Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Summary of the replies to the questionnaire

Redesign of Internet Voting Trials in Switzerland 2020

4th May 2020; Version 1.0

Introduction

This document summarizes the answers to the questionnaire and should serve at preparing the further discussions within the dialog. To that end, it highlights the thoughts and arguments that appear to enjoy support. It also contains individual ideas that seem particularly interesting for further discussion.

The document is composed of one summary per question, whereas the answers to the open question "Big Picture" are not summarized here. In some cases, the summaries give an indication of the degree to which arguments seem to be supported. Although we made an effort to be faithful to what seemed to be the relevant message of the authors, keep in mind that simplifications always come at the price of losing content. Also, we cannot exclude that our interpretations may be faulty at times. In order to understand the views of the individual experts, we advise to read the original answers.

If an idea appears to enjoy little support, do not give that too much meaning. Keep in mind that some experts are far more verbose than others, therefore making statements that do not directly reply to the questions. When brought to the discussion, such statements may still find strong support. Further, relevant ideas or arguments to a given question can sometimes be found in the answers to different questions. Such arguments are likely not to be reflected in each appropriate context of the present document. We therefore ask all experts to highlight any thought they find important in the further course of the dialog, independently of the degree of support suggested in this document.

We ask the experts to read the present document as well as the contributions to the first question as a preparation for the discussions.

Chapter 1: Big Picture

This open question is not summarized. Please refer to the original answers.

Chapter 2: Risks and security measures today and tomorrow

2.1 Verifiability

Question 2.1.1: Crypto-Protocol (Part 1) 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?	
Answers	12/15
Summary	The answers do not contain any significant contradictions. Most experts would seem to relate to one of the two nuances: 10/12: • "Building-blocks are unlikely to be flawed, if they are used correctly"; or • "Building-blocks are possibly flawed or likely to be flawed, given that they might not be used correctly." Areas of concern related to wrong usage of building-blocks: • Flawed implementation (this can involve errors in design-documents or code but also bad choices at instantiating from higher-level abstractions or when combining multiple building-blocks): 11/12 • Building-blocks particularly risk being flawed if they are not taken from widely accepted standards and if they are modified: 5/12 • Particularly zero-knowledge proofs (one expert also mentions mix-nets) for voting are complex and generally defined in research-papers and not taken up by widely accepted standards. Due to the generally high abstraction level, important considerations (e.g. setup, surrounding environment) are often not made explicit: 3/12

	• Building blocks or their mode of operation might not address the real-world needs (trust assumptions, attacker capabilities) sufficiently unless carefully chosen: 4/12 • Regarding the real-world needs: Quantum computers or advances in cryptanalysis may at some point subvert the soundness of today's standard building blocks: 3/12 The following risk-limiting measures were proposed: • Involve experts from cryptography at all relevant stages, particularly ensure vast scrutiny: 4/12 • Security proofs and their verification: 4/12 • Formal methods and automated proof-checking reduce the risk of a flawed proof and therefore of a flawed building-block: 3/12 • Closely relate choices to real-world needs, e.g. security proofs need to be checked against these needs: 3/12

Question 2.1.1: Crypto-Protocol (Part 2) How likely does it seem to you that such a flaw could be used for an undetected attack?	
Answers	2/15
Summary	That depends on multiple factors. There were flaws observed in the code released in 2019 that would have allowed undetected attacks, given access to the relevant infra-structure: 2/2

Question 2.1.2: Crypto-Protocol The effectiveness of the protocol also depends on whether it achieves the security goals in the de-fined 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?	
Answers	10/15
Summary	The answers do not contain any significant contradictions. It can be taken from most answers that the complex and nonstandard nature of voting protocols underline or amplify the related conclusions from the question above (2.1.1): 7/10

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 as-signed 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?	
Answers	12/15
Summary	The answers do not contain any significant contradictions.

	• Trusting the printing office at performing critical computations without verification is perceived as problematic, a majority seems to consider it highly problematic. Computations should be avoided or verified: 12/12 • The confidentiality of parameters hinge on whether they are generated based on true randomness. Their appropriate generation in particular should not be subject to mere trust: 3/12 • It is acknowledged that - in terms of the trust-model underlying the cryptographic protocol - the printer has to be trusted at least to the degree that printed values are not divulged. Therefore utmost care needs to be taken at defining the operations around printing: 7/12 • To the same end, solutions could be explored that involve two independent printing services thus requiring only one to be trusted: 2/12 • The trust-assumptions in the printing service are likely to impact the overall public trust in internet voting: 3/12 • Due to its criticality, a governmental printing service might be reasonable: 2/12 • One expert proposes to additionally discuss the trust-assumptions on the postal service with regard to the distribution of the voting material: 1/12 • Also it has been proposed to investigate methods to offer verifiability that do not rely on printed return-codes: 1/12

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?

Answers	13/15
Summary	The answers show different opinions with regard to whether diversity justifies the added complexity: • It is important to run software from different providers in order to limit the impact of a flawed piece of software: 8/13 ○ It has also been mentioned that introducing independent software leads to scrutiny of the underlying system-specification, which increases the chances of detecting flaws: 2/8 • There is another group that acknowledges the added value in running software from different providers, but gives priority to one properly implemented and reviewed software in order to avoid further complexity: 4/13 • Using multiple systems multiply the attack-surface and should therefore be avoided: 1/13

Question 2.1.5 Independence

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?

Answers	13/15
Summary	Most experts refer to their replies to the question above or repeat their statements. The same arguments are basically valid here. One expert points out that the verification software is easier to write than the control-components. Three experts come to a conclusion that differs from the one above. • It is important to run software from different providers in order to limit the impact of a potentially flawed piece of software: 10/13 • There is another group that acknowledges the added value in running software from different providers, but gives priority to one properly implemented and reviewed software in order to avoid further complexity.: 3/13 • Using multiple systems should be avoided: 0/13

Question 2.1.6: Independence

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?

Answers	8/15

Summary	The answers show different opinions with regard to whether diversity justifies the added complexity related to using different operating system and hardware: 6/8
	• It is important or advisable to use different operating systems and hardware in order to limit the impact of a flawed component, despite added complexity: 5/6
	• There is added value in using different operating systems and hardware, but it can be difficult and does not need to be considered a priority: 1/6
	The answers also show different opinions with regard to whether diversity justifies the added complexity related to using different components other than operating system and hardware: 4/8
	• It is important or advisable to ensure diversification of components other than operating system and hardware in order to limit the impact of a flawed component: 3/4
	• The possibilities of diversification of components other than operating system or hardware have their limits. It is conceivable to use shared components across the system to avoid the related difficulties: 1/4
	• Overall, the following components have been mentioned as possible subject to diversification:
	  • Compilers
	  • Java VM
	  • CPU
	  • GPU
	  • Standard libraries embedded in the operating systems
	  • Networking equipment
	  • System management controllers
	  • Peripherals, e.g. disks
	  • Not just different products, but also different vendors

	• Using different operating systems and hardware is less tricky than different application-layer software: 2/8

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?	
Answers	13/15
Summary	• This is a valuable approach. Some experts of this group particularly see opportunities regarding public confidence and achieving more security in the long run: 6/13 • At the same time, long-term privacy risks need to be addressed: 3/6 • No clear assessment. One expert raises concerns regarding the trustworthiness and user-friendliness of the voters' platform, the other one regarding long-term privacy: 2/13 • Not advised, particularly in the absence of a dedicated voter device or if long-term privacy issues are not solved. One expert of this group questions the idea per se of putting the task of verification on the voter: 5/13

Question 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?	
Answers	14/15
Summary	The answers do not contain any significant contradictions. The following practices have been proposed: • Security by design, particularly Microsoft SDL: 2/14 • OWASP Application Security Verification standard, FIPS, or Common Criteria: 1/14 • ISO 9000: 1/14 • Separation of duty: 6/14 • Best practices for deployment; e.g. verifying code using (public) hash / signature: 6/14 • Automated cross-checking and witness-cosigning techniques: 1/14

	• Deterministic build practices as the Debian Linux distribution, use different compilers: 2/14 • Parallel implementations: 2/14 • Ensure transparency and oversight of the whole supply chain and the relevant development processes; the US trusted foundry program was mentioned: 1/14 • Involve highly skilled people from academia and industry at development: 3/14 • Open development: 3/14 • Security testing: 2/14 • Ensure quality of documentation and code; perfect alignment; reduce complexity; scrutiny by publishing: 2/14 • Supervision of developers, traceability of all actions in development and deployment based on unforgeable ledgers: 1/14 • Reduce dependencies on third-party libraries: 1/14 • Apply formal methods and verification (CC EAL 7 was mentioned): 4/14 • Measures to protect the host, in particular by using trusted execution environments to ensure the correct software is running: 3/14 • Supervision by governmental expert group: 2/14 • One expert points out the importance to consider that the abstract specification must reply to the real-world problem. If it fails to do so, all measures to ensure trustworthy implementation and deployment can be rendered obsolete: 1/14

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?	
Answers	13/15

Summary	The answers do not contain any significant contradictions.
	• Threats to be considered
	  • Accidents / human mistakes: 4/13
	  • Social-engineering: 6/13
	  • Planting trojan horse or backdoor: 1/13
	  • Alleged attacks or malfuctions, framing attacks mentioned: 3/13
	• Threat agents to be considered
	  • State attackers: 3/13
	• (Security) objectives to be considered
	  • Trust in voting result: 1/13
	  • User-friendliness: 2/13
	• Weaknesses / assets to be considered
	  • Zero-day vulnerabilities: 1/13
	  • Printing office: 4/13
	  • Postal service (for delivering voting material): 2/13
	  • Ballot paper with regard to privacy (same as 3.1.4 but additionally applied to the objective “Protection of voting secrecy and non-disclosure of early provisional results”): 1/13

	• Risks to be considered (defined by objectives, threats, threat agents, and weaknesses/assets)
	  • 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 (largescale 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.
	  • 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. 2/13
	• Further statements
	  • Insider threats are by far the most underrated threat of e-voting systems. They are covered in the list, however the related counter-measures deserve more insistence (separation of duties, development process).
	  • Threats are difficult to identify generically, they must be identified on the grounds of a given system. Name threats based on basic components and data.
	  • The list of threat-agents should not be limiting. All possible adversaries need to be considered (eavesdroppers, criminals, activists, insiders, parties, nation states,..)
	  • Deserves more focus: 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).
	• Comment FCh: Due to Art. 3 VEIeS, the cantons are in charge of risk-analysis, where the generic list of threats is projected on the specific operations and the system to be used. The generic nature of the list is intentional: It needed to accommodate multiple systems in parallel and, in addition, both verifiable systems and systems without any form of verifiability. One question is how the conclusions from the discussion here should be reflected in the generic list. Another question is what role this list should play in the future (do we still need it? or, on the contrary, would security or trust building benefit from the Confederation taking up more responsibility at risk-analysis?). In any case, the conclusions from the present question will

	need to be taken into consideration when discussing risk-analysis (Chapter 6 of the questionnaire).

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)?	
Answers	9/15

Summary	• The answers do not contain any significant contradictions.
	• These requirements have been pointed out as either missing or insufficiently highlighted:
	  • Controls to ensure that the implementation conforms to the design: 3/9
	  ▪ Design logic (control flow, operations taken, etc.) should be reflected in the code
	  ▪ Ideally the code is formally verified
	  • System needs to be built on well understood and widely accepted security primitives
	  • Controls with regard to simplicity and user-friendliness of voting process, i.e. with regard to checking return codes
	  • Controls with regard to online and offline instructions aiming at return-codes to be checked and individual verifiability to be effective
	  • Communication plan / transparency with respect to the case of allegedly wrong results
	  • Controls to prevent malicious administrators
	  • Trustworthiness of human resources: Consider the risks of espionage / foreign-intervention
	  • Controls with the objective that single points of compromise in the end-to-end voting process be identified and addressed, including humans and in case of components, also their dependencies: 2/9
	  • Forensic readiness
	  • Software Quality Assurance
	  • Requirement 3.3.6 does not state what duration or security level should be taken into account.
	  • Proofs that should be considered substantive as long as there is no doubt about the correct implementation of the underlying crypto and that the trust-assumptions are justifiably fulfilled.
	  • Require software from different vendors for (in terms of the trust-model in chapter 4) trusted components.
	  • ISO27002:2013 §14, §15, §17, §18
	  • Some critical controls from §9 and §12 such as Network Access Control (NAC), authentication, privileged access management, vulnerability management
	  • Hardening of components
	  • §6: segregation of duties
	  • Some controls from §11 (supporting facilities, clear desk, clear screen policies, secure disposal of equipment, etc.)
	• Further comments:

	• The annex refers to an outdated version of ISO27001 • From one comment it became clear that the dependency between chapters 3 and 4 should be made clearer (chapter 4 overrides chapter 3) • Comment FCh: Similar as above, due to Art. 2 and 7 VEleS, the cantons are in charge of ensuring secure and audited internet voting. While chapter 4 is already more specific than chapter 3 of the annex, bringing chapter 3 to a higher level of detail too might at some point cross the line where the Confederation is beginning to specify concrete modes of operation and system features of a (cantonal) internet voting system. This would imply a shift of responsibilities, which in return could impact security or its perception. One question is therefore how the conclusions from the discussion here should be reflected in the requirements of chapter 3 annex, given the current division of responsibilities. Another question is what role this chapter should play in the future (do we still need it? or, on the contrary, would security or trust building benefit from the Confederation taking up more responsibility at defining security measures?). Similar questions will arise when discussing scrutiny (examinations as regulated in Art. 7 VEleS and chapter 5 of the annex are currently left to the cantons) and the other fields of action brought forward in the questionnaire.

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?

Answers	11/15
Summary	The question was in most cases not answered in relation with the requirements of VEleS annex. The experts do point out issues that deserve more attention. Some refer to their previous answers. The answers do not contain any significant contradictions. These aspects have been pointed out specifically: • ISO27002:2013 • 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 • Maximum transparency policy • Trust building: Decentralize the system as to involve the municipalities in the operations • Transparency at performing scrutiny (explain who and how examinations took place) • Security by design • Secure development • Plan for dealing with weak points / errors

	• Coercion and vote-buying deserve more attention • Postal voting should not be used as a benchmark for internet voting security, due to scalability in particular with regard to coercion/vote-buying • Secret-sharing schemes should be used consistently to protect sensitive keys or parameters • Network security; SCION could prevent many attacks (this was mentioned in various contexts and experts) • Source code should be minimal, not contain any dead-code, and include all necessary libraries to build the system • Extend 3.3.5 so all exchanged data is signed • Add stronger controls to 3.15.2 as to guarantee eligibility of voters (comment FCh: Management of electoral register is currently not regulated in conjecture with internet voting) The following requirements from VEleS were mentioned as not having been met: • VEleS annex 4.2.4; 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 • VEleS annex 4.4.2; a single untrustworthy control component would be able to provide a proof of correct mixing and partial decryption that would not be substantive The related findings from the two points above, in conjecture with efforts of the FCh, the cantons and Swiss Post towards more transparency, ultimately led to the ongoing redefinition of the trial-phase and the expert dialog. They are described in these reports: 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. Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. Ceci n'est pas une preuve, 2019. https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf. 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.

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).	
Answers	10/15

Summary	• The cast votes can be protected more effectively: 5/10
	• However, these experts impose one or multiple conditions from this list:
	  • Scrutiny has to be sufficiently effective as to ensure that requirements are fulfilled: 3/5
	  • There is sufficient separation between the trusted components: 1/5
	  • Social engineering attacks on the voter are sufficiently addressed: 1/5
	  • The conclusion does not entail privacy protection on the voters' platform: 1/5

	• The conclusion does not entail protection of data other than the votes, e.g. data revealing whether voters participated or abstained as well as voter registration data may not automatically be considered to enjoy more effective protection : 1/5 • Similar as above, but in the sense of internet voting being at least equally protected: 1/10 • Two experts do not make an assessment, due to the difficulty in comparing internet voting to other fields. They indicate that in internet voting more complicated (and more difficult to put into place) measures from crypto are needed due to weaker trust-assumptions and conflicting requirements (integrity vs. secrecy): 2/10 • One expert uses similar arguments as the two above, which however lead him to a negative conclusion (internet voting data would not offer better protection): 1/10 • Irrelevant question, given that the incentives of an attacker may be very high when internet voting becomes the norm, even strong protection measures may prove to be insufficient (comment FCh: indeed, attacker incentives and capabilities were ruled out from the question): 1/10

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?

Answers	15/15

Summary	The answers cannot be put into relation in a reasonable way due to the diversity of argumentation. The lists contain short summaries or extracts with some kind of judgement or particularly interesting remarks.
	• *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?*
	  • Postal voting is more vulnerable than internet voting to small-scale attacks
	  • Internet voting systems need to be designed to be resilient against attacks from state adversaries
	  • A badly designed internet voting system will allow large-scale manipulation
	  • Internet voting cannot be considered a gain in security due to the increased attack surface
	  • A recent study of the Swiss postal voting process has given a good summary of possible attack vectors in classical paper-based systems. 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.
	  • Internet broadens the threat-space due to scalability of attacks and freedom to act without physical presence

	• E-ID could bring an advantage over traditional voting • With the right design and sufficiently secure implementation and deployment, Internet voting could eventually be much more secure than postal voting. This however requires internet voting not to depend on the postal service to distribute the voting material anymore. • Attacks on internet voting are more likely, also considering that attacks do not have to be successful to spread distrust in the legitimacy of the result. • Internet Voting without independent, verifiable redundancy appears as a loss in security right now. Many problems could stay undetected. • Internet Voting introduces new potential, scalable attacks. Scalability of the attacks is a main concern with Internet Voting. • Influencing the outcome through internet voting is more expensive than other means. • Organizations might want to disrupt society or discredit the government. 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. • 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. • 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. • 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. 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. • 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. • I personally believe postal mail cannot be misused large-scale without being noticed. Therefore evoting could be considered as less secure since it has the potential threat of largescale attacks. Nevertheless, if all the security measures work as intended I'd also trust e-voting. However, to my knowledge also misuse 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. • 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.

- *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?*
  - Swiss political parties, Swiss and international lobbies, foreign intelligence services
  - Benign curious, technically literate voters, domestic participants in the political process (e.g. a political interest group), advanced persistent threats controlled by states.
  - States, or by globally organised interest groups, since attacks require high ressources
  - Limited ressources might be sufficient to spread distrust in the legitimacy of the result.
  - External parties (foreign governments, mafias, . . .) and internal parties (voting system operators, . . .)

- *What methods would they most likely choose? Are there also reasons why they would not apply certain methods?*
  - 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
  - Social engineering is a method likely to be chosen
  - 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 suspicioulsy looking statistics.
  - Overturn verifiability: Compromise printing office and spread malware yielding individual verifiability uneffective, or to the same end benefit from an existing vulnerability in the internet voting system.
  - Attack methods should not be excluded ex-ante
  - Use (hardware) backdoors and purchased vulnerabilities
  - Social engineering and the exploitation of (un)known vulnerabilities
  - 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.
  - 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.

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?

Answers	15/15

Summary	• Yes, it seems reasonable to believe enough voters will follow the procedure. 6/15
	• Some of these experts relate their conclusion to one or multiple of the following ideas or recommendations from the list further down:
	  • P1: 2/6
	  • P2: 2/6
	  • P3: 3/6
	  • P6: 1/6
	  • P13: 1/6
	• Pessimistic, but P3 could help: 1/15
	• Some experts do not give an assessment. One expert is skeptical, whether putting this burden on the voters is reasonable at all: 8/15
	  • P4: 2/8
	  • P5: 3/8
	  • P7-12: 1/8
	• This list summarizes stated ideas or recommendations, independently of any assessment on their effect:
	  • P1: The voting material has to be clear: 2/15
	  • P2: Online user experience needs to be appropriate, one mentions simplicity: 3/15
	  • P3: Ask the voters for an input that they can only give when checking the codes (the following examples were mentioned: The voting card could have a confirmation code per return code, or repeat the code through a different channel, or display multiple codes to the voter and ask him to select the correct one), whereas two experts also acknowledge the extra burden on the voters: 4/15
	  • P4: Awareness campaigns: 2/15
	  • P5: Research / studies on the voters' behavior are necessary to answer this question: 4/15
	  • P6: Be aware that voters might check the first few codes on the top. Voters with wrong codes might believe they did something wrong and therefore be hesitant to expose themselves by calling the administration: 1/15
	  • P7: The notion of "sufficient needs" needs to relate to parameters that are likely to be unknown before the end of a vote: the margin of the actual outcome, the level of public distrust, issued complaints,..: 1/15
	  • P8: The procedure must in any case entail reporting wrong codes to the administration. Just instructing voters to vote by mail when seeing wrong codes beforehand is insufficient as to detect systematic fraud: 1/15

	• P9: The rate of voters who check their codes is one thing. However, even a high rate brings no added value in case an attacker can predict who performs the check and who does not: 1/15 • P10: The entity who receives the reports of wrong codes needs to be trustworthy, i.e. should not risk being suspected of releasing falsified statistics on how many voters usually check/report and how many claims have been made: 1/15 • P11: Measures that would allow voters to seek assistance at verifying (i.e. while respecting the secrecy of the vote) could be explored, Helios, Scantegrity II or Prêt à Voter are references have such features: 1/15 • P12: Checking public boards might motivate more voters to verify, given that the experience would be more natural: 1/15 • P13: Switzerland has a substantial number of individuals who are concerned about e-voting fraud, and would thus perform active verification: 1/15

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?	
Answers	14/15
Summary	• Advising voters to check the TLS-fingerprint is a good approach to prevent PKI-level attacks, given good instructions: 2/14 • Advising voters to check the TLS-fingerprint is unlikely to bring much benefit. Two experts recommend to advise voters to enter the URL correctly and check the padlock symbol. Another expert recommends using SCION to prevent corresponding attacks. One expert notes that the fingerprint or browsers might change on too short notice: 7/14 • A group of experts does not give an assessment. One expert notes that studies are needed in order to estimate the voters' behavior. Another one proposes to ask voters to identify the correct fingerprint between two similar ones. One expert states that all one can do is ask the voters to verify. Another one underlines the value of instructing voters to only use TLS connections (padlock symbol). The same expert advises certificate-pinning, HSTS as well as ensuring that all official websites that link to the system use TLS-connections. One expert is skeptical, whether putting this burden on the voters is reasonable at all. Finally, one expert proposes using external devices to check the domain: 5/14

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?	
Answers	9/15
Summary	• Advising voters to check the correctness of the client application software is a good approach, given good instructions. One expert highlights that the solution

	could involve comparing fingerprints and checking signatures of the downloaded application against a reference. In this case, it would be important to make sure that a group is involved in signing, as to prevent malicious signatures: 2/9 • Advising voters to check the correctness of the client application is unlikely to bring much benefit. One expert states that the solution would be too difficult: 1/9 • A group of experts do not give an assessment. One expert states that a multitude of applications could be proposed, each one endorsed by different organizations. Another expert states that little can be done apart from installing browser extensions/plug-ins or external devices. Yet another one says voters should not be required to install any heavy weight applications. One expert notes that studies are needed in order to estimate the voters' behavior. Information campaigns and asking voters to verify is repeated from the statements to the previous questions. One expert is skeptical, whether putting this burden on the voters is reasonable at all. Finally, one expert states that trusted execution environments would be needed to obtain strong properties in this space (SGX or TrustZone on ARM devices): 6/9

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.	
Answers	8/15
Summary	• Most experts do not see a threat to integrity in the coming years. However, privacy deserves attention, given that data could be collected today and evaluated later, as four experts highlight. One expert notes that one must always assume that the encrypted votes might leak. Two experts highlight that breaking voter privacy would require to establish a link to the voter. This could be managed by withholding the personal data of the voters, that however would have to be done in an effective way: 6/8 • It is unclear whether quantum computers will exist in the near future or if they already exist. Therefore, it is not possible to determine when a post-quantum cryptographic redesign is necessary: 1/8 • Cryptographic schemes that offer resilience against quantum computers are being researched. These developments should be taken into consideration for the future. Three experts imply either that they are not sufficiently matured yet or complicated to implement. Three experts seem to recommend to first get it right with conventional cryptography: 6/8

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?	
Answers	13/15
Summary	• These measures make sense. However, almost all experts point out that they do not eliminate the risks related to corrupted voter platforms. Particularly, resourceful attackers must be considered to be capable of circumventing these measures.

	Two experts explicitly doubt that many will follow the guidelines. One expert sees general public information campaigns on cybersecurity more promising than election-related instructions. One expert highlights that trusted execution environments such as SGX would offer security even in the presence of malware. Another expert highlights that code-voting (each choice on the ballot is expressed by entering a distinct code) would remedy the problem, at the cost of usability: 12/13 • One expert did not assess the MELANI-guidelines, but brought to attention that rates of malware infection can be high: 1/13

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?	
Answers	15/15
Summary	• The risks are not or not much higher with internet voting. One expert clearly highlights the scalability of vote-buying in the absence of a resilient voting protocol. However, he locates the parameters as to whether vote-buying happens rather in societal than technical aspects: 7/15 • The risk is higher with internet voting, mainly due to anonymity and increased scalable technical feasibility: 8/15

Chapter 3: Independent examinations

Question 3.1 Which criteria should determine which persons or organizations are mandated with an exam- ination? 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 ducted by certification bodies seem reasonable?	
Answers	14/15

Summary	Criteria:
	• The most cited criteria are expertise and experience. For scopes related to crypto the examiners should be academics. One expert notes that for standards based examinations they should be approved by a standardization body. Independence is also mentioned, as in independence from each other, from companies having a stake in e-voting and from the Cantons and the Confederation.
	• Following scopes are mentioned:
	  • ISO 27000
	  • Proofs of protocol/Crypto
	  • Model vs design
	  • Implementation vs design
	  • Crypto source code
	  • Software
	  • CC is not relevant
	  • limit to key components, do not overburden
	Formal certification:

	• Most experts did not mention this topic in their answer. Those who did either agreed that formal certification was useful for the ISO 27k scope or stated that they are not convinced by standardized certifications.

Question 3.2	
In case measures that reply to security requirements from the VEIeS 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.	
Answers	14/15
Summary	There seem to be three different opinions on this subject: 1. Insufficiencies could be acceptable if risks and mitigations are analyzed from case to case. (6) 2. Insufficiencies could be acceptable after careful analysis but only if they do not relate to critical subjects: e.g. verifiability or conformance to Common Criteria. (2) 3. Systems with known defects should not be used because of the following reasons (6) a. it is difficult to assess the impact, b. it undermines trust, c. it would generate strong reactions of the public.

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).	
Answers	15/15
Summary	All experts who gave an answer noted that the credibility depends on who appoints the examination. They all agree that there should be different organizations for the different scopes and that they should be appointed by the government or an independent committee. The big four are explicitly excluded by one expert.

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?	
Answers	9/15
Summary	None of the experts did mention or comment on the six scopes listed in the annex of the ordinance. Although different terms are used, there are basically three scopes that are mentioned in the answers: • examination of proof of design (crypto) • examination that the model represents the design (specification) • examination that the implementation conforms to the design (code) Standards other than the ones already in the VEIeS are:

	• the “Voluntary Voting System Guidelines” (VVSG) by The U.S. Election Assistance Commission (EAC) • the Council of Europe recommendation on E-Voting. Some experts think that standards are too general and doing a checklist based certification is not useful. One opinion is that there should be continuous review rather than an examination (which is an opinion that is shared by other experts in Q 3.6)

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?	
Answers	13/15
Summary	There is an agreement that there should be an examination after significant changes. Following default intervals are given: • cryptography: every 5 years • processes: every 3 years • overall audit every year • continuous scan of infrastructure Again, some experts think that examination should be continuous.

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?	
Answers	15/15
Summary	How the experts should be involved: All information should be available to independent experts to carry out their examination. There should be bug bounties to motivate these experts. At which stage they should be involved: * as early as possible or at least before the examination (3) * during the examination (2) * after the examination, to be able to fix first issues (2) * the independent examinations should be continuous (3) When should their results be published: * two experts explicitly state that publishing of the results could be delayed, to protect an ongoing election or to let a panel of experts analyze the results. Some reasons cited for not publishing the results immediately are • to protect an ongoing election • to let a panel of experts analyze the results

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

Answers	11/15
Summary	The few explicit answers all point towards the Federal or cantonal authorities as responsible for handling differing opinions.

Chapter 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?

Answers	12/15
Summary	Several researchers talked about the Public Intrusion Test (PIT) instead of the source code publication (which ran as a separate project). Some of these responses can be read from a source code perspective as well. Some can't. They are listed and quoted under "No answer" and taken into consideration in question 4.7 again. Of those responses that really answered to the source code publication, a large group would like to see a transparent development process adopted. This would mean that all commits to the source code are visible; potentially in a slightly consolidated way. This does not necessarily mean that the result is software published under an open source license. Enforcing such a license is not very important for the experts. They just want to see the development of the code and they welcome a development model where the interested audience is welcome to submit criticism and proposals. A second group of similar size does not touch on the development model, but they want to see a broad publication of the source code with as few restrictions as possible. Many experts touch on the question of intellectual property rights. However, for almost all of them the need for maximum transparency has more weight. Several experts estimate it very unlikely that a competitor would steal the code or they mention methods to make it even more unlikely. One expert explains that specific parts of the source code might only be made available after registration and proof of qualification. Some individual interesting ideas: • 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.

Question 4.2

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

Answers	15/15
Summary	There is a clear majority opting to publish as much as possible so experts in different areas find everything they need to assess the system. Documents mentioned are all specifications, anything that could help auditors and every document that would be given to a developer or maintainer of a system.

	One expert goes as far as to demand the publication of all mandated examination reports. It is unclear if the other experts did not think in this direction or if this is an individual position. Another one stated the same in response to 4.7. Minority positions include some who opt to make some documentation available on demand; another one who would like to delegate the definition of the scope to a new-formed body or committee and a last one who thinks the publication can be limited to the E-Voting system and additional operational documentation can be withheld. Some individual interesting ideas: • 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. • 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. • 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. • The new committee can develop such guidelines and a needs basis.

Question 4.3 When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?	
Answers	13/15
Summary	There are two strong groups present here. One group would like to see the code and the documentation very early and regularly updated in a continuous process. The second group would prefer thorough testing and possibly a certification before the publication. The question about the indicator was not directly answered by anybody, however, indicators like "integration tests are complete" can be read as an answer to this question. One expert sees a reputation damage when too many silly errors are published. Another one is afraid that a code review can not be done on a moving target. This problem is not mentioned by other cryptographers and it may seem solvable if the review happens on tagged versions / release. Some individual interesting ideas: • In order for the publication to achieve the “transparency” objectives, the published code and documentation should correspond to the “production-ready” version. • 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. • This depends in part on the complexity of the system. The more complex a system is, the more time it takes to check it. • This is impossible too if the system is still undergoing change. • Involve citizens somehow. Citizen Science namely for code verification. • The new body can develop such guidelines and a needs basis.

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)	
Answers	11/15
Summary	There is unanimous consent that interested researchers need to be able to setup a complete election based on the published code, test data and accompanying documentation. One expert suggests to also provide preconfigured virtual machines so that researchers can save time.

Question 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?	
Answers	15/15
Summary	There is a strong and diverse call for a committee involving various experts responding to the public reactions. Which organization should appoint the committee is not discussed in detail. The question, namely the first part of the question, was read differently by different experts. So the responses stretch from public reactions in the form of software weaknesses identified, or more general reactions by the public. Therefore the responses are also quite diverse and the committee is either very operational with discussing every individual bug report - or it is a more general advisory board that discusses reactions, assesses problems and addresses the wider public with documents. Also, it is not entirely clear if said committee should give advice or have the power to stop an online voting system. What is clear is that all responses have to be transparent and made public; possibly after a certain delay. Minority opinions do not discuss a committee but rather emphasize the Federal Chancellery with regard to a technical lead position, they think reactions should generally be public by default or they read the question completely differently. Some individual interesting ideas: • 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 Confederation that authorizes the system. • 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. • Regular events can be held where questions from the public are discussed. Anyone can attend and participate in the discussion under certain rules. • 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). • It is worth exploring how a citizen science initiative could be involved in the process.

	• 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. • The Federal 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. • For each major release I suggest holding a press conference and then a technical discussion with independent experts. • I feel that this is a question for Swiss administrators. My main suggestion is to think about the incentives of all people involved.

Question 4.6 Should the system providers publish existing / fixed security breaches? Through which channels? When?	
Answers	14/15
Summary	There is a very clear majority insisting on full transparency of every security-related fix. Most experts opt to use a standard public development platform such as github / gitlab and use that as a publication channel. Most experts agree that security fixes are best published when the system has been patched (referring to an evolving industry best practice of a maximum delay of 3 months after the report). However several experts mention that this may be impractical in the e-Voting context. A few experts discuss the problems with security vulnerabilities reported during an ongoing vote. Another one, representing a minority position, opts to delegate this question to the committee that ought to be formed. Some individual interesting ideas: • Establishment of guidelines by the new body

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?	
Answers	14/15
Summary	There is agreement that penetration tests and bug bounty programs complement each other. Mandated Pen-Test first, Bug bounty afterwards. There is a strong group of experts that see a lot of value in making it a permanent program, also because it would then be part of the normal security posture of the service and not a one-time happening.

	A qualified majority of the experts think that restrictions should be dropped, maybe completely. A minority sees a bug bounty extending to ddos and social engineering as unpractical and resulting in harassment of employees of the system provider. Alternative tests that also cover these areas (ddos and social engineering are mentioned by many experts) can be done in the form of mandated penetration tests with subsequent publication of the results (a credible Pen-Test report that covers DDoS in detail removes the pressure to include DDoS in the bug bounty program). A second option is to add smaller focused programs that include qualified bug bounty hunters (maybe some who have proven their quality in the main program) and invite them to conduct DDoS and social engineering tests in a controlled environment. Two experts opt to give bounty hunters access to the backend systems as part of such a focused test. A hackathon has been mentioned as well. One expert states that the bounties must be much larger. He also proposes an insurance model that could keep the budget relatively low but still guarantee large payouts ("Hydra framework"), thus setting the incentives in a way that all findings are reported. Question 4.1 was also answered with the PIT in mind by many experts. One wants to put the Federal Chancellery in charge in the bug bounty, the other experts did not touch on this question. The other responses in 4.1 confirm the conclusions drawn in this section of 4.7.

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?	
Answers	14/15
Summary	Most experts see a limit to the electorate as a risk-limiting practice, that makes an attack less attractive. But of course there are very tight elections sometimes. When it comes to trust, there are two groups of similar strength among the experts. One group thinks that this limitation will not affect trust at all - possibly even reduce it as it clearly signals the system is not considered trustworthy. (7) The 2nd group thinks that low scale use will help to promote acceptance and trust in the long run. (5) Two experts have minority positions. They do not think there is any merit in limiting the electorate. This minority position is significant as both experts represent the small group of politologist among the experts. Summing things up, there are two strong groups here that disagree. Some individual interesting ideas: • 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. • 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.

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)?	
Answers	12/15
Summary	For the vast majority of the experts, this boils down to a question of transparency. Several experts connect the question with the need for a public bulletin board or at least with a publication of proofs that resemble a public bulletin board. Two experts ask to revisit this question even if it puts the secrecy of the vote in peril, namely in the post quantum world. One touches on this as the "ultimate tool" in their answer for 4.10, but also name it "not a conceivable option" due to the long term privacy problem. In the absence of a public bulletin board, some form of public ceremony seems a viable perspective for many experts. (8) Some of them would also like to align the tallying and verification process with existing processes for physical voting, thus "bootstrapping" on established trust. Two would like to see various verifiers, even a diverse open source market for those auditing tools in the case of one of them. (2) None of the experts touches on the problem that a third party verifier could fail and put a big question mark on the validity of the results of an election. One expert explains the underlying problem with counting and auditing the result and the need for trustworthy evidence in detail. Some individual interesting ideas: • Given the high complexity of e-voting systems, the Confederation and industry should support the cantons as much as possible, to reduce replication of effort by the cantons to a minimum.

Question 4.10 Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?	
Answers	12/15
Summary	Outside of a minority position, everybody agrees that the electronic voting shares should be published - have to be published in the words of several experts. For most of the experts this is about transparency and trust. Two experts see a different benefit: It would allow to discover bugs and accidental errors in the system. They quote an example where the name of a candidate was not displayed properly on some devices, which became visible in the electronic voting shares. One expert extends the idea of publishing electronic voting shares and adds additional proofs and evidence. This brings problems, but he has a clear, if fairly advanced plan, how to implement a scheme that does not open huge privacy issues. Some experts see a potential privacy problem, but transparency is more important for them. Most experts assume that electronic and physical voting channels will bring different results for sociocultural reasons which may lead to discussions. These are the downsides that are named consistently by many experts.

	Downsides: • 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... • ... important to consider carefully the tradeoffs between public verifiability and long-term vote privacy, ... • 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. • 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. • 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. • 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 • I don’t see any problem publishing as much details about the votations as possible as long privacy is not affected.

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.)	
Answers	12/15
Summary	The publication of detailed reports about infrastructure and other audit reports, possible at the moment of the vote / the publication of the results is seen as a measure that promotes trust. However, there are downsides to the publication as well. The common ground here is that the publication has to be of very high quality. Bad reports will undermine instead of supporting the trust. If published, the targets of the documents need to be clear. Detailed technical information should be addressed to the technically interested parties. There is also a call for a public bulletin board among the responses of the experts. Other ideas include a strong formal function for existing roles like "Stimmenzähler" (vote counter) and "Wahlbeobachter" (election observer) which give authority to the results and brings witness co-signing with it. One of the experts calls for an education initiative. He also thinks that the system should not be operated by a privately held company. Another expert does not really address this question, but he asks for strong infrastructure protection with IDS / WAF (he implies WAF, but does not mention it) as a deterrent.

	Some individual interesting ideas: • ... 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). • ... 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 • 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. • 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. • 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. • 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. • 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. • 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. • Publication of the content and results of system inspections by independent experts at election time would probably help as well. • 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. • 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.

	• 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.

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?	
Answers	14/15
Summary	Many experts see the plausibility checks as a technique that is very close to the risk limiting audits that are known to detect election fraud. However, one expert has ruled them out in the specific Swiss case because there is no paper trail to base them upon. Other experts see risk limiting audits as an option. No expert really named a plausibility check method like the question asked. The statistical plausibility checks are given less value because different voting shares are expected on the electronic channel. Most experts think that such a difference between the channels destroys the option to detect fraud that way. However, no expert explained how an attacker would be able to model the fraud without knowing the results of said voting districts in advance. Also there is no mentioning of experience with the results and the role of politologists interpreting the voting shares and making sense of the plausibility checks and thus establishing a definition which divergence is acceptable / explainable and where fraud would start. There is a minority position who thinks that these plausibility checks should only be for internal use, since there is a big risk to get the fine line between false positive and false negative wrong. One expert makes it very clear that plausibility checks can never be used as evidence, only as marker where to look. Some individual interesting ideas: • 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. 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. • ... 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

Chapter 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

Answers	14/15
Summary	1. For participation in «public scrutiny» there is an agreement that access to documentation and code as well as the possibility to publish the results are important. Some additional ideas are to organize workshops, found research or give bug bounties. 2. Examinations are clearly seen as a job that must be paid for. Some experts suggests creating a committee or testing institute to manage examinations. 3. This work is also seen as having to be paid for. One proposal is to involve a random group of voters. Creating a European network of experts was also suggested in general.

Question 5.2

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

Answers	15/15
Summary	Most experts agree that scientists are not motivated by political discussion. Some might be motivated, based on their personal opinions. Having an open debate with “few hurdles” may be a motivating factor. One expert noted that if research was funded, then participation to political debates could be asked in return.

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?

Answers	13/15
Summary	There are many different inputs here. Information should be high-level, simple, possibly in the shape of tweets, blogs or videos. Using mainstream media rather than specialized events. Communication experts could help, also a citizen-science approach. Publishing a simulator of all parts of the system could also help. The information should come from the Federal Chancellery or a specific committee.

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?	
Answers	14/15
Summary	The experts agree that there should be different levels of details depending on the audience. Then they give different inputs: • Use consistent terminology across levels. • Involve the local authorities for informing the voters • Publish all documentation, code, ... • Wait for the system to become trustworthy before promoting trust • There is already enough simple information, including videos. More will not make a difference • Do not promote trust, promote accurate public assessment instead.

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	
Answers	14/15
Summary	All experts seem to find public debates and hackathons useful. They have following interesting remarks: On scientific events: • Revive events like the Swiss e-voting Workshops • Create a dedicated track at a regular conference • Set up a scientific seminar Other types of events: • Citizen-Science approach, e.g. for statistical tests • Decentralized events to let local voters see or touch the system • Debates on mainstream media • Intrusion test events, like the Defcon voting village Words of caution: • Beware that the topics of debates are subtle and finely nuanced, since there is always a residual risk. • Trust should be promoted once there is a consensus on the trustworthiness of the system • Be completely transparent • Involve experts early and continuously (not just tests of the final system) • Also consider events happening in the world • There will always be skeptics and conspiracy theorists. Do not invest energy fighting them.

	The organizers should be either the Federal Chancellery, the Cantons or local administration.

Chapter 6: Risk management and action plan

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?	
Answers	11/15

Summary	• All experts agree on a continuous / regular (yearly or bi-yearly) assessment of the risks.
	• 4/11 think that the risk assessment has to be updated before every ballot as threats might change depending on the content of the ballot.
	• 3/11 think that it should be updated with (major) system change.
	• Though there is no consensus about it, input for this assessment could come from:
	  • Science
	  • (Security) events
	  • Federal entities
	  • Public
	  • Other countries
	• 2/11 recommend that a specific (scientific) body created to accompany e-voting activities takes the lead for the risk assessment.
	• Some individual interesting ideas:
	  • Publish the risks on a webpage to allow the public to review it and submit new ideas
	  • Having an independent authority providing the risk analysis and then having the risk assessment done by the system provider and cantons based on it.
	  • Consider conflict of interest when assigning responsibilities for doing the risk assessment

Question 6.2: What are the benefits and downsides of publishing the (dynamic) risk assessment?	
Answers	10/15

Summary	• Benefits:
	  • 6/10 Trust building
	  • 3/10 Increased transparency
	  • 3/10 Public involvement
	  • 1/10 Allow wise decision (face the truth)
	• Downsides
	  • 6/10 Reveal weaknesses
	  • 3/10 Brings controversy
	• Half of the experts declare that they are in favor of publishing the risk assessment as long as it does not endanger the vote.

	• Some individual interesting ideas:
	  • The risk of revealing weaknesses is unfounded, as the adversary already knows about them.
	  • Make a distinction between operational risk assessment and overall risk assessment of the system, which should be published.

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?	
Answers	6/15
Summary	Half of the experts think it is a tricky problem that the cantons might not be able to handle. Most of the proposed solutions fall under ISO 27002 controls (contractual clauses, penalties, criteria for choosing a provider, careful planning and verification of the deliveries). Some individual interesting ideas: • Cantons build and operate their own system • Modularize system with different providers • Redundant infrastructure through national datacenters • "chip-x-ray" system developed by PSI for checking hardware

Question 6.4 Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?	
Answers	7/15

Summary	• 3/7 Criticality
	• 3/7 Urgency
	• 3/7 Feasibility
	• 2/7 Effort (Cost) / Benefit (Risk reduction, effect on trust)
	• 2/7 Impact
	• Some individual interesting ideas:
	  • Prioritization is useless, each and every action has to be implemented
	  • One mentioned minimization of negative impact on public trust as objective, as another one mentioned maximization of public trust

Question 6.5 To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?	
Answers	5/15

Summary	• Standard methodologies:
	  • 2/5 ISO 27005
	  • 2/5 NIST standards
	  • 1/5 OCTAVE Allegro
	  • 1/5 BSI Grundschutzhandbuch

	• 1/5 EU Risk assessment methodologies for Critical Infrastructure Protection
	• Two experts mentioned that the benefit in using standards comes from having a structured and comprehensive way of analyzing assets, threats, vulnerabilities and risks.
	• Some individual interesting ideas:
	  • The quality of the risk analysis depends on the quality of those performing it
	  • Systematic testing and review is necessary

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?	
Answers	11/15

Summary	• 8/11 see a committee of experts as a good body to support the risk assessment process. However, the composition of such a body differs across experts:
	  • 7/11 Science representatives (research groups, teacher, Risk Center ETH)
	  • 6/11 Consultants (security, usability, software, statistics, economy, insurance)
	  • 2/11 Federal agencies
	  • 2/11 Election officials from cantons
	• 3/11 propose to assign different roles to the different kinds of experts. Scientist should take care of conceptual and technical aspects while consultants should take care of the concrete risk assessments, possibly with the help of federal agencies for threats and risks identification.
	• Some individual interesting ideas:
	  • The risk assessment process looks like a relevant subject for PhD theses, that could be run in collaboration with the Confederation
	  • 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

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?	
Answers	6/15
Summary	Three solutions emerge here though no consensus exists: • The Confederation, in collaboration with the different stakeholders, issues a core security concept that inventories threats, proposes mitigation controls in a comprehensive manner and defines the responsibilities for implementation. • As this task needs sovereign capabilities, the cantons are responsible for it. They can however get help from outside if they lack the competencies. (status quo) • The committee of experts is in charge

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?	
Answers	8/15

Summary	• Half of the experts says that the splitting could be done but in a different way. The idea would be to have a group (Confederation, cantons, providers, external experts) defining a neutral risk concept. The practical risk assessment, by the canton and/or operator, would then focus on residual risks specific to their organization and the implementation of the controls and its effectiveness.
	• A quarter of the experts mention that splitting the risk analysis could pose problems because, in general, security does not compose well. The risks of two systems taken separately do not cover the interactions between the systems. Some kind of additional analysis would be needed to identify new risks that come from these interactions.
	• Some individual interesting ideas:
	  • Only one risk analysis by the cantons
	  • Risks for each canton should be considered in one forum

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.1 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?	
Answers	5/15

Summary	• 3 are in favor of the methodology, 2 are against it.
	• Strengths:
	  • Recognized as a straightforward, pragmatic and popular methodology for IT risk management
	  • Clear and objective
	  • Lightweight and easy to use
	  • Treats technology as well as people
	• Weaknesses:
	  • Absence of links between threats and controls
	  • Too lightweight
	  • Will likely miss subtleties arising from the particular adversary model and problems in the actual implementation or configuration
	  • Scope rather different from that of an e-voting platform as it is designed to assess information security risks within a large organization
	• Some individual interesting ideas:
	  • Develop an individual e-voting risk assessment tool
	  • Use a catalogue of generic threats mapped with 27002 controls
	  • Methodology is not critical in the process of securing a system

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

Chapter 7: Crisis management and incident response

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?	
Answers	9/15

Summary	• Mentioned key elements are:
	  • 6/9 Defined processes (encompassing detection of attacks, termination of attacks, assessment of the damages and impact on results, recovery, communication and prevention)
	  • 4/9 Action and communication plans must be ready beforehand
	  • 3/9 Dedicated team
	  • 2/9 Direct links with e-voting actors
	  • 2/9 Links with feds (GovCERT, MELANI, ChF, NDB) possibly also private companies
	• A third of the experts highlights the key role of detection of an attack in crisis management and one of them proposes to set up a monitoring that includes what is happening within the network and servers, feedback from the voters (e.g., lack of access or individual verifiability checks failed) and feedback from election auditors.
	  • Some individual interesting ideas:
	  • Get advice from others (e.g. BAG, FCh's e Strategic Management Support Section)
	  • Do not forget the political aspect of the crisis
	  • Inform voters ongoing instead of after the vote
	  • Review the plans for every election
	  • There may be a serious incident without anything obviously having gone wrong, which is precisely what verification is meant to prevent

Question 7.2 What are the right events and thresholds for an activation?	
Answers	7/15
Summary	There is no consensus on this question. The only idea that is shared among experts is that one has to consider events that could have an impact on the results. The proposed events can be part of 3 categories: • Evidence of errors • Evidence of malfeasance • Evidence of significant public concerns And the sources for those events could be but not limited to: • The internet voting hotline • Secret service or cybersecurity firm • Monitoring at the canton/system provider (system log files, physical access log file, behavior of employees, server integrity checks, etc.) Some individual interesting ideas: • All irregularities should be communicated

	• 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). • The definition prepared beforehand includes a reflection on which incidents are considered as "benign" and can be ignored or handled 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

Question 7.3 Who should be involved in crisis management, with which role?	
Answers	6/15
Summary	Here again, no consensus except that there should be a defined group with broad competencies (e.g. technique, communication, voters' behavior expertise, official representation). The group could consist of: • 2/6 Federal chancellery • 2/6 Cantons • 2/6 System provider / operator • 2/6 Communication expert (could come from cantons and/or Fch) • 2/6 Independent technical expert 2/6 experts propose to have the Federal chancellery leading this group and the system provider/operator for monitoring their systems and people and investigating. Some individual interesting ideas: • The independent technical actor is responsible for validating or challenging the results of this investigation (and thus prevent any conflict of interests). • There should be liaisons people, for example to the Swiss telecommunication service, GovCert, and the cybersecurity office of the government/military, etc. • There should be a national voting expert, who can frame and explain a voter's reactions.

Question 7.4 How should the communication be organised (internally and externally)?	
Answers	5/15
Summary	3/5 experts plead for a quick and transparent communication to the public in case of an incident. 2/5 experts think that the external communication should occur through the cantonal authorities. Regarding communication inside of the crisis team, one recommends that they are collocated and another one that clear communication channels are established with frequent update on the situation. Both are pursuing a common understanding and vision of the situation. Some individual interesting ideas: • Technical communication must be distinguished from public communication • For external communication, it is recommended to employ a communication expert, who can explain the problems that occurred in a greater political context

Question 7.5 Are there already structures that should be involved in crisis management (e.g. GovCERT)?	
Answers	4/15
Summary	All experts that have answered this question are clearly or somewhat in favor of the involvement of such entities. GovCERT, MELANI could be involved. Some individual interesting ideas: • A few identified private companies capable of providing expertise and/or manpower could be on the stakeholders' list. For this last category, it could be interesting to assess the possibility of relying on existing organisms like Swiss Cyber Experts (SCE). • Governments often have intrusion detection systems integrated into the national network. The US, for example, uses a Suricata based Alert sensor system.

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?	
Answers	6/15
Summary	Investigation has not been understood in the same way by all experts. A third of them recommend leaving it to the police. However, apparently, for the police to be involved, one would have to fill in a complaint, which cannot be done for each incident. The other two thirds have understood investigation of incident in a broader way, which is what was meant in the question. 3/6 experts propose the following structure for investigating an incident: • Identification / Detection • Containment / Eradication / Termination • Recovery / Impact assessment • Lessons learned 3/6 experts recommend involving external experts specialized in the area. Some individual interesting ideas: • 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. • If the audit fails, then, incident investigation will become an important part of the election • 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. • 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 FCh.

Question 7.7

What are the requirements and stakeholders for digital forensics and incident response?	
Answers	4/15
Summary	Half of the experts mention the need to have a system designed for digital forensics, notably tools and immutable logs. The logs could be secured by a blockchain technology or other crypto methods like Merkle trees. The tools should be available to efficiently identify, authenticate, classify, analyze, integrate, interpret and evaluate digital traces. Some individual interesting ideas: • 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. • It may be required to establish partnerships with private companies that would be capable of assisting in the investigations. They are to be trained on the solution. • A system that is designed for digital forensics 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. • If the servers are out of the jurisdictions of the Swiss police it may be very difficult to collect the information

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?	
Answers	5/15
Summary	2/5 experts write that while investigation is something achievable, prosecution is quite complex and depends on external factors (e.g. international cooperation and laws). Some individual interesting ideas: • 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. • Experts in crisis management must be involved and available at any time, particularly during a voting period. • 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).

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?	
Answers	8/15
Summary	5/8 experts mention that the validity of the results depends on the impact the attack had on them. The interpretation of results here is not clear. It could be the exact count of

	votes for an option or another or the outcome of the vote (acceptance or refusal of a proposition or the elected person). If one choses the first interpretation, the result is only valid if the investigation can prove that the count has not been altered. With the second interpretation, the result is only valid if the investigation (which is to be done at least if the share of internet voting votes is big enough to change the outcome) can prove that the outcome would not have changed even if votes have been altered. The latter interpretation seems to be the most widely shared. 2/8 experts write that this is a political question that needs deliberation and acceptance by all stakeholders. Some individual interesting ideas: • The trustworthiness of the system can be measured by how trusted/accepted its remediation processes are. If they are politically accepted, the system is trustworthy enough for the democratic electorate, if not, it should not be used, as it cannot settle political conflict. • 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. • It would be good to integrate the robustness to failure and recovery into the voting system. • If auditing the evidence succeeds, then the result is valid. • Ideally, the VEIeS should state exactly what has to happen in each case of incident/failure. • 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. One therefore circumvent a paralyzed government that relies on the courts to determine the election result in the case of an incident.