Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

Political Rights Section

Redesign of Internet Voting Trials in Switzerland 2020

Instructions for the questionnaire

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

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

Material

Federal legislation:

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

[2] Federal Chancellery Ordinance on Electronic Voting VEleS

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

Information of the Federal Chancellery:

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

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

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

Information of Swiss Post:

[7] Documentation and reports

[8] Explanations

Redesign of Internet Voting Trials in Switzerland 2020

Questionnaire for Workshop 1

First name		**Last name**	
Organization			

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

1. Big picture

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

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

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

[2] https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html
https://www.bk.admin.ch/bk/en/home/dokumentation/medienmitteilungen.msg-id-74508.html

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

2. Risks and security measures today and tomorrow

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

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

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

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

Goals

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

2.1 Verifiability

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

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

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?
2.1.5	Similarly for «the auditors' technical aid» that is used to verify the proofs underlying universal verifiability (sometimes called «verifier»): How do you assess the added value and downsides of running software on the auditors' technical aid that was written by a different provider than the one of the voting system?
2.1.6	The VEleS requires operating systems and hardware to differ. As how relevant do you consider operating systems and hardware to differ? (In comparison to the application layer software?) Do you see any other machine components that could constitute a significant risk in case they do not differ across control components / auditors' technical aids? How do you assess independence created by separating duties at operating control-components and auditors' technical aids? How far could separation of duties go? What are the downsides?
2.1.7	**Other forms of verifiability** The trust model was defined under the assumption that the voters' computers should not be trusted with regard to manipulations of votes. At the same time, user-friendliness was a strong concern. This is why voting with return-codes was chosen. By assuming that voters have a device they trust, the remaining trust assumptions could be additionally relaxed: For instance voters could post and confirm their vote on a public bulletin board and also verify the proof allowing universal verifiability. Or they could send a signed digest of their vote to an electoral commission that checks that the encrypted vote has been recorded as cast, i.e. that the vote passed to the tally. How do you assess the added value and downsides of an additional verifiability service based on a device trusted by the voter, given that voters would need to transfer and evaluate cryptographic values using different equipment in order to benefit from individual and universal verifiability? Considering a solution where votes are posted to a public bulletin board, how do you asses long-term privacy issues?
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?

2.2 Security related risks top-down

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

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

2.3 Selected risks

ID	Questions
2.3.1	Individual verifiability should allow voters to detect manipulations and, in case they have doubts, to choose another voting channel. Individual verifiability is also meant to allow the cantons to detect systematic fraud. This however hinges on the number of voters who check their return-codes and report observations that could imply a manipulation (i.e. a return code not being displayed or being displayed incorrectly). Does it seem reasonable to believe that a sufficient number of voters will be capable of checking the codes according to instructions delivered in the voting material and to inform the administration in charge in case a code is not displayed or displayed incorrectly? What measures could be taken in order to maximize the number of voters who check their codes?
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?
2.3.3	The voters must be given the possibility to verify that their client application is correct, i.e. that the correct encryption key is applied (the effectiveness of individual verifiability does not hinge on the correctness of the client application). This is to address the case where the client application is tampered with on the server side. Which measures could meet this requirement in an effective way and what are the downsides? What measures could be taken in order to maximize the number of voters who check that they are running the correct client application?
2.3.4	How, if at all, do you think the developments in the area of quantum-computing should be addressed? Who / which organizations will be able to use these computers if anyone ever? When do you expect quantum computing to become relevant? Assume that encryption and soundness of proofs and must hold for months (the latter with regard to premature results being known), the secrecy of the vote (which person voted how) should at least last for decades. Regarding the secrecy of the vote you may assume that no personal voter data (i.e. names) is transmitted through the internet.
2.3.5	The voters' platforms hold the votes in plaintext. In some cases in the past, voters were instructed to use a platform they trust to cast their vote. To what degree can

	voters influence their level of protection from malware, e.g. by following the guidelines from MELANI[4]?
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?

3. Independent examinations

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

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

Goals

- Obtain a concept for effective and credible examinations

ID	Questions
3.1	Which criteria should determine which persons or organizations are mandated with an examination? Please outline the scopes for examination you find important and relate your answer to these scopes. Given that internet voting is not standard technology, in which areas (e.g. software, operations/infrastructure, trusted components) does formal certification conducted by certification bodies seem reasonable?
3.2	In case measures that reply to security requirements from the VEleS seem not to be implemented in a sufficiently effective way, under which circumstances would it seem reasonable to plan fixes only for the future, and to accept insufficiencies for the short term? Relate your reflections to actual security risks but also to the public perception.
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).
3.4	Which adaptation / clarification regarding scope and depth of the examinations would be appropriate? Can reference be made to existing standards? Which ones?

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

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

4. Transparency and building of trust

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

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

Goals

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

ID	Questions
4.1	How should the terms and conditions with regard to source code access be defined in order for them to enjoy credibility, i.e. to be accepted by the 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?

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

4.2	What should the scope / coverage of the published documentation be in order to achieve meaningful public scrutiny?
4.3	When should the code and documentation be published considering the workflows (development, mandated examinations and authorization)? Which indicators could be relevant?
4.4	Is it appropriate for the preparation and publication of documents to go beyond the current requirements of the VEleS? (e.g. test data, instructions for simulated voting)
4.5	Under what conditions should public reactions be discussed? 1. To whom should feedback be addressed? (System provider, administrations of the Confederation or the cantons, a new entity such as a scientific committee, common platform of multiple actors, etc.) 2. Which entities should be involved in the discussion?
4.6	Should the system providers publish existing / fixed security breaches? Through which channels? When?
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?
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?
4.9	How should the process of tallying and verifying conducted by the cantons be defined in order to be credible (verifying the proofs that stand in reply to universal verifiability, tasks and abilities of the members on an electoral commission / a separate administrative body charged with running votes)?
4.10	Is the publication of electronic voting shares of election and popular vote results likely to increase trust? Do you see downsides?

4.11	What additional transparency measures could promote security and / or trust? (Infrastructure inspections, publication of the minutes, for example, of an electoral commission, publication of the crypto proofs, etc.)
4.12	Which statistical plausibility checks method could be meaningful (e.g. comparison with other voting channels)? Is the publication of the results and method of any benefit? Do you see downsides?

5. Collaboration with science and involvement of the public

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

Goals

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

ID	**Questions**
5.1	Which are the conditions to be met in order to ensure that independent experts (particularly experts from science) participate? Which measures must / could be taken to meet or promote these conditions and thereby participation? 1. Participation in «public scrutiny» 2. Participation in examinations mandated by the public administrations of the Confederation or the cantons or the system providers 3. Supporting the public administration in the further course of the trial phase, e.g, at implementing the measures currently being defined in the course of the redesign
5.2	Which are the conditions to be met in order for representatives from science to participate in the political debate?
5.3	How could facts on internet voting be prepared and addressed to the public in a way that is recognized by representatives from science (e.g. describing the effectiveness of verifiability)? How would it have to be prepared and communicated?
5.4	Which pieces of information on internet voting should be prepared and addressed to the voters in order to promote trust (e.g. how verifiability works, under which conditions examinations were performed, etc.)? What should the level of detail be?

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

6. Risk management and action plan

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

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

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

Goals

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

ID	Questions
6.1	What should a continuous risk assessment process for internet voting consist of? How often should risk analyses be updated? Based on which input? Who should provide them? At which depth should risks be analyzed?
6.2	What are the benefits and downsides of publishing the (dynamic) risk assessment?
6.3	How could supply chain risks be properly handled by the cantons towards the system provider and by the system provider toward its contractors?
6.4	Which criteria for prioritizing action plan measures are relevant and in what order (including significance, urgency, feasibility, electorate impacted)?
6.5	To what extent can risk analyses be better aligned with standard methodologies? Which one would you recommend?

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

7. Crisis management and incident response

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

Goals

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

ID	**Questions**
7.1	What are the key elements in crisis management when it comes to internet voting? How should the fact that internet voting involves multiple actors be taken into consideration?
7.2	What are the right events and thresholds for an activation?
7.3	Who should be involved in crisis management, with which role?

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

7.4	How should the communication be organised (internally and externally)?
7.5	Are there already structures that should be involved in crisis management (e.g. GovCERT)?
7.6	What would the process of investigating an incident (potential manipulation of votes, intrusion in the voting system, distribution of malware on voters' platform, etc.) look like?
7.7	What are the requirements and stakeholders for digital forensics and incident response?
7.8	In practice, is it possible to investigate and prosecute a case in an effective and efficient way? If not, what measures could be taken?
7.9	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?