625-016-0412-2).

Journalists are informed well by the federal government, by the cantons and by scientists about the technology, the cryptographic algorithms and the e-voting workflows. The journalists are able to follow the process of producing voting material, sending the letters to voters, entering the votes etc. thus they are able to understand every single step. As a consequence the media reports positively and technically competent about e-voting. Therefore the citizens trust the e-voting system.

After each votation all voters are able to verify their personal vote within a simple list of codes. Every citizen is able to download this list and check with a regular spreadsheet soft-ware the correctness of all votations. Thus it is easy to understand for all opinion-leaders among the voters how the process works and that all votes are counted correctly.

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening.

With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail
- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	

2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?
I believe this is a very important issue. Although I'm not a crypto nor security specialist I believe there could be a simple solution to this challenge: A board of trusted and independent academics or also a highly skilled IT audit company could be assigned to verify that the installed system on production-sites is indeed being built from the same source code of the software being published openly. Technically I assume this could be done by comparing some hash codes of the binary files of the software.	

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be

met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
I've read all the 24 listed threats. I don't see any additional threats. However, I have to repeat that I'm not a crypote nor security specialist.	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
As I'm not a crypto nor security specialist I'd rely on the professional opinion of experts regarding best practices in this area.	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
With my current knowledge it is hard to say for me if e-voting is potentially more or less secure than voting by postal mail. Today I believe the most secure way of voting is personal appearance at the voting booth. However, this is also the channel that has to be replaced with a more convenient way to vote. I personally believe postal mail cannot be missused large-scale without being noticed. Therefore e-voting could be considered as less secure since it has the potential threat of large-scale attacks. Ne-	

vertheless, if all the security measures work as intended I'd also trust e-voting. However, to my knowledge also missuse of e-voting on a small-scale is possible in case the envelope with the codes is being stolen or copied for buying a vote. Therefore as long as e-voting is based on codes sent by postal mail I don't think it is more secure than postal voting. In case one day e-voting is possible with some E-ID then it could become more secure than postal voting since missuse becomes more difficult.

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or dis-played incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
Today it is probably not yet possible to expect the average e-voting citizen using these technical possibilities. However, if one day e-voting is available to all Swiss voters then I assume that people are made aware of their verification possibilities by media, political parties, colleagues etc. Possible measures to increase these activities include short promotional and learning videos, online campaigns, media informations, press releases about the number of people checking vs. not checking their return-codes etc.	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
Sorry I can't answer this question.	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
I'm not an expert in these type of questions but I assume this can be addressed by similar measures as mentioned in question 2.3.1: public security awareness campaignes, informing journalists that they report about the security checks.	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the

	vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
As I'm not an expert in crypto nor in quantum-computing I'm not able to answer this questions.	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
I think the more companies and governments report about hacking attacks and that the threat is real, the more people also are aware of personal security issues. Nevertheless security is always an arms race, therefore there won't be a static solution to this problem.	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
Yes I think this issue should be addressed once again when introducing e-voting. I see a higher likelihood of this threat when people are using e-voting since it seems to be more anonymous.	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
Frankly I'm not really convinced of the effect of standardized certifications and security audits. They have a positive influence in a way that IT teams are aware that their system is being audited. However, the standard tests measure only the obvious things. I think public intrusion tests based on the source code and the infrastructure	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

are really hardening the systems. Thus such a test that the Swiss Post performed last year should have been conducted much earlier.	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
I don't know the technical details but in my perception there is zero tolerance of the public regarding any security issues related to e-voting. Although some risks are somewhat hypothetical it still matters to the public perception if critics point out flaws or possible threats which have not yet been addressed by the technicians or administrators.	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).
Absolutely. The best security experts are in my opinion on the one side from academia since they have no interests. On the other side boutique security companies also have very skilled experts that can audit certain components. I wouldn't assign Big-Four companies since price-for-money is usually not in an ideal relationship.	
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
Sorry I can't answer this question as I'm not a security expert.	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
Sorry I can't answer this question as I'm not a security expert.	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
Independent software and security experts should be involved as much as possible. E.g. although the Pirate Party or the Chaos Computer Club are strong critics of e-voting systems occasionally there are knowledgeable and constructive people among them. I'd suggest to inform them individually and try to take their feedback seriously showing improvements. I'd follow the saying «Keep your friends close and your enemies closer».	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
I don't understand this question.	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
The PIT is a key element of trust and transparency issues. The terms and conditions should not restrict the PIT in any way since every limitation reduces the credibility of the PIT. Money is a good incentiviser as it also compensates the time experts spend for analyzing the code. Intellectual property concerns are not problem anymore if the source code is published below an open source license. In my opinion an e-voting system is an important digital public infrastructure that everyone should have the right to investigate and improve. Frankly I can't think of a better case where governments together with private companies can build an open, solid and trusted digital infrastructure.	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
Everything should be made transparent in order not to raise concerns about hidden components.	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
Before a new software release goes into production I suggest a PIT and other ways making the public aware of the new e-voting version.	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
I believe the current level is sufficient if the issues raised in 4.1 are addressed.	
4.5	Under what conditions should public reactions be discussed?

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

	1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
For each major release I suggest holding a press conference and then a technical discussion with independent experts.	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
I suggest using standard state-of-the-art open source development tools such as GitLab. Thus all fixes are made transparent and open for comments.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
I'm not an expert in these issues but in general I think there should be as few restrictions as possible. It lowers the credibility of a PIT if several threats are not allowed to be addressed.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
I guess the low-scale use of e-voting decreases the risk of strongly falsifying votations and elections. But personally I think it doesn't help building trust in e-voting since obviously not even the Federal Council believes that the system is secure. Thus it doesn't seem to be a coherent approach. In addition many times votations and elections are very tight votes. Thus even if only a few percentages of votations are wrong the results may be flipped.	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
This is a very tricky question. I've not enough experience in such kind of processes thus I can't provide a qualified response. In general I think the more transparent everything is handled, the more trust is being created.	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
I don't see any problem publishing as much details about the votations as possible as long privacy is not affected.	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)

In my opinion the best thing are independent, trusted experts that have been involved in all the processes and thus can confirm that everything went well – or point out areas of improvement.	
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
The plausibilty checks should be easy to understand and reproduce. Publishing votation data as open data (e.g. on the Open Government Data platform opendata.swiss) could help making the process more transparent and thus more credible. Applying anonymization techniques such as k-anonymity is important to prevent privacy breaches.	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
Academia usually needs to things in order to be involved: First, results of investigations and tests need to be of scientific value (publishable in peer-reviewed journals) thus there must not be any restrictions in publishing also inconvenient issues. Second, academia needs longterm funding for really getting involved into the technical depths. In the case of e-voting I think interdisciplinary research must be conducted: There need to computer science experts (security, crypto, software engineering etc.), information systems experts (organizational issues, architecture etc.), business administration (sustainable business models etc.), political science, communications science, public management experts etc.	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?

Scientists have to be experts in a topic in order to make public statements. Thus it need time and published research before scientists are willing to participate in political debates. Also they need to understand the basic processes of other fields involved. E.g. computer scientists would want to understand the key political processes and structures involved in votations.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
Votations and e-voting sound quite simple but they are not. Therefore there exists a lot of semi-knowledge – even I don't know all the details altough I've been involved in politics for many years. Therefore I'd suggest to inform scientists the same way as to address the public: With easily understandable information, professional video clips, news reports etc. Scientists usually are very strong in their field of research but know only little outside their focus areas. However, they are always very interested to learn new things, otherwise they would not be in academia. Therefore they are open to learn about political processes, votation rules etc.	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
As with the representatives from science also the public needs to know the key terminology. I wouldn't limit the level of detail but allow drill-down for anyone interested to really understand all the foundations.	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
Both technical and non-technical events seem important to me. I've made very good experiences with hackathons where domain experts/data owners bring their data and a challenge, programmers solve these challenges and designers create an attractive user interface and visualizations for the end users. In these kind of maker-events also scientists feel welcome.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
First of all the generic risks (section 2) and their attack vectors need to be explicitly named, evaluated and mapped towards probability of occurrence and possible damage. Second, for each votation individual risks need to be evaluated, e.g. which interest groups lobby for or against a certain political issue, especially if the stakeholders are from foreign countries. Those possible risks need to be checked e.g. with statistical tests.	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
It is delicate to publish the risks explicitly since criminal elements would be informed if they are on the radar or not. Therefore I'd only publish data and analysis that show everything went well and if something went not the regular way.	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
I don't understand this question.	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
Sorry I don't know the answer to this question.	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
Sorry I don't know the answer to this question.	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
I think science can support the government in such workshops as planned to verify and extend the conceptual and technical aspects of e-voting. However, security and statistical practitioners should support governments with repeating risk checks etc. since such assessments have little scientific value. Ideally the Federal government can hire such practitioners that support the cantons. If this is not possible this knowhow has to be procured externally.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?
In my opinion it is the software vendor who is responsible for the system covered within a Service Level Agreement (SLA). He needs to make the Federal government	

and the cantons aware of risks and possible attacks. They have to monitor their systems possibly with the help of external experts.	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton's processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
It makes sense to include the system provider into the risk analysis since he knows the implementation details of the system. Also assuming that many cantons use the same system it seems important to share the experiences among the cantons and reuse risk analysis procedures. This supports comprehensiveness and consistency.	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
The dozens of Excel sheets with makros etc. doesn't seem to be a very practical way of managing risks. I'd suggest to develop an individual e-voting risk assessment tool that builds upon the content of the methodology but has a better user experience.	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
I'm not an expert in crisis management thus I don't think my responses to this and the following questions would be of any value.	
7.2	What are the right events and thresholds for an activation?
Sorry I don't know the answer to this question.	
7.3	Who should be involved in crisis management, with which role?
Sorry I don't know the answer to this question.	
7.4	How should the communication be organised (internally and externally)?
Sorry I don't know the answer to this question.	

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
Sorry I don’t know the answer to this question.	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters’ platform, etc.) look like?
Sorry I don’t know the answer to this question.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
Sorry I don’t know the answer to this question.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
Sorry I don’t know the answer to this question.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
Sorry I don’t know the answer to this question.	

Responses to Swiss Federal Chancellery e-voting questionnaire

Vanessa Teague

March 12, 2020

1 Big Picture

It seems to me that the main advantage of democracy is the ability to examine and correct mistakes. My suggestion for the purpose of e-voting regulations is to think about the feedback mechanisms that are being put in place. Do they encourage good quality systems above those more oriented around secrecy? Do they provide mechanisms for meaningful feedback so that improvements can constantly be made? Do they incentivise honest appraisal and corrections of errors, rather than the pretence that errors are non-existent or not important?

In my opinion, the existing regulations are very good (compared to others in the world), but there's always room for improvement. The discovery of problems that had gone unnoticed in earlier versions is an endorsement of the stronger transparency provisions of the 100%-level certification. The less-transparent certification at earlier levels didn't work so well, so this seems to be good empirical evidence that those greater transparency mechanisms were more effective.

Another important aspect of the Swiss regulations is their very specific nature, and again I think this is well done. For example, the complete verifiability model requires that there must be at least 4 control components and they must all need to collude in order to manipulate the vote. This sort of specific requirement is good for two reasons: it makes the requirements and assumptions clear to decisionmakers, and it means that a system found to fail this requirement can be excluded fairly. (In places with more vague regulations, even serious errors can be deflected by claiming there are other defences.) But again, there is room for improvement: it would be better to insist on a closer and clearer link between the security proofs and the requirements. If there's a 'security proof' but it doesn't actually prove that the system meets the specified requirements under reasonable assumptions, then there isn't really a security proof. Similarly, if the practical procedures don't achieve the assumptions used in the security proof, then the security proof isn't relevant to the practical system.

1.1 The alignment between proofs and requirements

There are several reasons that an implemented protocol might not meet the requirements even if a security proof has been provided:

1. It might make mathematical assumptions that are not correct, e.g. that certain components of the protocol have certain properties.

2. It might prove things about an abstraction or a restricted version of the protocol.

3. It might not prove all the things specified in the requirements.

4. It might make assumptions that are not achieved in practice, e.g. that certain sets of components cannot be simultaneously compromised by the same adversary.

Some of these are inevitable: to some extent, any security proof describes an abstraction of the full protocol and relies on assumptions about its components. However, much more care could be taken to explain the abstractions and limitations of the proofs that are made available.

Consider Scytl's proof of complete verifiability for sVote version 2.0 [Scy18b]. I have not read it in enough detail to check thoroughly for logical or mathematical errors, but the four issues are already apparent.

1. It relies on the soundness of its ZKPs, which as we have shown are not sound in the adaptive model [HLPT19]. (Note this version was written before we explained these issues).

2. It uses a simplified version of the protocol in which there is only one choice in a vote (see Section 6, paragraph 2), thus sidestepping the issues described in Section 3.1 of [PT19].

3. The proof does not seem to cover the case of a malicious Vote Verification Context—this is explained in my answer to Question 2.1.2.

4. It relies on an assumption that sets of control components cannot all collude, which does not seem reasonable given that they are all implemented and administered by a single entity (Scytl and SwissPost respectively).

Another misalignment concerns the role of the bulletin board. The complete verifiability proof (like the trusted-server security proof) relies on a public bulletin board, but the actual system doesn't have one. The implications of this are unclear. In particular, because the proof assumes a public bulletin board but the system has only a private one, it's not clear which of the verifiability properties carry over and which don't.

Summary/Recommendation: A good proof would make very clear at the beginning what its assumptions and conclusions were, and a good product would make very clear how it deviated from the assumptions in its proofs. Such deviations are probably inevitable, but need to be clearly stated. At the moment, they are buried in the details of the security proof.

Each vendor or supplier should be obliged to provide a much much clearer set of trust assumptions and claimed properties, including a full explanation of the implications for manipulation and privacy breach, a complete and convincing proof that those assumptions imply those properties, and fully open code and docs so that everything can be independently assessed. The practical procedures should then be carefully implemented to ensure those assumptions are met.

In the case of the complete verifiability version of the system, it is far from guaranteed that SwissPost/scytl is going to meet that set of requirements in any reasonable timeframe.

1.2 Summary of the important questions

The questionnaire raises many questions that are outside my expertise—for these, I have marked them as "best effort," on the assumption that my opinions are no more informed than anyone else's, and in some cases significantly less informed, such as when the question relates to Swiss culture, opinions or public acceptance.

Among the questions that do relate to my expertise, two main themes stand out:

1. Can a *protocol* be designed and implemented correctly to allow for privacy and verification, under reasonable assumptions, in keeping with the regulations? If so, how? And how would we check? (Questions in Section 2.1)

2. Can *people* (particularly voters) be trained or motivated or encouraged to do the verification necessary to ensure their vote is cast as they intended? If so, how? And how would we check? (Question 2.3.1)

I feel that there are decent possible answers to the first question, as long as it is interpreted to mean a process of continual improvement of systems in which good people are more likely than not to find bugs before bad people. I am not sure that the incentives of the current marketplace tend in the right direction, however. I have a lot more faith in a completely open academic system like Helios, with its years of open academic examination, than a commercial system.

The second question is actually much harder to answer, because it relies not only on the soundness of a protocol, but on the behaviour of people. I feel that this second question represents the main unsolved problem of remote e-voting. I have expanded on this in my answer to that question.

2 Answers to other questions

2.1.1 *(Expertise)* For sophisticated building blocks such as Zero Knowledge proofs, there aren't really well-established standards. (For encryption and authentication etc, there are.) So unless the particular system and its components have been subjected to a rigorous analysis, it seems likely that some components might be flawed. As to how likely that the flaw could be used, that depends on the nature of the problem and the access granted to the adversary. In the case of the parameter generation for the shuffle proof, this was straightforward to exploit and perfectly undetectable, so anyone with access to the mixing server (including both the vendor and the administrators, I assume) could have performed it.

2.1.2 *(Expertise)* Yes, I think complete-verifiability version of the protocol in its current form, along with its security proof, is likely to be flawed. For example, I am not convinced by the proof that a collusion between 4 control components is the only method of manipulating votes on the server side. The Annex V2.0 Sec 4.3 requires "A single control component must - like the system - be assumed to be untrustworthy. However it may be assumed that at least one control component per group is trustworthy, but without specifying which it is." [Cha18] However, in Section V of the final version of our paper [HLPT19]. we show an attack that allows a malicious client in collusion with the Vote Verification Context to cheat, assuming that the printing office has colluded in the malicious generation of parameters. The summary is:

> In this section we show how a cheating client, in collusion with a cheating Vote Verification Context (VVC), can manipulate the vote but retrieve all the voter's expected choice codes.
>
> This will pass verification and show the voter her expected choice codes even though the vote is chosen by the client.
>
> The attack relies on maliciously generated parameters for representing the voting options, a reasonable assumption given the weaknesses that were identified in practice in version 1.0 [LHK19]. Although patching that gap thwarts the attack described here, it does not really solve the fundamental problem, which is that the code-return process is meant to be a verifiable distributed computation among 5 parties, with detectable misbehaviour if any subset of the *CCR*s collude, but there is no proof that this property holds and, indeed, it does not hold in its current form. There may be other exploitable failures even if the system is patched to thwart this particular attack. For example, although the specification document requires the VVC to verify some zero knowledge proofs that the CCRs generate, the audit document [Scy18a] does not require the auditor to verify them again. There may be other attacks in which a cheating VVC col-

ludes with a CCR to allow the wrong computation even though the ZKPs do not verify.

Examining the security proof with this claim in mind shows an example of exactly the sort of misalignment of assumptions I described in Section 1. First of all, the attack relies on multiple voting options, while the security proof describes only a single voting option "for simplicity." Second, it relies on a bulletin board, which does not exist in the production system.

Third, the precise attacker model varies through the security proof to the extent that it never actually covers the case in which a cheating VVC colludes with a cheating client. The security proof merges the Election Context, Voting Workflow Context and Vote Verification Context into one entity, the server, which it allows to be adversarially controlled. So far, this is perfectly reasonable. The possible attack described above relates to the malicious mis-execution of algortihm CreateRC, described in Section 4.4.5 of the proof. Section 5.5 of the proof gives an informal description of why cheating by a compromised server should be detected by an honest auditor, but no precise proof. The introduction to Section 6 (p.40) gives an overview of the main idea of the proof that attempts to substitute votes will fail verification. It says, "Since the attacker controls CCR_2 and the Voting Device it can compute..." That is, the assumption of server collusion seems to have disappeared.

It takes quite a lot of careful reading to see why Game A (p.41) is the relevant game, and why it does not cover all the attacker models that it needs to. The function used in the possible attack—CreateRC—is not mentioned explicitly as something run by either the challenger or the attacker, so the possibility that it might be run maliciously or incorrectly is never modeled. Instead, the proof is "oriented to prove that all the information the Attacker may have access to is independent from the Choice Return Code it has to generate," without considering that the party entrusted to generate that Choice Return Code might collude with it.

Also note that there is no explicit assumption of correct parameter generation by the printing office. Instead, there are generic references to the Decision Diffie Hellman assumption.

I am not certain whether there is a successful attack when the parameter-generation is trustworthy. However, I am quite sure that the existing security proof is incomplete.

2.1.3 *(Expertise)* Another way to express this question is to ask, given that the printing service has to be trusted, is there any meaningful notion of verifiability for a code-return voting system of this kind? I feel that the answer in principle is yes, but I'm not sure how to express it.

One interesting option could be to say that one could in principle (I'm not suggesting this is practical) distribute the printing office's functions,

so that each voter got two (or three or more) cards from separate printing offices, or so that the printing itself was performed in a distributed way [ECHA09]. In that case, one could make a well-defined argument that collusion among multiple parties was necessary in order to cheat without detection. But that would preclude unverifiable parameter generation, for example, except by a protocol that required collusion from all parties.

This is an important question deserving further thought.

2.1.4 *(Expertise)* There are several aspects to this question.

First consider the possibility that the specification of a control component's algorithm is buggy. In that case, independent implementation of the protocol would not automatically solve the problem, though it might make it more likely to be detected.

Second, even if they are running software from different providers, we still need to consider the possibility that they might be attacked (or administered legitimately) by a single entity.

But overall I feel strongly that it would raise the level of difficulty needed for a successful attack to insist on a very clear specification of the control component, and use implementations from different sources administered by different entities. This doesn't guarantee no shared flaws or common attacks, but it makes them less likely.

(Reminder that the question of whether simultaneous compromise of 4 components is truly necessary also needs to be addressed, but is probably a separate question.)

2.1.5 *(Expertise)* I assume the "auditors' technical aid" is the verification algorithm that the auditors run on the proof transcript after the election.

I do not think it is appropriate for this software to be written by the vendor. It is too easy for matching errors or omissions to occur in both the proof generation and the verification, even if there is no malicious intent. When we add the possibility of malicious compromise, the possibility of simultaneous compromise of the voting system and its verification code is an unacceptable risk.

The vendor should be obliged to provide a precise verification specification, which Scytl already does for sVote 2. That specification should be clear enough to allow the auditors (or their representatives/contractors) to implement it themselves. The auditors are then taking responsibility not only for running an automated test, but for examining its logic and convincing themselves that it is valid. The more independent teams of auditors, and the more responsibility they take for independent implementations, the higher the likelihood that protocol flaws and incorrect election results will be detected.

2.1.6 *(Best-effort outside expertise)* The question of using different operating

systems and hardware is related to the question of varying the administration and implementor of the other control components.

This is about grounding in some realistic assumptions the protocol-level assumption that not all the control components collude.

2.1.7 *(Expertise)* This question is asking about a Helios-like cast-as-intended verification mechanism in which voters cast a vote on one machine and then use some sort of direct method on a separate machine to verify that their votes were constructed as they requested.

These systems have the potential (if properly designed) for a much stronger form of verifiability, without placing trust in the secrecy of printed codes, but at the expense of sacrificing receipt freeness (usually, depending on the details) and making it hard to obscure who voted (which if I understand rightly is important in Switzerland).

Again the question of a publicly-visible bulletin board is relevant, because this would give voters the opportunity to check that their vote had been included in the count, without trusting control components.

I think these designs are well worth further consideration of their tradeoffs.

2.1.8 *(Expertise)* "The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)?" To be clear, the flaws we found in 2019 were in the specification, not in the deviation between the spec and the code. So the question you have asked is one half, and the other half is to ask how we can be confident that the specification meets the requirements/regulations—I have written a lot about this in the introductory section.

I'm not sure about what measures could be put in place to ensure the correct software is running. This doesn't affect verifiability, though it does impact on privacy and on the likelihood of the protocol completing. Of course, it also affects whether the assumptions necessary for valid verification (e.g. the non-collusion of CCRs) are true.

2.2.1 *(Expertise)* I feel that insider threats are by far the most underrated threat of e-voting systems. Although the VEIeS does mention these threats, it could be improved by more insistence on defences such as separation of duties and development, as described in Q2.1.3–6.

2.2.2,3 *(Best-effort outside expertise)* These are very good questions, but I have not re-read the VEIeS in sufficient detail to think of good answers (yet).

2.2.4 *(Best-effort outside expertise)* I do not feel qualified to comment on this in the case of Switzerland, where I assume the average standard is very high.

However, remember that complete verifiability relates to integrity, whereas most of the other security critical data you mention either needs privacy

primarily (e-health) or relies on a trusted authority (banking). Hence I do not think a comparison can be made. There are very few other fields in which both individual privacy and public verifiability are necessary.

2.2.5 *(Expertise)* Without knowing the details of Swiss paper-based electoral processes it seems hard to make the comparison. However, I would question whether, even in the postal system, there is an opportunity for manipulation comparable to the opportunity given to Scytl/SwissPost (or anyone who compromises them) if the flaws in their shuffle and decryption proofs had not been identified. The key characteristics are the possibility to manipulate a very large number of votes, very quickly, with perhaps only one person acting as attacker, and producing a proof transcript indistinguishable from a truthful one.

It also depends on how you define "undetectable" fraud. Many traditional paper-based systems have an option to audit or recount the paper, but that option isn't always taken up, implying that fraud may be detectable but not detected in practice.

Overall, the comparison depends on the exact protocol and procedures for both internet voting and traditional paper-based voting. Of the particular protocols I have seen, in both Australia and Switzerland, the opportunity for one well-placed person to commit substantial undetectable fraud is greater in the e-voting system than in that country's postal voting system.

2.3.1 *(Expertise)* In my opinion this question identifies the primary unsolved problem of remote e-voting. I cannot think of good answers either in the Swiss case or using the other designs (Helios, Estonia etc) mentioned above.

Part of the complexity here is that "sufficient" depends on other factors such as how close the election outcome is, how much public distrust is expressed, whether anyone challenges the result, etc. These may not be apparent until after polls have closed. Rigorous statistical methods such as Risk Limiting Audits expand their samples when the margins are close or the error rates are high. It is difficult (though not necessarily impossible) to do that for online voter-verification.

I would also characterise the value of individual verifiability differently from the way you have in your question. You've written "Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel." This argument would give assurance only for those people who have carefully performed verification. An alternative characterisation would be to consider those who verify as a kind of random audit that indicates an overall level of error or malfeasance. With that interpretation, a voter who detects a problem should not quietly vote by a different method, but should make public the fact that there is a problem, allowing for a population-wide estimate of the overall rate of error.

However, this then leads to the problem is that the people who check their codes are not a random sample, but self-selected. If an attacker can predict who will verify and who won't, undetected deception might be much easier.

Finally, there's the question of who gets evidence of the true verification rate. In recent testimony to a New South Wales parliamentary committee, a Scytl representative claimed a very high verification rate for the Australian Scytl e-voting system: "In this most recent update, Scytl introduced the verification client - a mobile app that allowed a voter to review the vote they had cast to see if it reflected their intention. This time, take-up has been significant, with almost one in every two voters choosing to verify their vote. That is a lot of voters; we have gone from 1.7 percent to something just under 50 per cent." [1] The New South Wales Electoral Commission made the same claim in their report from the election.[2] This is a remarkably steep increase between successive election cycles, amounting to more than 100,000 voters who apparently verified their vote without any mention of any discrepancies. Given that that 50 percent rate is much higher than the equivalent rate for the previous election, is significantly greater than comparable statistics from, for example, the IACR elections, and is itself unavailable for independent confirmation, I am highly skeptical. Even if that verification rate is true, the fact that the only people who can measure it have an incentive to inflate it is arguably not acceptable.

Overall, this is a hard but important question. One nice property of Helios and the paper-based verification procedures of schemes like Prêt à Voter and Scantegrity II, is that cast-as-intended verification itself does not violate vote secrecy—for Helios, you're challenging a vote that wasn't cast; in Prêt à Voter and Scantegrity II you're challenging a ballot that wasn't used. Hence these checks can safely be performed by third parties for other people's votes. This doesn't completely solve the problem, but it might help.

The Swiss code voting scheme doesn't have that property, but it might be an interesting thing to ponder. Is there perhaps a way to allow a third party to help with verification in a way that didn't reveal to that third party how the person voted?

2.3.2 *(Best-effort outside expertise)* Again, a very good question. One assumes that the return codes would help to detect if their vote had been stolen, but of course that doesn't help for privacy and also doesn't help if the person doesn't check the return code.

A related question is to check that the voter is visiting over TLS, rather

[1] `https://www.parliament.nsw.gov.au/ladocs/transcripts/2299/CorrectedTranscript-Inquiryintothe2019NSWStateElection-PublicHearing19February2020.pdf`

[2] `https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/Election%20reports/NSW-Electoral-Commission-2019-State-election-report_Part-1.pdf`

than accepting an unencrypted connection (presumably to an attacker's server). Some web browsers (including Chrome and Firefox I believe) now flag non-encrypted connections. Measures such as certificate pinning and HSTS might also help.

Similarly, ensure that all links from within other Swiss govt or SwissPost websites use TLS connections (https:// ...).

2.3.3 *(Best-effort outside expertise)* Not sure about this one.

2.3.4 *(Expertise)* My feeling is that quantum-resistance is important in principle, particularly for votes in long-term storage, but that in the immediate future it is a difficult enough challenge to achieve the security properties you need in current models of computation.

However, there are some schemes with a property called "everlasting privacy" [MN06, MN10] in which the secrecy is protected perfectly (i.e. information-theoretically). The tradeoff is that there must be a computational assumption for integrity, though in practice this is there already for the Fiat-Shamir Heuristic.

2.3.5 *(Best-effort outside expertise)* Not sure. Unfortunately, rates of malware infection can be very high.

2.3.6 *(Best-effort outside expertise)* I'm not sure about the question in practice, because it is partly a function of Swiss culture and habits. Note, however, that even if it isn't an issue for 95% of Swiss citizens, the remaining 5% are probably among the most vulnerable who most deserve the protection of their democratic influence.

As a purely technical question, there are modes of coercion that are possible with e-voting but not possible (or much harder) for postal voting. For example, as already mentioned in our previous report, the e-voting system returns a signed encrypted vote which allows the voter to prove to a third party how they voted, even if the third party was not present at the time. Not all internet voting schemes have this property, though many do. I do not think there is a similarly easy and definitive proof of how you voted, if you voted by post, and wish to convince someone who was not physically present.

3.1 *(Expertise)* There are two slightly different questions: who should be *permitted* to join in an examination, and who should be employed/paid to do so. One possibility is to engage some experts (e.g. from a university) and also to permit others (e.g. political appointees).

It is worth noting that certification of e-voting systems doesn't work very well in other countries either. I am aware of serious errors in 'certified' voting systems in both the US and Australia. Although it is not my area of expertise, certification seems to work well when there is a very clearly-defined specification and set of certification criteria (e.g. FIPS certification for cryptographic primitive implementations).

Certification is a less-useful concept when considering something that is very complex, less poorly defined, and more likely to have subtle bugs. For example, verifying the security proofs and the cryptographic protocol is a continuous work-in-progress. The report on sVote 1.0 by David Basin and his group actually makes some important suggestions and raises some significant concerns, but because it was interpreted as "certification" rather than "examination with a view to improvement and assessment," those concerns do not seem to have been acted upon.

3.2 *(Best-effort outside expertise)* Being completely honest with the voters (and candidates) about them is a must. I would also suggest that privacy is different from verifiability/security. Some people might not mind using a system with weaknesses in its privacy protections, so it might be acceptable to run such as system as long as the potential users were accurately informed, and as long as alternative privacy-protecting voting options were available to them. However, it seems hard to justify running a system with verifiability gaps even if people know they are there.

3.3 *(Best-effort outside expertise)* Yes. I think the right way to think about it is to consider the incentives of the people involved. To return to my theme from Section 1, when is there an incentive to identify, accurately report, and correct errors, and when is there an incentive to overlook them or downplay their severity? Individuals' incentives are affected by who they are and who employs them—it makes a difference whether they are employed by those who benefit from a positive public perception of the software, or those who are independent, or those who have a political interest in the electoral process. Other things matter too, though: for example, if a person is employed to write a report in the context of an open process in which both their report and the artefacts they are examining are public, then their work itself is much more likely to be put under third-party scrutiny and this is likely to incentivise more care and honesty.

In Australian traditional paper-based elections, our rule is that any candidate in the election may appoint a representative to scrutinise the electoral process. They don't always bother in practice, but nevertheless the fact that the process was open to such scrutiny tends to increase trust, even among those candidates who couldn't send a representative to every polling place. I am not sure whether a similar rule would make sense in the Swiss context, but it is worth noting that the incentives of political candidates are quite different from the incentives of those who write or administer the software.

3.4 *(Best-effort outside expertise)* Clear link with the regulations. The examination should, roughly, be testing whether the protocol and implementation meet the written regulations.

3.5 *(Best-effort outside expertise)* If you think of it as a process of continual examination and improvement, then this question isn't really meaningful

any more. Nobody will truthfully be able to say "I'm 100% certain it's perfect." More likely, any real examination will identify some issues of greater or lesser importance, and there may always be other aspects that were not examined. At any time, I would hope there's a clear public description of what has been examined and what the known issues are, and what the intented remediations are.

3.6 *(Expertise)* 45 days is perfectly reasonable; indefinite extension is not. Also recognise that the normal rules of responsible disclosure balance the public's need to know against the risk of exploitation of the vulnerability. For insider-only attacks, or software that is not running, arguably there's no real justification for any delay. But there's a great complexity around the fact that the same software may be running elsewhere, and that the people involved in the disclosure may not even know. The argument for delay then is that the vendor needs to patch before any external attacker gets in and exploits the problem. The argument for immediate publication is that there is a heightened risk of insider attack as soon as the insiders are notified, so voters and candidates should be notified immediately too.

This is another instance of the theme of who is trusted—the vendors would like to control the disclosure and patching process, and if they were perfectly trustworthy then that would be entirely appropriate. However, nobody is perfectly trustworthy, and it is the vendors and administrators themselves who are, by definition, in the best position to exploit an opportunity for insider attack. Hence the question of how quickly a matter should be publicly disclosed should arguably be taken out of their hands, for example using an explicit set of rules or guidelines from the Federal Chancellery.

3.7 *(Best-effort outside expertise)* I am not sure—this is a question for Swiss administrators.

4.1 (*Partial expertise)* I don't see any real reason why the source code and documentation couldn't be made openly available. I am not any kind of expert on IP law, but I think the notion of vendor intellectual property is much overstated. For one thing, a great deal of the funding for this system, along with much of the intellectual basis for the overall design, has come from Swiss public-sector entities. For another, having looked at Scytl's system in particular, those aspects that are of value are generally not Scytl's IP.

As for notification and publication, 45 days is reasonable but indefinite extensions are not. Also (depending on Swiss electoral law) arguably there should be a *shorter* timeframe during elections, because the public's (and the candidates') right to know might be important for resolving disputes about the election. You could also consider different kinds of public notifiation. For example, if another problem were identified affecting verifiability, it might be appropriate to tell the public immediately that a

problem was known, but you might choose to delay publicising the details until the end of the election.

One thing that is clearly not acceptable is to behave as the Australian authorities in New South Wales did, and claim that a problem was "not relevant" when it demonstrably was.[3] Note that publicly available source code would at least allow the public to assess specific claims of this kind.

I don't think there's anything wrong with offering incentives, as long as they're aligned with constant improvement.

4.2 *(Expertise)* The more documentation is made public, the more opportunity for assessment there is, but at least the code, protocol specification, verification specification and security proofs. (I should say, however, that these are only the artefacts that I understand, and perhaps there are other valuable artefacts that people with different expertise would benefit from.)

4.3 *(Expertise)* The earlier the better. You have seen what happens for publication 6 months in advance—later would have been worse; earlier would have been better.

4.4 *(Best-effort outside expertise)* There's never harm in publishing more than required by law.

4.5 *(Best-effort outside expertise)* I feel that this is a question for Swiss administrators. My main suggestion is to think about the incentives of all people involved.

4.6 *(Best-effort outside expertise)* Existing, definitely yes, at least to some independent federal authority, if not to the public, and especially if it impacts an election. Past, fixed, issues are less important.

4.7 *(Expertise)* Yes, but there are also important limitations.

Arguably, if the claimed security property of the new system is defence against an untrusted server, then the proper form of PIT would be one in which researchers/participants are given control of up to 3 (or whatever) server components. I'm not entirely sure how to make this work in practice.

4.8 *(Expertise)* Yes, I think the fraction of votes accepted over the Internet significantly affects the likelihood of successful manipulation of the overall election result.

Note, however, that in a very close election (which happens sometimes), even a small fraction of votes cast over the Internet may be decisive.

4.9 *(Expertise)* In the academic literature, the end-to-end verifiability schemes typically envisaged completely open verification of a public transcript.

[3] `https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/MediaRelease/190322-NSW-Electoral-Commission-iVote-and-Swiss-Post-e-voting-update.pdf`

Thus the question of who should do the verification didn't really arise. I understand why the Swiss bulletin board is secret (in order to protect the privacy of who voted), but it still represents a significant sacrifice—(a) voters now rely on authorities to post their vote on the bulletin board, without being able to verify it themselves, (b) it introduces a degree of trust on the people who perform the verification, and the people who appoint those people, etc.

So I'm not sure of the right answer to your question, but I think it is worth revisiting the possibility of a public bulletin board. At least, during the discussions it is worth listing the pros and cons of secret vs public bulletin boards.

4.10 *(Expertise)* In New South Wales this has been a helpful way of discovering (presumably accidental) problems. For example, in 2015 there was a scrolling problem that (probably) lowered the vote of those parties that didn't fit within the width of a typical screen—this was quite obvious from the separately-reported iVote data, but it wouldn't have been obvious from unified paper and electronic data, because the paper results would have swamped the bias in the small fraction of votes cast over paper.

I'm not sure that the separation proves very much that's meaningful about deliberate surreptitious manipulation, but it might help to detect accidental electronic problems. A deliberate attacker would probably ensure that the electronic returns didn't differ from the paper ones too much, but an accidental bug might cause a noticeable bias or anomaly in the electronic returns which might be easily detected if they were separated out.

4.11 *(Expertise)* As above, consider the tradeoffs for a public bulletin board.

4.12 *(Expertise)* I'm unconvinced that many of the advertised statistical plausibility checks are meaningful, unless they are specifically designed to defend against an intelligent attacker who knows what checks will be performed. As above, they might be useful ways to detect some honest mistakes and accidental bugs, but I don't think they can be a defence against deliberate manipulation.

(Obviously I am not talking about Risk-Limiting Audits, which do defend against manipulation of any pattern, but require an independent trustworthy basis for the ballot records.)

5.1 I would suggest that the long-term sustainable strategy is to engage the many excellent researchers from Switzerland, who can be expected to take a long-term interest in the security of their own democracy.

5.2 I'm not sure whether this is asking when scientists should be obliged to participate, or when they should be permitted to participate.

I feel comfortable participating in political debate in my own country, and even in the US (where I lived for many years), but less comfortable in

Switzerland because I have much less of an understanding of the context and tradeoffs. In this case, I feel that my role is to explain the security properties of the technology and mostly to leave political decisions to the Swiss.

5.3 I think the artefacts that the regulations currently require, source code, documentation and security proofs, are appropriate. (again, see q. 4.2—I am listing the documents that I would read because they are relevant to my expertise, but there may be other sources of information that are relevant to other kinds of examination.)

5.4 This is another extremely important question. This seems to me to be at the heart of any potential future success of verifiable electronic voting.

People can be frustratingly irrational in what they choose to trust. In practice, I'm sure that indicators of reliability such as ease-of-use, website uptime, convenient language support, etc, would have more influence on the trust of ordinary people than the true verifiability properties of the protocol.

Hence I'm not sure that promoting trust is actually the right objective. Arguably, promoting accurate public assessment of the risks (for better or worse) is the right objective.

5.5 Anyone who wants to! Note that if the source code were completely open, anyone could run these sorts of things. For example, a canton that was thinking about becoming a customer could run an open hackathon or whatever they wanted and then, on the basis of what people in that canton told them, could decide whether or not to buy it.

6.1 Constantly and in the open.

6.2 This relates a little to the responsible disclosure question. In my opinion, the only justification for not making an issue open is the expectation that it cannot be corrected in time for the election, and publicising it makes it more likely to be exploited. If it can be corrected, or if the election is complete, I don't see any justification for keeping it secret.

6.x I don't have sufficient expertise in risk management to answer these questions, but I'd suggest that it's important to think about who has an incentive to assess the risk accurately rather than an incentive to mininise or discount it.

7.x I don't have sufficient expertise in incident response to write anything sensible here.

Note, however, that there may be a serious incident without anything obviously having gone wrong. This hidden trouble is precisely what verification is meant to prevent, but of course if verification isn't perfect there's always that risk.

References

[Cha18] Swiss Federal Chancellery. Annex to the FCh (OEV, SR 161.116) ordinance of 13 december 2013 on electronic voting - version 2.0, July 2018.

[ECHA09] Aleks Essex, Jeremy Clark, Urs Hengartner, and Carlisle Adams. How to print a secret. In *Proceedings of the 4th USENIX conference on Hot topics in security, Hot-Sec*, volume 9, pages 3–3, 2009.

[HLPT19] Thomas Haines, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. How not to prove your election outcome. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 784–800, 2019.

[LHK19] Philipp Locher, Rolf Haenni, and Reto E. Koenig. Analysis of the cryptographic implementation of the swiss post voting protocol. `https://www.bk.admin.ch/dam/bk/de/dokumente/pore/E-Voting_Report_Locher_Haenni_Koenig_Juli%202019.pdf`, July 2019.

[MN06] Tal Moran and Moni Naor. Receipt-free universally-verifiable voting with everlasting privacy. In *Annual International Cryptology Conference*, pages 373–392. Springer, 2006.

[MN10] Tal Moran and Moni Naor. Split-ballot voting: everlasting privacy with distributed trust. *ACM Transactions on Information and System Security (TISSEC)*, 13(2):1–43, 2010.

[PT19] Olivier Pereira and Vanessa Teague. Report on the swisspost-scytl e-voting system, trusted-server version. `https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/berichte-und-studien.html`, July 2019.

[Scy18a] Scytl. Scytl svote – audit of the process with control components - software version 2.1 - document 3.1, 2018.

[Scy18b] Scytl. Scytl svote – complete verifiability security proof report - software version 2.1 - document 1.0. `https://www.post.ch/-/media/post/evoting/dokumente/complete-verifiability-security-proof-report.pdf`, 2018.

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name	Ulrich	**Last name**	Ultes-Nitsche
Organization	University of Fribourg		

Internet voting security is costly. The low scale trials conducted since 2004 have allowed the Confederation and the cantons to learn and improve while keeping risks limited and prices affordable. The revelations that were made in 2019[2] now give rise to further improvement. The Federal Council commissioned the Federal Chancellery to work with the cantons to redesign the trial phase of internet voting in Switzerland until the end of 2020. The aims are to further develop the systems, to extend independent audits, to increase transparency and trust, and to further the involvement of experts from science. The requirements and processes are also to be reviewed. Resumption of trials must be conducted in-line with the results of the redesign of the trials.

1. Big picture

In this section, we would like to get a sense of where you think the journey could be headed, where you locate priorities and the sequence of steps that could be taken in that direction.

We also ask you to relate your statements to the rest of this document (which are the critical questions?). You are also asked to point out any important issue you feel has not been taken into consideration yet.

ID	Questions
1.1	You visit an imaginary country where internet voting is widely used. Given your background, you want to assess to which degree internet voting in that country may be considered «trustworthy» with respect to past and future votes. (Assume the possibilities that technology currently offers, i.e. no futuristic devices. Assume that coercion / vote buying are not a problem.) Which are the most important questions you would need answers to? (Think for example of roles and responsibilities, operations, system, scrutiny) Which are the most important answers you need in order to conclude that internet voting is trustworthy? How does the origin of the answers influence your conclusion? Which piece of information would need to originate from which source in order for you to consider it relevant for your assessment (e.g. information on system features, third party examinations or voting procedures)? Then relate your statements to the Swiss case. Which key-elements from the answers above do you observe in Switzerland? Which existing key-elements could be

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html

https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

	improved? What is missing? Can you identify any low hanging fruits? Where can you spot alternative approaches you find interesting? We would like to understand the reasoning behind your views in detail. Please give extensive explanations. If this requires writing extra pages, please do so.
First, I would aim at getting information about how verifiability, both individual and universal, is achieved conceptually. Can I assess the effectiveness of the measures in place? Second, I would try to assess the software development process. Best practices for developing safety-critical systems would be a good reference frame. In addition, the ability (based on prior experience) of the developers to implement cryptographic protocols would be a major concern for me. Finally, I would aim at getting a clear understanding of the trust assumptions made in the security assessment of the Internet voting system. Clearly, I would have to base my assessment on information provided by others. I would never base my assessment on information from the system developers only. The systems must be assessed by independent auditors – ideally involving some who are not in favour of Internet voting. All given information should be verifiable in the sense that one could (if able and willing) check statements made about the system on the open source code of the system. If I relate this statement to the Swiss case, I do not consider the source code in the usual sense as being open. Here I see scope for improvement.	

2. Risks and security measures today and tomorrow

The Federal Chancellery Ordinance on Electronic Voting VEleS and its annex regulate the technical conditions for the cantons to offer internet voting, in particular for systems offering so-called complete verifiability. Article 2 VEleS in conjecture with chapters 2, 3 and 4 of the annex relate to security measures that need to be put in place. Articles 3 and 6 additionally require risks to be assessed as sufficiently low. Articles 7, 7*a*, 7*b* and 8 VEleS in conjecture with chapter 5 of the annex regulate certification and transparency measures towards the public. In an authorization procedure (Article 8 VEleS and chapter 6 of the annex), the cantons demonstrate towards the Confederation that these requirements are met.

The cantons are in charge of elections and votes. They have to provide the necessary means for conducting them according to the law. This is also true for internet voting: the cantons procure an internet voting system, operate it and are responsible that the system works properly. Elections and ballots are tallied on Sundays, three to five times a year, on all three state levels (federal, cantonal and municipal). The results should be announced before the evening. With regard to that, irregularities (e.g. observed in the process of verification) should be manageable in such a way that conclusions can generally be drawn within hours. In particular with regard to additional security related measures, it is important to the cantons that ways are explored to keep the complexity of the operations bearable and ideally to aim for solutions that can be implemented with existing resources. With regard to the complexity of their operations, we ask you to take into consideration that the cantons – and not the service provider[3] – are responsible for the following tasks:

- Import from the electoral register
- Configuration of the vote (incl. generation of codes for individual verifiability)
- Preparation and delivery of voting material
- Splitting of private decryption keys and casting of test votes
- Support for voters
- Detect double voting: Querying the internet voting system for every vote cast through postal mail

[3] The requirements of the VEleS are not tailored to one specific internet voting service. However, since the future plans of the cantons interested in offering internet voting in the near future exclusively aim for Swiss Post as their service provider, the core facts of operating that service are outline here.

- Decryption and counting of the electronic votes (incl. the test votes)
- Verification of results (by the means of universal verifiability and by comparison with the other voting channels)
- Transferring the results to the systems used by the cantons for aggregating the votes from non-internet voting sources

Goals

- Risk-identification
- Identification of counter-measures
- Assess counter-measures

2.1 Verifiability

«Complete verifiability» as defined in the VEleS stands for the possibility to detect manipulations by putting to use independent equipment and thereby avoid needing to trust one individual instance. The secrecy of the vote is addressed simultaneously by defining an appropriate crypto-protocol. The trust-model in chapter 4 of the VEleS annex defines the trust-assumptions that underlie the effectiveness (the security objective) of the protocol and thereby the effectiveness of « complete verifiability». The effectiveness of complete verifiability also hinges on the independent equipment applied (their number, the «degree» to which they are independent, their protection from unauthorized access and the correct implementation of their functionality as defined by the protocol).

ID	Questions
2.1.1	**Crypto-Protocol** The effectiveness of the protocol depends on assumptions on the effectiveness of cryptographic building-blocks. Does it seem likely to you that building-blocks are flawed even if they comply with known standards? How likely does it seem to you that such a flaw could be used for an undetected attack?
If the building blocks really apply to the known standards, the likelihood is from my point of view small. However, if the statement refers to “a known standard was the basis for the given implementation”, then the likelihood is not negligible that flaws are introduced by inadequate programming. Here, the open availability and therefore reviewability of the source code should help to minimise the likelihood of undetected flaws and attacks resulting from them, assuming that one reacts immediately to the publication of flaws in building blocks of one’s systems. (I assume here that, when the code is open source, a flaw will not be detected solely by a single individuum who could exploit its knowledge in an attack, by that flaws will be detected by many people in a reasonably small time span, and at least one individual will the system provider and other involved entities in due course.)	
2.1.2	The effectiveness of the protocol also depends on whether it achieves the security goals in the defined trust model. Does it seem likely to you that the protocol and its security proof is flawed? How likely does it seem to you that such a flaw could be used for an undetected attack?
It is not very likely, but also not excluded. From past experience we know that protocols considered secure, or even cryptographic primitives, can turn out to being flawed. The likelihood of undetected attacks still is fairly low, assuming that one reacts immediately to the publication of flaws in protocols applied in one’s systems.	
2.1.3	**Printing office** For «individual verifiability» to be effective, the return codes the voters receive by postal mail need to remain confidential. Since it is infeasible to protect the return-

	codes by cryptographic means from being divulged during and after printing, the trust-model allows the functionality of the printing office to be considered trustworthy. However, the VEleS is not clear about which functionality can formally be assigned to the printing office. Should the printing office only decrypt and print? Or could even some parameters be generated in the printing office? Formally assigning functionality to the printing office is intriguing, because that functionality could then formally be considered trustworthy and it would be obsolete to verify the output using independent equipment. With the system of the Swiss Post, the generation of certain parameters has not been designed to be verifiable (formally, the generation of those parameters have been assigned to the printing office). How does this affect the effectiveness or the credibility of verifiability? Which enhancements would you propose?
I would leave the trust assumptions as low as possible. Transferring duties to the printing office, first of all, only formally does it make it obsolete to verify the output. The output could be flawed only because of an accidentally improper realization of the creation of security parameters. I see it as a weakness that creating certain parameters does not happen in a verified way. Has it ever been established that the generation of these parameters by the printing office is nearly certainly not flawed?	
2.1.4	**Independence** The VEleS allows to assume that 1 out 4 «control-components» is trustworthy. The effectiveness of verifiability hinges on the degree to which these components are distinct. Using distinct components reduces the probability that all components share the same flaw that could be exploited to launch an unnoticed attack. Yet, the VEleS allows to use application-layer software from the same provider on each control component. In practice, at the PIT 2019 the identical software from Scytl was run on all four control-components. How do you assess the added value and downsides of running software from different providers on the control-components? Does the added security benefit offset the added complexity and the potential new attack vectors opened?
First of all, it looks a bit dubious if a security measure is achieved by concurrently executing different components, assuming that at least one will be trustworthy, and then having only one software component “sitting on top” of these different components. The public perception may suffer from such an architecture. Personally, I would also prefer different software from different providers running on the control components. It simply reduces the risk of systematically overlooking something that may be important. The need for interoperability will certainly increase the complexity. To be honest, I cannot really judge whether or not the increase in complexity outruns the potentially increased security.	
2.1.5	Similarly for «the auditors’ technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors’ technical aid that was written by a different provider than the one of the voting system?
I would clearly not have the system provider develop the technical aid for auditors. Most likely, even not knowingly, the system provider’s view on the technical aid will be biased by its system and implementation knowledge. An independent developer of the technical aid will have a much more unbiased view on the proofs for universal verifiability.	
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could

	constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
I consider the requirement for different hardware and operating systems a must to circumvent the exploitation of weaknesses that a single OS or computer architecture may contain. As I am not sure about how far the term "different hardware" does go, I would even prefer the requirement that at least one system uses a processor family different from the processors used in the other systems.	
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
If the device could indeed be trusted it would solve a problem that is not very frequently addressed: vote secrecy. Verifiability always deals with disclosing manipulations of votes or vote counting. It is assumed that a manipulation of a vote is not problematic as long as it can be recognised by the system/voter, e.g. by incorrect return codes. The problem that a voter's choice (i.e. the vote) can become publicly known, if the voter's computer can be manipulated by an attacker, remains open. Inherently, Internet voting seems to make the assumption that the potential disclosure of a vote to an attacker is a risk a voter has to take when using Internet voting (similar to postal vote when someone steals and then opens the letter with a vote; even though disclosing votes would scale much better when done in Internet voting). Guaranteeing vote secrecy could be increased significantly when voting with a trusted tamper-free device. In addition, as mentioned in the question, verifiability could be improved when a trusted device is used for casting an Internet vote. Using a public bulletin board contradicts the indefinite secrecy of a vote that, to my knowledge, is a legal requirement for elections/referenda.	
2.1.8	**Correct implementation and protection from unauthorized access** The software that was published in 2019 had security flaws. Which measures could be put in place in order to avoid these flaws (i.e. to make sure that the protocol is implemented according to its specification)? The VEleS did not set a strong focus on development and deployment procedures but rather on the final product. Do you know any standard that would likely lead to better procedures at development if required by the VEleS? Which measures could be put in place in order to ensure that the correct software is running (as examined and authorized based on the source-code), in particular on the trusted components? What could the role of independent experts from academia and industry be?

In safety critical system develop, their exist criteria for software development, depending on the criticality of the system. I would regard an Internet voting system equivalent to a highly safety-critical system as its failure has a severe social impact. Therefore, ideally, formal verification should be applied to the software development process that turns the protocol specification into code. That means, one should formally verify that the code respects the specification under all possible computation sequences. This process is very costly, but from my point of view the most rigorous way of debugging critical software.

2.2 Security related risks top-down

The top of chapter 3 of the VEleS annex reflects the basic systematic of how the cantons should assess risks. The security requirements in chapters 3 and 4 of the annex need to be met by implementing security measures to the extent that the risks are adequately minimized. According to article 6 VEleS additional measures need to be taken if necessary.

ID	Questions
2.2.1	Are there any threats you feel are not covered by the basic threats in chapter 3.1 of the VEleS annex?
In 3.1.1-3.1.4, it is not considered that the systematic manipulation of each vote is a non-classical denial of service attack: assuming individual verification works (i.e. the risk of an inaccurate vote is annihilated), cast votes can be manipulated systematically (3.1.17 does not apply), and will be recognized as falsified. So the intended service of casting a vote is denied. Or is that aspect assumed to be covered by 3.1.17? Then I would rather say “Malware on the voter’s computer makes **casting intended votes** impossible” Doesn’t 3.1.10 also affect (depending on the way individual verifiability is achieved) “non-disclosure of evidence of vote casting behaviour”?	
2.2.2	Are there any security measures that seem imperative and that would not fall under the requirements in chapters 3 or 4 of the annex or of the referenced standards (controls due to ISO 27001 and Common Criteria Protection Profile)?
The security measures given in Chapters 3 and 4 seem pretty much comprehensive. Cryptographically as well as record-keeping-wise (protocol runs, involved systems) up to human-resource requirements I do not miss anything. As a side remark: it is quite difficult to keep the overview of what is presented in Chapters 3 and 4, particularly Chapter 3. Would it make sense to run through a number of scenarios to illustrate the breadth of the covered security measures?	
2.2.3	Do you know, from your experience with the Swiss case, any critical requirements that have not been met in an effective way? Apart from the Swiss case, are there any security requirements for which you believe that they are important but might typically not be met in a sufficiently effective way unless the requirement is stated in more detail? Do you know any measures or standards that – if required by the VEleS – would likely lead to more effectiveness?
I do not know of requirements that need to be stated in more detail. In particular in the Swiss case, the requirements are, from my point of view, sufficiently detailed. The question is how to achieve them effectively.	
2.2.4	Given a completely verifiable system that complies with VEleS requirements: Would it be safe to state that in terms of integrity and secrecy the cast votes are protected far better than security critical data in other fields (e.g. customer data in banking, e-health, infrastructure, etc.)? Please relate your answer to conditions on the effectiveness of verifiability (soundness of underlying crypto, assumptions on

	trusted components, number, independence and protection of trusted components, correctness of software in trusted components).
Yes, I'd say so. The cryptographic effort to provide evidence that a transaction (the casting of the vote) has been carried out as intended is higher than in other areas. Also providing verifiable cryptographic proofs of the correct execution of different steps in a system, including giving evidence of the correct result processed by the entire systems outruns security efforts in other fields (to my knowledge). However, to me, the secrecy of a vote is a more important and more vulnerable asset than secrecy in other contexts (including banking and even health), and with a potentially manipulated election there is more at stake than in other contexts. Even though not being handled worse than in other contexts, in particular vote secrecy is problematic as long as the user platform cannot be assumed to be secure (achievable most likely only with tamper-free special purpose hardware).	
2.2.5	Voters have two options to cast a vote: at the voting booth or by postal mail. Internet voting is a third option (the same voting material received by postal mail also allows to vote through the other two channels). Do you feel the effort for powerful actors to circumvent the protection of internet votes is likely to be higher than with in-person or postal voting (>90% of voters vote by postal mail)? Or could secure internet voting potentially even be considered a gain in security? Which kind of powerful organization might try to manipulate or read votes? What methods would they most likely choose? Are there also reasons why they would not apply certain methods?
This is quite speculative. Clearly if powerful criminal or terrorist organizations just would like to disrupt an election, they could attack polling stations, the premises where postal votes are collected or whatever. First of all, such attacks will not go unnoticed, they are very targeted, and they require the physical presence of the attacker. It is hard to imagine that such attackers could bribe sufficiently many people involved in the electoral process or infiltrate the authorities in such a way that they could manipulate elections unnoticed. The "unique potential" of Internet is to "only" have to crack a technical system unnoticeably, if you want to manipulate an election, and your physical presence in the country you are attacking is not necessarily required. So the risk for an attacker is lowered. In many aspects, Internet voting is at least as secure as the two conventional channels, but it also gives rise to novel risks. Verifiability (individual and universal), for instance, gives rise to counting votes with less error than in postal voting. But an exploitable vulnerability in the Internet voting system may give rise to a much more scalable manipulation. In that sense, I do not consider Internet voting being more secure than the two conventional channels (it is just another channel with its strengths and weaknesses).	

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly).

	Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
Yes, I am fully and utterly convinced that Swiss citizens take referenda and elections very seriously and are sufficiently IT literate so that a sufficient proportion of the voters would identify such fraud and inform the authorities.	
2.3.2	The voters are also advised to check the TLS-Fingerprint in their browser. This aims at enabling them to detect connections to a wrong server. What measures could be taken in order to maximize the number of voters who check the fingerprint?
To be honest, I have no clue. I am convinced that at the beginning, when Internet voting is introduced on a larger scale, people may check the TLS fingerprints, but once Internet voting has become sort of commonplace, I doubt that many voters will check the TLS fingerprints. Repeating that it is important will not do the job.	
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
I am not sure, I understood the question correctly. Are you assuming that on the client side verifiable code is running? I do not see the average user being able to verify that they are running the proper client application. I hope I am not misunderstanding the question entirely.	
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
I would ignore quantum computing completely for the moment. The rise of applicable quantum computing has been announced regularly in the past without any effect and no hint that quantum computing is available secretly to any organisation. I do not expect applicable quantum computing to be ready within in my lifespan.	
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
On the whole, following the guidelines, for instance from MELANI, can influence the trustworthiness of user's platforms significantly by installing good antivirus software and showing a generally good	

[4] https://www.melani.admin.ch/melani/en/home/schuetzen.html

security-aware behaviour. However, I challenge the rationale of the question. The guiding principle should be that the voters' platforms are not trustworthy.	
2.3.6	Despite postal voting being used by more than 90% of the voters, vote-buying and coercion are not considered to be a concern in Switzerland. Do you think internet voting would in practice be likely to increase the number of successful attempts of vote-buying or coercion?
In Switzerland, I doubt it very much that vote-buying and coercion would increase with a comprehensive introduction of Internet voting. The democratic processes in Switzerland and in particular the democratic self-conception of the Swiss voters would render attempts of large-scale unrecognised vote-buying impossible. There would always be sufficiently many voters who would make such attempts public.	

3. Independent examinations

The security issues mentioned above have not been identified as blocking issues at certification. This gives rise to the question, how examinations should be performed in order for them to be effective.

Due to article 8 VEleS in conjecture with chapter 6 of the annex, the cantons demonstrate to the Confederation that certification has been conducted successfully. Formal certifications related to operations and infrastructure (ISO 27001) and to the internet voting software (certification based on common criteria) are required. In practice, the cantons had their system provider Swiss Post mandate a certification body for certification according to the two standards and separately experts to verify the security proofs of the cryptographic protocol.

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
I do find this a very difficult question. Obviously, the organizations must be independent etc. They also should not be mandated by the system provider to avoid any conflict of interest. Certification is certainly very important – it helps finding problems, but does not necessarily prove their absence. Formal certification certainly is the most rigorous way of trying to find errors in a system, and should from my point of view be applied. One could learn from the safety critical systems community how to increase the confidence it the correct operation of a critical system (such as an Internet voting system).	
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
There might be "mild" security problems that technically would not force one to abandon using the system. This could, however, be quite dangerous with respect to the public perception of the trustworthiness of the system. In particular when Internet voting is in its infancy – as it is currently in Switzerland – the public acceptance could change very rapidly if someone exaggerates purposefully	

the severity of the problem. Having to admit the existence of a security problem, even of the mildest form, the election authority may lose its authority.	
3.3	Does the credibility of the outcome of an examination among the public (and experts from the public) hinge on which organization appoints the examination? Please relate your answer to individual areas of the scope (e.g. software, operations/infrastructure, trusted components).
The independence of the organization conducting the examination from the organization appointing the examiner is critical. It should never be a provider of a component of the system who appoints the examiners. There should also be provable financial independence between them. The public must trust the examiner being technically capable of conducting the exam as well as in the independence of the examiner from the system provider as well as the election authority.	
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?
To me, an Internet voting system is a critical system ("socially critical"), and I believe examinations should be done to a similar level as in safety-critical systems industry, for instance software safety in airborne systems. There exist standards such as ED-12C (Europe) / DO-178C (US), and derived best practices, e.g. as applied by NASA. The main remaining problem is probably cost. The required development and evaluation procedures are very involved, and not easily implemented. Adhering to the best practices from current security standards is certainly also very important. However, I am not fully convinced that these standards are sufficient given the application context of Internet voting. Therefore the note about the safety-critical system best practices.	
3.5	How long can results of examinations be considered meaningful? Which events should trigger a new mandated examination? In which intervals should mandated examinations be performed?
I am not sure whether or not intervals are the best measure here. There should be guidelines about events triggering additional examinations, like new security issues with systems applied within the voting system or software updates affecting critical system components.	
3.6	How should independent experts in the public (not mandated for the examination) be involved? How and at which stage should results be presented to them / to the public?
I believe that communicating all procedures and possibly identified problems very openly is the mechanism to get independent experts on board, taking into account the risk of misinformation on purpose.	
3.7	How could the event of differing opinions be handled in the context of the Confederation's authorization procedure?
Have an open debate. I have no other suggestion to make.	

4. Transparency and building of trust

During the past years, transparency has played an ever-increasing role in the matter of public affairs and trust building. In voting especially, transparency and trust play an important role. In reply, the steering committee Vote électronique has set up a task force «Public and Transparency» which produced a report in 2016. Following this report in 2017, the Federal Council decided to include the publication of the source code as an additional condition in the VEleS. Accordingly, articles 7*a* and 7*b* have been added. Additionally, the Confederation and cantons agreed that a public intrusion test (PIT) would be conducted after the publication as a pilot trial as well.

In February 2019, Swiss Post disclosed the source code of its system developed by Scytl, aiming at fulfilling the requirements for completely verifiable systems. The access to the code

was granted upon registration and acceptance of conditions of use.[5] A few weeks later, the PIT was running under a separate set of terms and conditions [4]. Due to the publication of the source code, numerous feedback from the public could be gathered, in particular three major flaws were uncovered. The PIT led to the discovery of 16 breaches of best practice. Yet, these exercises led to criticism in the public and in the media.[6]

Goals

- Identifying communication measures, in particular aiming at integrating the independent examinations into the public dialog
- Setting out the conditions related to source code publication
- Setting out the requirements related to public scrutiny

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the specialized community? Would incentives for participation at analyzing system documentation be reasonable? How could intellectual property concerns of the owner be addressed at the same time?
I argue in favour of open source code. All code should be openly available – not only after a registration procedure, etc. The licensing should take this into account. I know that this will clash with the current ownership of the code, but to me that is the only way to go to achieve full transparency.	
4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
All should be published, documentation, code, evaluation procedures (e.g. how it is tested).	
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
Whenever it is available. I would not necessarily see the general public as “the enemy” – I hope I am not too naïve.	
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
I would phrase Article 2 c) more generally (with respect to open source). Otherwise I am fairly happy with the requirements.	
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
If the federal system permits it, I would create a contact point on the level of the confederation, interfacing with the cantons and the system providers. In addition, there could also be a contact point on the cantonal level. However, the cantons and the confederation should then collaborate very closely. If it is indeed a discussion of general interest, the media should be involved. If it is quite a personal	

[6] Netzwoche - Veröffentlichung auf Gitlab, Republik - Postschiff Enterprise

opinion that was expressed, a direct response to the person submitting the feedback should be sufficient.	
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
Yes, via a web-site, run by the confederation.	
4.7	Can security benefit from a PIT the way it was performed? Or a different form of bug bounty? Can public trust benefit from a PIT / bug bounty? Consider the scope restrictions of the PIT (e.g. social engineering, d-DOS, only external attacks) in the federal and cantonal requirements regarding public intrusion tests [5]. Should the restrictions be relaxed? Are there alternative, more appropriate ways to submit the untested elements to public scrutiny? What incentives should be provided to ensure participation?
Yes, I believe that PITs are helpful, also to communicate that the security of the system is handled seriously. If you can even gain something when you identify a problem, even better. I would be rather broad with respect to what I would honour as valuable feedback (from a potentially working social engineering attack up to problems with the crypto). If the code is public source, even potential insider attacks could be found.	
4.8	Is the effective low-scale use of internet voting (the effectively limited electorate provided with voting material that enables internet voting as well as the effectively low fraction of votes submitted through the internet) in combination with an agenda towards more security likely to promote trust? Could a federal regulation to enforce low-scale use of internet voting additionally promote trust?
I would think so. Do I get the question right that it is about keeping Internet voting low-scale indefinitely? If not, it is likely that some people will argue that as long as Internet voting is used in a restricted way, it could be a test bed for slowly learning the system's weaknesses so that an attack is started only when Internet voting is eventually used on a large scale. It is difficult to argue against such odd reasoning.	
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
Difficult for me to answer. Definitely, proofs in reply to universal verifiability should be verified. Possibly, one could charge a specific administrative body with executing elections. Might be costly. If the cantons have qualified staff, using them should be sufficient.	
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?
It shows openness, therefore I am in favour of it. I do not see downsides.	
4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)
It is probably hard to achieve, but I would make whatever is there publicly available. Internet voting is by far not only a technical problem. Anything increasing societal acceptance is a plus. Should one not have published anything that someone else demands, one should make it available – always with the risk that its exploited against Internet voting – in my opinion a risk one should take.	

4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?
My immediate reaction would have been the comparison with other channels, but you mention that anyway. As the fraction of the population using Internet voting could generally be composed of individuals with a particular bias on some topics, deviations of the “Internet electorate” from the “conventional electorate” could be compared with deviations in previous elections to identify a certain consistency, if possible.	

5. Collaboration with science and involvement of the public

Important security findings have reached the internet voting actors not through certification procedures but from actors from the science community, in some cases thanks to voluntary work. This raises the question what measures are appropriate to ensure the participation of the science community to the benefit of security. At the same time, security concerns have increasingly become a matter of public debate. This raises the question how the views and concerns of stakeholders that do not belong to the expert community should be replied to and taken into consideration in the future.

Goals

- Identifying the conditions necessary for institutions from science to participate
- Identifying measures aiming at a stronger involvement of the public

ID	Questions
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g., at implementing the measures currently being defined in the course of the redesign
Experts from science should be free in their participation. They should, for instance, if anything exploitable results from their participation, be entitled to publish their findings, no strings attached. Support for the administration in the course of the trial would certainly be an interesting aspect to increase the participation of scientists, including possibly (if that is permissible) getting students involved.	
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
The only condition I see is that the debate is on an aspect of Internet voting in which the respective scientists have credibility. The expected independence of the scientists could increase societal acceptance.	
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?

Does this questions aim at having scientists as the addressees of the information? If yes, some sort of white paper on the detailed functioning of the voting system could help explain it to a scientific audience.	
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?
Also for the general public, I would see a comprehensive explanation of the entire system to be useful. Here, different from the scientific audience, the representation should be in layman's terms (popular science). A comprehensive popular science presentation of the systems and its verifiability will be quite challenging.	
5.5	Which measures would seem reasonable to get representatives from science and the public involved? In the case of organizing events, who should the organizers be in order to promote trust? • Public debates on selected issues • Hackathons around selected challenges • Others you might think of
Public debates as well as Hackathons seem to be reasonable. They could be organized by the confederation as well as on a cantonal level. If need for additional research should arise, research contracts would get scientists on board. Regarding the general public, regular columns on various aspects of the Internet voting systems in national papers or even covering the topic in TV science shows could increase public involvement.	

6. Risk management and action plan

Structured risk management is an important tool for controlling risks (by consciously accepting them or implementing counter-measures).

The threat landscape is constantly moving and calls for the risk management process to be continuous as well. But too complex a process leads to people not understanding it and ultimately not using it. Therefore, we need to elaborate a process that allows adapting to a moving context while keeping things simple and lean.

So far, the authorization procedure of the Confederation did not allow to take into account counter-measures planned for the future. An action plan could allow the Confederation to issue an authorization depending on the elements of an action plan, in case a risk should be addressed in the medium or long term.

Goals

- Establishing a continuous risk assessment process establishing a concept for assessing risks for the cantons and the supplier
- Drafts for risk assessments and action plan

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
"Classical" risk assessment would require an identification of the assets, a probability estimation of security relevant events, the estimated costs attached to the breach / loss of an asset, the estimated costs of countermeasures, etc. I do not thinks that this applies here. Maybe something similar to	

fault-trees trees (even though faults are in the given context no component failures but “failures” induced by someone e.g. attacking a component of the system or even only the risk that one could attack them) would be applicable or Event Tree Analysis. This would highlight dependence of high-level requirements on low level components. Also for the low-level components, a (comprehensive) list of security assumptions could be derived by such an approach. Intervention would then be triggered by vulnerabilities found that would violate a component’s security assumptions. The severity would then result from the effect the component has on the respective high-level system requirements. (These are first ideas, not fully thought through – they’d need much more reflection.)	
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
Beneficial is the demonstrated transparency as well as the possibility of feedback about overlooked weak points in the risk assessment.	
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
I do not know – sorry!	
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
The measure must address the severity of an identified threat. Severity levels need to be defined.	
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?
As mention earlier, I believe that looking at analysis methods from the safety critical industry could help to a certain extent (e.g. by replacing probability models of circuit failure by probability models of successful attacks against system components).	
6.6	Who can / should support the public administrations of the Confederation or the cantons in its risk assessment (threat modelling, risks identification, etc.)? What could the role of science be?
I believe that science can come up with models that could be beneficial to risk assessment specifically for Internet voting systems. Sometimes it is tough to identify what an appropriate and a not appropriate risk model is for a given context, and it can be hard to evaluate model appropriateness.	
6.7	Some risks can only be assessed in knowledge of implementation details. At the same time, the public administration carries the risks that are in scope here. How should responsibilities be defined to ensure that the relevant aspects are dealt with effectively and credibly? Can the handling of certain issues be outsourced? To whom?
Some assessments would even include knowledge about the software development process. I cannot say to whom, but handling of issues can always be outsourced. Sometimes the responsibility is outsourced with the issue handling. I doubt that this is the case in Internet voting – the administration will always assume the responsibility.	
6.8	Would it be meaningful to have a risk analysis from the canton focusing on the canton’s processes and infrastructure and a separate analysis from the system provider focusing on its processes and infrastructure? How to ensure comprehensiveness and consistency in this set up?
Yes, that would make sense. The canton’s as well as the provider’s analyses both must take into account the interfaces between them (not only technical interfaces but also with respect to how their respective processes interact). The resulting two risk analyses concerning the interfaces would have	

to be checked independently (i.e. by another authority, e.g. by the federal chancellery or someone mandated by the chancellery).	
6.9	Attached to this questionnaire is a proof of concept (as an illustration) of a risk analysis based on the Octave Allegro methodology.[7] Would this methodology be appropriate to handle the risks from the cantons' / system provider's point of view? Do you see any weakness / strong points in this methodology?
I have not found the mentioned proof of concept risk analysis. However, having had a look at the provided link, the Octave Allegro methodology seems to be a valid one for risk assessment, including the case of Internet voting. I believe that it is in the end not only the method that matters, but how thoroughly the assessment is done, and how much time and expertise one is willing to invest into conducting the analysis.	

7. Crisis management and incident response

The Confederation and the cantons have agreed on communication procedures with regard to crisis. Considering the context exposed in the previous chapters, proper response to incidents is a crucial part in internet voting. To promote public confidence, the public administration has to demonstrate that attacks or supposed attacks are handled appropriately and effectively. The moment the election or voting results become official, it must be clear and plausible that the result is correct despite the crisis.

Goals

- Establishing a concept for crisis management
- Identifying the elements that are necessary for incident response

ID	Questions
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
I believe that crisis management should be a centralized task, i.e. it must take place on the level of the confederation. Cantons should also handle crises locally, but be supported by and collaborate closely with the federal administration.	
7.2	What are the right events and thresholds for an activation?
Whenever a certain percentage of the Internet votes seems to be affected (in whatever sense, i.e. rendered impossible by a DoS attack, voters reporting invalid return codes, …), crisis management should be activated. I am unfortunately not in the position to estimate a good threshold value.	
7.3	Who should be involved in crisis management, with which role?
Definitely the confederation, the canton being affected, as well as the system provider.	
7.4	How should the communication be organised (internally and externally)?
There should be a permanent Internet-vote master on the level of the confederation who would be the contact point and match maker in critical situations. Similar Internet-vote masters could be established on the cantonal level.	
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?

[7] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

I am not sufficiently familiar with the concrete tasks of GovCERT, but since it's a CERT it could get involved in particular in not Internet-voting-specific situations (e.g. DoS).	
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
Complete computer forensics examination; identify system components being attacked and trigger detailed analyses of these components.	
7.7	What are the requirements and stakeholders for digital forensics and incident response?
Scientists and institutions with an expertise in computer forensics. Requirements: disclose what incidents have occurred, aim at identifying which vulnerabilities rendered the incidents possible.	
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
It is partly a matter of effort one is willing to invest. Technically, many details of security incidents can retroactively be investigated. I cannot say anything about potential prosecution.	
7.9	How should the validity of election or voting results be handled in case of an incident? Which investigation outcomes or further circumstances could allow or would need to prohibit declaring a voting result as valid?
That will depend strongly on the incident(s). If it is possible that many votes were manipulated, the incident would require a very detailed analysis taking more than just a day. Then the election results should at least be "put on hold" until further facts are available. One would have to define a threshold for the percentage (or total number) of potentially manipulated votes that will trigger further investigations and, depending on the results, a nullification of the election result.	