Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

Political Rights Section

Redesign and relaunch of trials

Final report of the Steering Committee Vote électronique (SC VE)

30 November 2020

Contents

1. Background

1.1 E-voting in Switzerland

Online voting ("e-voting") in Switzerland has been in a trial phase since 2004.[1] E-voting forms part of the federal and cantonal governments' strategy 'eGovernment Switzerland'. The statutory provisions for the trial phase can be found in Article 8*a* of the Federal Act of 17 December 1976 on Political Rights (PRA; SR 161.1), Articles 27*a*-27*q* of the Ordinance of 24 May 1978 on Political Rights (PoRO; SR 161.11) and the Federal Chancellery Ordinance of 13 December 2013 on Electronic Voting (VEleS; SR 161.116). The principle of the project has remained, from the very beginning, 'security before speed'. In Switzerland, only e-voting systems which meet the high security standards set in federal law are permitted.

Since 2004 a total of 15 cantons have enacted legal provisions at cantonal level and in over 300 pilot tests have allowed some voters to vote online. In all cantons, Swiss living abroad have been permitted to take part in the trials, and some cantons have allowed some of their resident voters to cast their vote electronically. Two online voting systems were available to the cantons in recent years: that of the Canton of Geneva and that of Swiss Post. As both of these providers withdrew their systems in mid-2019, e-voting is currently not available in Switzerland (see Sections 1.3.1 and 1.3.2).

1.2 General conditions for trial phase to date

1.2.1 Tasks and roles of the Confederation and cantons

In the exercise of political rights, a federal division of powers applies. In federal votes and elections, the conditions are set by the Confederation and the cantons are responsible for conducting the voting procedure. This division of responsibilities also applies to e-voting, and is set out in the existing legal provisions on e-voting trials. The cantons thus decide whether they wish to organise e-voting trials for their voters. They can operate their own system for this purpose or use the system of another canton or of a private company (Art. 27*k*^{bis} para. 1 let. b PoRO). The Confederation is responsible for authorising the trials, supports the cantons in legal, organisational and technical matters and coordinates the projects at national level.

1.2.2 Gradual introduction as third voting channel

The principle of 'security before speed' has been applied from the very beginning of the project. E-voting is to be introduced in a step-by-step process. Strict security requirements for e-voting systems and their operation are written into federal law. These are structurally linked to the gradual development of electronic voting. In the graduated requirements, the number of voters that can be admitted for online voting is limited: 30, 50 or 100 per cent of voters at cantonal level and 10, 30 or 100 per cent of the entire Swiss electorate. Swiss abroad who are entitled to vote are not taken into account when the upper limits are calculated.

1.2.3 Control and oversight

Authorisation procedure

Before they can introduce e-voting, the cantons require an basic licence from the Federal Council, and an authorisation from the Federal Chancellery (FCh) before each ballot is held. In the authorisation procedure, the FCh checks that the proposed e-voting system is compliant with federal law.

For cantons conducting their first e-voting trials, an basic licence can be granted for a maximum of five ballots (Art. 27*a* para. 2 PoRO). The Federal Council can grant an basic licence for a longer period thereafter (Art. 27*a* para. 3 PoRO). In practice, the maximum licensing period is two years (BBl 2013 5194). Special authorisation must be obtained for the use of e-voting in National Council elections (Art. 27*a* para. 4 PoRO).

[1] The Canton of Geneva conducted its first e-voting trials at cantonal level in 2003.

Independent examination

Article 7 VEleS states that the cantons are responsible for ensuring that an independent body checks compliance with all the requirements. If a canton wishes to offer e-voting to more than 30 or 50 per cent of its voters, there are stricter requirements for the examination of the system. Normally the bodies conducting such examinations are accredited by the Swiss Accreditation Service (SAS). The particulars of accreditation are regulated in the PoRO and the VEleS.

The authorisation procedure also involved the use of 'support groups' composed of representatives from the cantons. These groups conducted user tests, could pose questions about the documentation submitted along with the authorisation request and helped with the exchange of information.

1.2.4 Security requirements

The technical and operational requirements are set out in the VEleS and its annex. The key requirements for observing security standards in e-voting are as follows:

- Verifiability: Verifiability allows any manipulation of the voting system to be detected, while at the same time respecting voting secrecy. The VEleS differentiates between individual and complete verifiability:
  - Individual verifiability allows voters to determine whether their vote has been correctly registered by the system, i.e. as it is cast. They can therefore know that their vote has not been fraudulently altered on the e-voting platform used or on the internet.
  - Complete verifiability ensures that errors in the system caused by software failure, human error or manipulation attempts can be recognised by independent means throughout the voting process. In order to ensure voting secrecy is protected, votes are encrypted at all times, remaining so from the moment they are cast until the cryptographically mixed votes are decrypted. Cryptographic procedures must be employed that are specially designed for e-voting in order to overcome the apparent contradiction between traceability and protection of voting secrecy.
- Distribution of responsibility: E-voting systems must be spread across multiple computers that are set up differently, some of which may not be connected to the internet. Technical and organisational measures must be in place to ensure that no individual can access critical data or votes without the involvement of another person (multiple-assessor verification).
- Examination: The systems are regularly examined by independent organisations (external examinations, certification, repeated examinations for recertification). The cryptographic protocol is tested by highly specialised experts in cryptography.
- Best practices: In accordance with the mandatory ongoing improvement process, the systems must be continuously adapted and constantly protected against the latest security vulnerabilities.

1.2.5 Risk and crisis management

The cantons are responsible for conducting federal ballots and bear the risks when using e-voting systems. They must present a risk assessment demonstrating that the security risks are kept as low as possible. The risk assessment requirements are set out in Article 3 in conjunction with Article 6 VEleS.

The Confederation and cantons set out in a crisis agreement how information, cooperation and communication are to be managed if there is an incident in the e-voting process.

1.2.6 Transparency measures

It is essential that the public should have confidence in the voting system. The e-voting process thus involves a series of measures to promote transparency. In particular, federal law requires the source code and documentation from completely verifiable systems to be made public (Arts 7*a* and 7*b* VEleS). Moreover, in 2017 the Confederation and the cantons signed a declaration of intent stating that before the first deployment of a completely verifiable system, a public intrusion test (PIT) would be carried out in which interested persons could try to attack the e-voting systems.

1.3 Situation in 2019

1.3.1 Swiss Post system

In 2016, Swiss Post launched an e-voting system with individual verifiability, and this was put to use by a number of cantons. It also developed a new system with complete verifiability, for which it published the source code in February 2019. This system underwent a public intrusion test (PIT) organised by the Confederation, the cantons and Swiss Post from 25 February to 24 March 2019. The feedback from the participants provided indications as to how the system could be improved to comply with certain best practices in security technology. No infrastructure penetration, vote manipulation or breach of voting secrecy was identified in the course of the PIT.[2]

However, considerable security vulnerabilities in the area of verifiability were discovered in the published source code. One such flaw concerned individual verifiability and thus Swiss Post's system, which had been in operation until that time. The FCh subsequently commissioned an independent review of Swiss Post's individually verifiable system. While the Swiss Post's operational processes were positively judged, further vulnerabilities were identified in the system.[3]

In July 2019, Swiss Post announced that the individually verifiable system would no longer be used and that it would concentrate on developing the completely verifiable system.

1.3.2 Canton of Geneva system

The Canton of Geneva is one of the pilot cantons which permitted their eligible voters to vote electronically in federal ballots as far back as 2004. The canton developed and ran its own e-voting system, known as CHVote. Several cantons besides Geneva used this system, which employs individual verifiability. Geneva has been working since 2016 on developing a system with complete verifiability.

In November 2018, the Canton of Geneva announced that it would not be developing its CHVote system any further, pointing out that it was not the canton's task to single-handedly develop, operate and finance an IT system of such complexity and size.[4] In June 2019, the canton announced that the Federal Council decision regarding the use of e-voting in the National Council election, postponed to mid-August, would come too late, and that the canton would cease operating the CHVote system with immediate effect.[5] The Geneva system was thus employed for the last time in the popular vote of 19 May 2019.

The Canton of Geneva published parts of the source code of its system with individual verifiability under an open source licence in 2016. In 2019, the source code of the system with complete verifiability was published, although this had not yet been fully developed.

1.3.3 E-voting as standard voting channel

On 19 December 2018, the Federal Council launched the consultation procedure on the partial revision of the Political Rights Act (PRA), which would see the completion of the trial phase and the introduction of e-voting as a third standard voting method. The bill contained the main requirements of e-voting, namely the verifiability of ballot-casting and ballot-counting (i.e. the result), transparency of information about the system used and its operation, accessibility for all voters and the cantons' obligation to obtain approval from the federal government to use the electronic voting method. The bill still permitted the cantons to choose whether or not to introduce online voting.

[2] See the steering committee's final report 'Vote électronique – Public Intrusion Test 2019' August 2019 at www.bk.admin.ch > Political rights > E-voting > Public intrusion test.

[3] Members of the e-voting group at the Bern University of Applied Sciences (BFH) studied the implementation of the cryptographic protocol in the system specification and in the source code, and researchers Olivier Pereira (Université de Louvain) and Vanessa Teague (University of Melbourne) examined the implementation of the protocol on the basis of the system specification. In addition, the company Oneconsult wrote a report on the implementation of the technical and organisational security measures on the basis of the cantons' risk assessments. The reports are published on the FCh website: www.bk.admin.ch > Political rights > E-voting > Reports and studies.

[4] Canton of Geneva press release of 28 November 2018, available at www.ge.ch/document/point-presse-du-conseil-etat-du-28-novembre-2018#extrait-12897.

[5] Canton of Geneva press release of 19 June 2019, available at www.ge.ch/document/point-presse-du-conseil-etat-du-19-juin-2019.

The consultation showed that a clear majority of the cantons and political parties are in essence in favour of introducing e-voting. The Conference of Cantonal Governments and 19 cantons were in favour of e-voting becoming a standard voting method. However, the parties generally in favour of e-voting did not feel that the time was right for this next step. As a result, the Federal Council decided on 26 July 2019 not to proceed with the partial revision of the PRA at the present time.[6]

1.3.4 Conclusions on the situation in 2019

The following conclusions can be drawn from the implementation of transparency measures in 2019 and in particular from the subsequent discovery of significant security vulnerabilities in the current and future Swiss Post system:

- The transparency measures provided some important findings and revealed several flaws, based on which the e-voting systems could be improved.
- The disclosure of the source code and the PIT allowed experience to be gained in the area of public scrutiny and the broad involvement of external specialists. This experience also showed the need for action in the way the source code was disclosed and its quality.
- The discovery of some major vulnerabilities indicated that there were severe shortcomings in the development process to date and that action need to be taken with regard to quality assurance.
- The flaws and shortcomings identified were not detected by the control and certification processes already in place. The existing processes were not effective enough.

Developments in the e-voting project ‘Vote électronique’ have led to parliamentary initiatives at both federal and cantonal level. These have addressed the issue of system provider requirements,[7] overall security of electronic voting and conditions for the continuation of the trial operation.[8] The discussion surrounding e-voting is also influenced by suspicions that other countries will seek to interfere in elections and by reports on various incidents relating to cyber security and data protection, although these do not have immediate relevance for e-voting. E-voting thus forms part of the fundamental debate on the opportunities and risks posed by digitalisation.[9]

1.4 Situation in late 2020

Developments in recent years have also led to changes in the market situation on both the supply and demand side. Swiss Post is currently the only remaining system provider; it is the only provider that is continuing to invest in the further development of an e-voting system. The multi-product strategy goal formulated by the federal government and the cantons in 2017 has not been achieved as hoped. What remains of the Canton of Geneva's e-voting system is the system core with complete verifiability, completed by the Bern University of Applied Sciences and published under an open source licence. Developing and operating a system with complete verifiability has proven to be a demanding and costly undertaking. It is to be assumed that there will be little change in this situation in the foreseeable future.

The situation has also changed considerably on the demand side. Whereas 14 cantons conducted trials with e-voting in the popular vote held on 14 June 2015, only ten offered this form of voting in the popular vote of 10 February 2019. Only a handful of cantons are currently interested in resuming trials in the near future. The other cantons are focusing on digitalisation in other areas. This also means persons who have worked on e-voting in the cantons for many years are taking on new tasks and their expertise is being

[6] Federal Council press release of 27 June 2019; accessible at www.bk.admin.ch > Political rights> E-Voting > Media releases.

[7] Confederation: Mo. 18.4225 Wehrli 'Elektronische Stimmabgabe in den Grundversorgungsauftrag der Post aufnehmen'; Mo. 18.4375 Sommaruga 'E-Voting. Ein schneller und entschlossener Einsatz für ein System auf Open-Source-Basis und in öffentlicher Hand'; Cantons: incl. adoption of a bill by the Geneva Cantonal Council requiring the design, management and operation of the system used by the canton to be entirely in public hands.

[8] Confederation: Parl. Initiative Müller 18.427 'Ja zu E-Voting, aber Sicherheit kommt vor Tempo'; parl. initiative Zanetti 18.468 'Marschhalt beim E-Voting'; Mo. 19.3294 Zanetti 'E-Versand statt E-Voting'; Cantons: incl. St Gallen Cantonal Parliament: Rejection of Motion 42.19.07 demanding the immediate cease of E-voting trials; Lucerne Cantonal Parliament: Rejection of Motion 683 on a moratorium for e-voting in the Canton of Lucerne.

[9] See also Sotomo Research Institute (2018): Digitale Lebensvermessung und Solidarität, Verhalten und Einstellungen der Schweizer Bevölkerung, Zürich; digitalswitzerland (2019): Am digitalen Puls der Bevölkerung, Ein Bericht über die Einstellung der Bevölkerung zum Thema Digitalisierung, aufgenommen im Rahmen des Digitaltags 2019.

lost. Whether and how the redesign of e-voting will be successful depends to a large extent on the willingness of the remaining system provider and the remaining cantons to invest in developing the Swiss Post system and to restart trials. More cantons would also have to participate.

1.5 Redesign of e-voting trials

1.5.1 Federal Council mandate and objective

In June 2019, the Federal Council commissioned the FCh to work with the cantons on redesigning the e-voting trial operations.[10] This decision was based on the results of the consultation on e-voting becoming a standard voting channel and on the flaws identified in the Swiss Post system.

The Federal Council mandate states that the redesign of the trials should have the following objectives:

1. Further development of the systems
2 Effective control and oversight
3. Increasing transparency and trust
4. Stronger connection with the science community

The mandate also requires the FCh to look at whether current federal legislation needs to be amended. The legal requirements must be able to effectively measure and ensure the quality and security of the systems used. The requirements must also meet the expectations of Parliament and the general public with regard to security and transparency, in order to increase trust.

1.5.2 Cooperation between Confederation and cantons

Based on the Federal Council mandate, on 29 November 2019 the Steering Committee Vote électronique (SC VE) set up a task force, which was mandated with drawing up measures for the redesign and relaunch of the trials. It was asked to propose a staggered approach to the measures, allowing trials with the completely verifiable Swiss Post system to be resumed in the first stage of the redesign process.

The task force comprised the FCh Vote électronique project team (management and secretariat) and representatives from the Cantons of Bern, Fribourg, Basel-Stadt, St Gallen, Graubünden, Aargau, Thurgau and Neuchâtel. The task force conducted its work between December 2019 and October 2020. Swiss Post, as the only remaining system provider, attended the task force meetings.[11] This report contains the task force’s findings. The SC VE approved the report at its meeting on 30 November 2020.

[10] Federal Council press release of 27 June 2019; accessible at www.bk.admin.ch > Political rights > E-voting > Media releases.

[11] The service provider Swiss Post is responsible for developing and operating its e-voting system on behalf of the cantons. Swiss Post was invited to the dialog to give its expertise in the practical application of security requirements. It was not involved in decisions regarding the redesign measures.

2. Dialog with the academic community

2.1 Involvement of experts

In drawing up the basis for the redesign of e-voting, the FCh, with the participation of the other members of the task force, conducted a dialog with experts from academia and business circles. The external experts commissioned by the FCh included computer scientists, cryptographers and political scientists.[12] They helped the task force to establish the action required and to identify the issues concerning possible redesign measures. The dialog with these experts was funded by the e-Government Switzerland organisation.

Representatives of other cantons[13] and federal agencies[14] were kept constantly informed about the dialog with the academic community and received access to the discussion platform.

2.2 Dialog: procedure and form

For the dialog with external experts, the FCh along with other task force members defined the following topics for discussion:

1. Risks and security measures today and tomorrow
2. Independent examinations
3. Collaboration with science and involvement of the public
4. Transparency and building of trust
5. Risk management and action plan
6. Crisis management and incident response

When the dialog began in February 2020, the experts were asked to complete a comprehensive questionnaire of around 60 questions. Because of the measures to contain the coronavirus, the workshops originally planned were replaced by a written exchange moderated on an online platform. The online discussions took place between May and July 2020.

The questionnaire covered all six topic areas. The experts had the opportunity to express their general opinions on 'trustworthy e-voting', to answer specific questions about possible measures and to propose other measures. The aim of the questionnaire was to provide a broad overview, so that a consensus could be established and any need for discussion and clarification highlighted and addressed in a structured way.

Based on the assessment of the questionnaire responses, the following areas for the online discussion blocks were defined:

Topic areas	Discussion blocks
1	Block 1: Effectiveness of cryptography
1	Block 2: Diversity to support security and trust-building
1	Block 3: Print office (distributed parameter generation)
1	Block 4: Public Bulletin Board
2	Block 5: Examinations Mandated by Government
4	Block 6: Development and publication
4	Block 7: Public Intrusion Test / Bug Bounty
5	Block 8: Risk management and individual risks

[12] See list of mandated experts of June 2020 at www.bk.admin.ch > Political rights > E-voting.

[13] Cantons of Zurich, Lucerne, Glarus, Ticino and Geneva.

[14] National Centre for Cyber Security (NCSC), Armed Forces Command Support Organisation (AFCSO), the FDFA Office of the Special Envoy for Cyber Foreign and Security Policy and OIC MELANI at the Federal Intelligence Service (FIS).

5	Block 9: Risk limiting audits and plausibility checks
6	Block 10: Forensic readiness
all	Block 11: Big picture
3	Block 12: Future dialog

For each discussion block, theses, proposed solutions and unresolved issues were drawn up with and by the experts. The participants discussed different topics in parallel, could respond to the answers of other participants and ask each other questions. The contributions were visible to all participants. The aim was to arrive at a consensus, clarify unresolved issues, validate the conclusions and record any divergences in opinion.

Over 700 responses were recorded on the platform in total, ranging from short statements to detailed answers. In parallel with the online discussion, individual experts were commissioned to address further issues in relation to possible measures. At the end of the dialog, the FCh and other members of the task force drew up a summary of the findings. All documents are published on the FCh website.[15]

The dialog with the experts was moderated on behalf of the FCh by Christian Folini, senior security consultant at netnea AG.

2.3 Summary of dialog findings

2.3.1 General assessment

The experts see a need for action with respect to security, transparency and independent scrutiny, while recognising that valuable experience has been gathered in the last 15 years. They recommend that other means of voting should also be analysed with respect to security, and that questions about building trust should be examined in depth. The experts emphasised the importance of involving specialists, in particular from science, at all times in the planning, development and testing phases of internet voting. On a number of occasions they also suggested establishing a scientific committee.

2.3.2 Providing a secure system

Authorities should continue to set security standards

The experts were of the opinion that it is the responsibility of the authorities to determine risks and put measures in place if necessary. A scientific committee could provide support in this area.

Standardisation of cryptographic building blocks

The security standards already required today in the field of cryptography are important and should be continually adapted according to the latest insights and progress of science. The experts also recommended that the authorities work towards standardizing cryptographic building blocks.

Ensuring the quality and auditability of the source code

Care must be taken to ensure that the system documentation and source code are available in a form that allows an effective review of conformity with the legal requirements. The experts mentioned various standards as a possible basis for the development processes. The basic principle of the system design should be simplicity.

Greater diversity as a basic condition for trustworthiness

The experts are of the opinion that the diversity of components that are important for verifiability (i.e. so-called control components and verifiers) is a basic condition for a system's trustworthiness: Defects in

[15] www.bk.admin.ch > Political rights > E-voting.

individual components would not have an impact on verifiability if other components function properly (exponential increase in security). Software is one of the elements subject to diversity. The experts also see potential for improvement in generating system parameters (for example of verification codes for individual verifiability), which should be verifiable and conducted in a distributed manner. They also outlined solutions for a distributed printing process for polling cards. The experts acknowledge the costs and greater operational complexity of introducing wider diversity but emphasise the additional benefit.

Public bulletin board allowing more verifiability

The use of a 'public bulletin board', which is known from the scientific literature on internet voting, was discussed as a complementary approach to enhance verifiability and make it more independent. The experts consider a public bulletin board to be a suitable instrument for building trust, but think that trust could be jeopardised if mistakes are made in the design or the implementation. Voters' needs with respect to communication, visual illustration and user-friendliness must be studied early on and taken into account.

2.3.3 Commissioned examinations and public scrutiny

Commissioned examinations

Certification of the systems is not deemed to be of crucial importance. Nonetheless, certification could be useful in the course of examinations of the operations (ISO27001 certification). Instead of certification, the authorities should look to independent examinations by people with the necessary expertise. Cryptographers should be consulted also when inspecting the source code and the operations. Scrutiny should adopt a holistic approach in order to prevent gaps in the scope, and it should be commissioned by the Confederation or by an independent committee.

Public scrutiny

The experts consider public scrutiny to be very important. They would welcome the public intrusion test of 2019 being replaced with a permanent ongoing bug bounty programme with financial compensation. The bug bounty programme should not be limited to successful attacks on the provider's infrastructure, but also include errors in the system's documentation and in the source code. The Confederation or an independent committee should be responsible for defining the objectives and the provisions as well as for supervising a bug bounty programme. In addition to a bug bounty programme, other measures for involving the public could also be considered, such as 'hackathons'. Involving people who do not have a technical background could also be useful, for example as part of a citizen science project on user-friendliness or on communication.

Transparency and source code disclosure

Transparency is a condition for public scrutiny to be effective. The experts are of the opinion that source code disclosure should not be subject to a non-disclosure agreement. Besides the source code, all documents necessary for understanding how the system works and is operated should also be disclosed. It should also be possible to test the system on private computers. If adjustments to the source code are not disclosed immediately, the experts advise carrying out a first series of examinations to avoid unnecessary errors and a subsequent loss of trust. Any shortcomings should be divulged and information from the public should be responded to. The Confederation should define the detailed provisions in this respect. Most of the experts also advise publishing test reports. However, some of the experts are concerned that publishing test reports of poor quality may lead to a loss of trust. The experts consider it possible that disclosure allows expedient public validation even without an open source licence.[16] However, they consider disclosure under an open source licence to be more promising.

[16] Open source licences allow software to be used for any purpose.

Dealing with non-conformities

Ideally, commissioned and public examinations should take place far enough in advance so that nonconformities are identified early enough to be rectified before putting internet voting into operation. Decision-making procedures should be established for dealing with non-conformities that are discovered late. Not every non-conformity must prevent the use of internet voting. The experts consider it plausible to accept minor risks. The difficulty is to assess the risk accurately; comparing risks that are already accepted may be helpful. Further factors to consider are the de facto loss of voting rights by a part of the Swiss electorate abroad and the fact that rejecting internet voting results in greater use of voting by post, which also entails risks. The more a system and the surrounding processes are affected by a nonconformity, the sooner it must be remedied. As a principle, errors in the cryptographic protocol or its implementation in the source code should not be accepted.

2.4 Assessment of the dialog with the academic community

The involvement of experts from a range of specialist areas led to a wide-ranging discussion of where action needs to be taken and of possible solutions. This provided the task force with a sound basis for its work. The feedback from the experts was positive; they welcomed being involved in the dialog. Furthermore, they were in favour of the dialog between the public authorities and academic circles continuing. The focus was on technical issues in particular; in future, the social and societal aspects of e-voting will be considered to a greater extent. The experts also expressed the view that, in the discussion about security issues, not only e-voting but also the other voting channels should be considered. A holistic view of possible attacks would improve the security of the voting process in general.

The Confederation and the cantons share the view that there should be greater cooperation with experts from both business and academic circles in the future. The task force will draw up measures to encourage their involvement in a range of areas.

3. Description of measures

The measures for the redesign and relaunch of the trials are explained and evaluated below, and are considered in the light of the dialog with the academic community (see Section 2.3 as well as the summary of the expert dialog).[17] An overview can be found in the catalogue of measures in the annex. Input from the experts will be considered when the measures are implemented.

A. Further development of the systems

No	Measure	Timeframe implementation	Responsibilities
A.1	Draw up precise criteria for source code quality and documentation quality	Relaunch	Requirements: FCh Implementation: Cantons, system providers

Objective and description of measure

The quality of the source code and documentation is a key element in the security of e-voting. The current legislation sets out the requirements to be met in this respect. However, the wording is rather general, e.g. preparing and documenting according to the best practices (Art. 7*b* VEleS) and implementing certain of the common criteria selected according to the protection profile of Germany's Federal Office for Information Security (BSI). Action is required in this area. The FCh will therefore specify the existing quality criteria that the source code and its documentation must meet. Clear criteria aim at ensuring the high quality of the e-voting systems. Furthermore, this should make it easier for tests to be carried out by all actors, including the public.

In specifying the quality criteria, the FCh will be guided by existing standards (e.g. ISO Systems and Software Quality Requirements and Evaluation) and adapt the statutory provisions accordingly. These criteria must be met when trials are relaunched. Furthermore, the quality assurance process in software development should also take account of these criteria.

Dialog with the academic community

The source code and documentation must be of high quality and in a form that allows effective verification of conformity with the legal requirements and the security model. Moreover, the system design should display a high degree of simplicity. The quality of the source code and documentation is a cross-cutting issue; for more detailed assessments by the experts, please refer to the comments on other measures (e.g. independent reviews, quality assurance in the development process, disclosure of source code).

Impact of measures[18] and SC VE general assessment

E-voting has always demanded a high-quality source code and documentation. The requirements will now be made more detailed. This both creates transparency for system providers about the requirement level and helps to ensure that the developed software meets the expected quality demands. Furthermore, the verifiability of the source code and documentation will be improved. This measure is related to quality assurance in the development process (Measure A.2), build and deployment (Measure A.3), independent testing (Measures B.1 and B.2) and source code disclosure (Measure C.2).

Ensuring the high quality of the source code and documentation is cost-intensive. This measure involves giving a more detailed specification of the quality criteria, and should not incur additional costs for the Confederation and cantons.

[17] The full documentation is published on the FCh website: www.bk.admin.ch > Political rights > E-voting.

[18] In the assessment of the financial impact, estimates of additional costs (external costs or additional resources) incurred by the Confederation and the cantons are given in each case. Scale: low (< CHF 50,000) / medium (CHF 50,000-500,000) / high (CHF 500,000-1 million) / very high (> CHF 1 million).

No	Measure	Timeframe implementation	Responsibilities
A.2	Improve quality assurance in development of e-voting systems	Relaunch	Requirements: FCh Implementation: Cantons, system providers

Objective and description of measure

The quality of e-voting systems must be assured throughout the development process. The FCh will set out more detailed requirements in order to raise the quality. This is to achieve the following objectives:

- It must be possible to trace and verify any changes to the system.
- It must be possible to ensure traceability between the individual elements of the documentation (protocol, specification, architecture, etc.) and the source code, at all times and in both directions.
- The results of test processes flow back into development.
- Conformity with legal requirements is ensured and maintained throughout the entire life cycle.

The FCh will specify in the legal bases any related requirements for the resumption of tests.

Dialog with the academic community

The experts listed a number of different standards as a possible basis for the development processes. Many of the experts believe that traceability is the most important feature of the development process. Moreover, they stress the importance of transparency, of involving independent experts and of the correct system set-up from the source code (see Measures A.1, A.3 and C.2). The cryptographic security standards already required today are important and should be continually adapted according to the latest insights and scientific progress. Furthermore, the experts advise the authorities to work towards a standardisation of the cryptographic building blocks.

Impact of measure and SC VE general assessment

It is important to improve quality assurance in the development process. By setting more detailed specifications, there is a focus on system quality throughout the development process. This aims at ensuring a high level of system security and make it easier for the authorities and independent experts to conduct tests. This measure should have no direct financial consequences for the Confederation and the cantons.

No	Measure	Timeframe implementation	Responsibilities
A.3	Use a proven and traceable build and deployment method	Relaunch	Requirements: FCh Implementation: Cantons, system providers

Objective and description of measure

Correct deployment of the system from source code to its installation in production (build and deployment) must be ensured. For this purpose, the system provider must use a proven and traceable build and deployment method. The corresponding build and deployment requirements will be revised to meet the following objectives:

- The build and deployment method ensures that the deployed software conforms to the published, tested and approved version (traceability).
- Moreover, the build and deployment method will help prevent the manipulation of system components as much as possible.
- The introduction of vulnerabilities into the system when the development tools and libraries for the software are deployed must be avoided. A process will be developed for dealing with non-conformities (see Measure B.3).

The FCh is adapting the legal bases to include the necessary requirements for system providers. The new requirements must be met before trials can be relaunched.

Dialog with the academic community

The experts confirmed the importance of using an effective and verifiable build and deployment method. This method must be suitable for the provision of secure systems and allow traceability and verification of the deployed software. Best practices in build and deployment were discussed.

Impact of measure and SC VE general assessment

This measure, in conjunction with measures A.1 and A.2, is intended to improve the quality, traceability and verifiability of the system throughout. Implementation of this measure has no financial consequences for the Confederation; for the cantons, a minor financial impact is projected.

No	Measure	Timeframe implementation	Responsibilities
A.4	Deploy manufacturer-independent components (verifier / control components)	Study and request for online control components to SC VE: up to two years after relaunch Conditional implementation: c. five years after relaunch	Online control components study: Cantons with FCh involvement

Objective and description of measure

Verifiability can be strengthened by creating greater diversity and independence for individual components in the software. The following components could be operated with software that is not supplied by the manufacturer of the rest of the system:

- Control components for generating the verification codes and for storing votes until counted (also 'online control components').
- Control components to shuffle votes.
- Verifiers to check that all votes recorded by the online control components have been correctly shuffled, decrypted and counted.

The SC VE intends to deploy manufacturer-independent online control components for about five years after relaunch provided the necessary funds are available. A critical amount of active cantons is needed to share the financial burden: a sufficient number of cantons must agree to meet the costs to be borne by the cantons. A further proviso is that no significant reasons against implementation arise unexpectedly at a later date.

Priority will be given to developing a basis for the online control components. As a first step, a study will be carried out to establish who should be responsible for awarding contracts, conducting system maintenance, conducting operational processes and handling any technical issues, and how these aspects will be carried out. The study will also clearly state the implications for the cantons in terms of both operational processes and costs. Furthermore, it will propose a clear implementation plan (according to an initial assessment by the cantons, implementation will take between three and five years). The study will provide a basis for making the decision regarding implementation. The cantons are responsible for organising the study.

Once the study has been completed, the FCh and the cantons will submit a proposal to the SC VE on further action to be taken.

Dialog with the academic community

Having a range of diverse components to implement verifiability (control components and verifiers) is, in the experts' view, vital in creating a trustworthy system; an error in one component that might otherwise have a negative effect on verifiability can be overridden by correctly functioning components (exponential security gain). The experts therefore advocate the use of manufacturer-independent software on the important components ('control components' and 'verifiers'). They acknowledge that introducing greater diversity entails higher costs and leads to greater complexity in the operation of the system, but stress the added value this brings.

Impact of measure and SC VE general assessment

Diversity of the components that are important for verifiability is vital in ensuring the trustworthiness of an e-voting system. The use of independent online control components is thus a medium-term objective.

The costs of conducting the study will be low to medium for the cantons; no costs are incurred by the Confederation. The study will examine the precise design of independent control components, how they can be used and the associated costs. Based on current assumptions, Swiss Post has provided an initial estimate of the costs of implementation:

- One-off costs: CHF 1.8-2.2 million
- Recurring costs (average): CHF 600,000-800,000 / year

The Bern University of Applied Sciences estimates the following costs for implementing an independent verifier:

- One-off costs: CHF 900,000-1 million
- Recurring costs (average): CHF 200,000 / year

Under the current division of responsibilities, the cantons would have to bear these costs. However, they point out that the implementation costs would exceed their resources. Co-financing by the federal government should therefore be considered.

No	Measure	Timeframe implementation	Responsibilities
A.5	Weaken trust assumptions in the printing process and in the software that generates cryptographic parameters	Extension / adaptation of protocol: 1 year after relaunch Request to SC VE: up to two years after relaunch Conditional implementation: c. 4 years after relaunch	Issues to be clarified for requirements: FCh Implementation: Cantons

Objective and description of measure

Verifiability in e-voting is only effective if the relevant cryptographic parameters are correctly generated in the preparation phase and confidential values (e.g. verification codes) do not fall into the wrong hands. Under current legislation, voters' confidential values may be printed by a single printing press. Organisational security measures must therefore be extensive enough for these values to remain secret. The law does not specify the extent to which the correct choice of parameters may also be based on organisational measures. Action thus needs to be taken to improve the effectiveness of verifiability.

The permitted trust assumptions in the printing process and in the software that generates cryptographic parameters need to be weakened. Using manufacturer-independent software, it is possible to determine that cryptographic parameters, and in particular the verification codes, have been generated randomly. To achieve the desired entropy, at least four control components must be used to generate individual values. Randomly selected polling cards are to be checked to determine whether the values have been correctly printed with regard to the verified values.

The SC VE intends to adapt the parameter generation as well as the printing process within about four years after the relaunch, provided the necessary funds are available. A critical mass of active cantons is needed to share the financial burden, and a sufficient number of cantons must agree to meet the costs to be borne by the cantons. A further proviso is that no significant reasons against implementation arise unexpectedly at a later date.

In a first step, the FCh and cantons will draw up more detailed proposals. The cantons will have the cryptographic protocol adapted and work with Swiss Post to define their processes. An initial assessment of the time required showed that implementation (including adaptation of the cryptographic protocol) will take a good three years. More detailed implementation planning will take place in the initial phase.

Once this is completed, the FCh and the cantons will submit a proposal to the SC VE on further action to be taken.

Dialog with the academic community

The experts agree that correct parameter generation (e.g. of the codes for individual verifiability) needs to be verifiable and distributed where necessary (based on several random values). They see room for improvement in this area. They outlined solutions for a distributed process for printing the voting material and suggest that the values should not all be printed using the same printing machine, but instead that several different machines should be used. The experts acknowledge the costs and the greater operational complexity caused by the introduction of diversity, but they underline the advantages this brings.

Impact of measure and SC VE general assessment

In a dialog with the academic community, the FCh, in collaboration with the cantons, submitted to the experts an outline of a possible regulation in this area. This brings security gains, but for cost reasons still provides for the use of a single printing press. Swiss Post and the Bern University of Applied Sciences (BFH) prepared an initial study of the feasibility of the outlined requirements for their respective systems and submitted it to a number of experts. The findings show that it should be possible to implement the requirements. Swiss Post calculated that the necessary adaptation of the cryptographic protocol would take about a year. More detailed bases for weakening trust assumptions will be drawn up in a first stage.

Weakening trust assumptions is important in order to increase trust in the e-voting system. This is a medium-term objective.

More detailed planning entails minor costs for the Confederation. Adapting the cryptographic protocol, however, entails high costs. According to Swiss Post's initial estimates, the following costs will arise:

- One-off costs for adapting the cryptographic protocol: CHF 850,000 to CHF 1 million

Who will meet these costs is yet to be decided. The modalities and implementation costs will be drawn up in detail in the study. Swiss Post has provided an initial estimate of the costs of implementation based on current assumptions:

- One-off costs for further implementation: CHF 700,000–900,000
- Recurring costs for support, maintenance and operation (average): CHF 100,000 / year

In accordance with the current division of responsibilities, the cantons would bear these costs. However, they point out that the costs for the first stage and the subsequent implementation costs would exceed their resources. Co-financing by the federal government should therefore be considered.

No	Measure	Timeframe implementation	Responsibilities
A.6	Enhance the foundations for additional verification mechanism whose effectiveness is not based on current trust assumptions	Study: one year after relaunch Request to SC VE: up to two years after relaunch	Study: FCh with cantons' involvement

Objective and description of measure

With the aim of increasing diversity, the possibilities of an additional verification mechanism will be explored and analysed. One issue is whether and how an additional instrument to those provided by the manufacturer to assure verifiability can be offered to voters. A public bulletin board could be one such mechanism. With a public bulletin board, voting data could be made public while preserving the secrecy of the vote, and voters could use a second device (e.g. a mobile phone) to determine whether their vote had been correctly received by one or more entities independent of the manufacturer. This would mean that individual verifiability would not depend on the trustworthiness of the printing company or on the control components. As part of their universal verifiability testing, the cantons could establish whether all the votes received by the independent entities had been considered in the count.

Initially, a study will be developed to examine the benefits of an additional mechanism and of the way that this might be implemented. The study will address technical implementation issues as well as trust-building and acceptance, the latter in consultation with voters. The FCh is responsible for organising the study.

Once the study has been completed, the FC and the cantons submit a proposal to the SC VE as to whether and how a public bulletin board could be applied. Funds must be earmarked for possible future implementation.

Dialog with the academic community

The experts discussed a further option for verifying votes, namely publication of the encrypted votes on a public bulletin board. This mechanism, additional to the verification codes, is well known from the academic literature. The experts consider the use of a public bulletin board to be a suitable instrument for building trust, but they also warn that trust could be eroded if mistakes are made in its design or implementation, or if the needs of voters are not taken into account, namely in terms of communication, visual presentation or user-friendliness. In this respect, citizen science projects were mentioned as a measure to accompany possible trials. How to deal with reports from voters on negative verification results and security aspects needs to be further discussed so that a clear solution can be presented.

Impact of measure and SC VE general assessment

As part of the dialog with the academic community, a number of experts conducted a study to examine the topic in greater depth from a cryptographic perspective and to identify possible approaches. This needs to be pursued further before a decision can be taken on the possible implementation of such an additional verification mechanism. A number of issues are currently unresolved, such as the possible modalities and the opportunities and risks this solution involves. In particular, the study will address in greater depth issues of user-friendliness and communication towards voters. Conducting the study will incur medium costs for the Confederation; there are no additional costs for the cantons.

The modalities and implementation costs will be drawn up in detail in the study. An initial estimate of the costs of implementation has been made based on current assumptions:

- One-off costs: CHF 600,000
- Recurring costs (average): CHF 200,000 / year

Responsibility for implementation and thus for financing is to be established in the study. The cantons point out that the implementation costs would exceed their resources. Co-financing by the federal government should therefore be considered.

No	Measure	Timeframe implementation	Responsibilities
A.7	Improve bases for detection (monitoring) and investigation of incidents (IT forensics)	Definition of requirements and improvement process: Relaunch	Requirements: FCh Improvement process: System providers, cantons

Objective and description of measure

E-voting systems must allow for effective detection and investigation of incidents – such as suspected vote tampering or system attacks. The entire system must be designed and developed in such a way as to anticipate the occurrence of incidents and to use appropriate tools to investigate them ('forensic readiness'). The information gathered and stored must be available as digital evidence for any incident investigation and subsequent legal process. The federal requirements currently in force lay down certain principles for detecting and reporting security incidents and weaknesses, as well as for dealing with them and making subsequent improvements (Section 3.2 of the annex to the VEleS).

Before trials are resumed, the existing requirements for gathering evidence must be tightened. Consistent protocols on all system elements must be drawn up to aid the detection and investigation of incidents. These protocols must be drawn up, transferred and stored in such a way that they cannot be manipulated. The contents and scope of the protocols must be defined in such a way that incident investigations can be carried out effectively. Voting secrecy must be guaranteed at all times.

In a second step, a continuous process for improving methods to detect and investigate incidents will be defined and implemented when trials are resumed. The following aspects should be taken into account in particular:

- There is an open dialog between the Confederation, cantons and system providers at all times.
- Regular analyses will be conducted of the suitability of the bases for monitoring and investigation. The scenarios defined in the crisis agreement will be taken into account in these analyses. Improvements can be made more efficiently by involving IT forensic experts.
- Findings from the analyses will influence improvements in the instruments and processes.

Dialog with the academic community

The experts are of the opinion that it is important to construct the system in such a way that incidents can be identified and investigated. The necessary information must be clearly accessible throughout the process. Voting secrecy must be guaranteed at all times. Suitable instruments for gathering information must be used and simulations of an investigation regularly run in order to establish whether the right information has been gathered and can be clearly accessed.

Impact of measure and SC VE general assessment

The aim of this measure is to create an open dialog between the Confederation, cantons and the system provider regarding continuous improvements in monitoring and IT forensics. The statutory provisions need to contain clear, detailed requirements for the elements necessary to ensure incidents are detected and investigated properly. This will improve the forensic readiness of the system and increase trust in e-voting.

Implementation of this measure has no financial consequences for the Confederation. As it is a matter of specifying more detailed requirements, the cantons do not expect any additional costs. However, the improvement process the measure is intended to initiate could result in costs of an as yet undetermined size.

No	Measure	Timeframe implementation	Responsibilities
A.8	Create a joint plan for implementing measures for the Confederation and cantons	Relaunch	FCh, cantons

Objective and description of measure

The Confederation and the cantons have a joint plan for implementing measures going forward. The set of measures reflects the decisions regarding redesign of the e-voting trials and shows which measures are already being implemented in the relaunch and which measures will constitute the further development of e-voting in the medium to longer term. Wherever possible, a time schedule for implementing the measures or for the initial stages should be given. The set of measures will be approved and published by the SC VE as a statement of intention, at the latest when e-voting trials are relaunched. The set of measures will be regularly reviewed, thus ensuring that the latest developments are taken into account to ensure security.

Dialog with the academic community

The experts agree that there is a need for action and that suitable measures must be applied. Some of these measures are complex and time is required to implement them.

Impact of measure and SC VE general assessment

A published set of measures is a target-oriented instrument to show the public and all actors involved the planned developments and work in progress. Drawing up a set of measures has no direct financial impact for the Confederation or cantons. The cost of implementing the measures will be shown with each measure in the plan.

B. Effective control and oversight

No	Measure	Timeframe implementation	Responsibilities
B.1	Adapt responsibilities in the examination of the system and the underlying processes	Relaunch	FCh

Objective and description of measure

Experiences from 2019 showed that the previous requirements for system and process examinations were not effective. The disclosure of the source code and a subsequent independent examination revealed significant security flaws that had not been identified by previous examinations and certifications. In order to ensure the effectiveness and credibility of the examinations, this measure will adapt the responsibilities and Measure B.2 will adapt the design of the system examinations.

Independence between the auditing body and the audited entity plays an important role when responsibilities are altered. The division of duties between the Confederation and the cantons will thus be adapted so that the Confederation assumes more responsibility and a more direct role in examining the systems. The responsibilities will be adapted as follows:

Examinations as in VEleS annex	**Responsibilities - current**	**Responsibilities - future**
5.1 Cryptographic protocol examination	Entity responsible: Canton Client: System provider Supplier: Accredited body	Entity responsible: FCh Client: FCh Supplier: Cryptography experts
5.2 Functionality examination	Entity responsible: Canton Client: System provider Supplier: Accredited body	Entity responsible: FCh Client: FCh Supplier: Cryptography experts and development experts
5.3 Infrastructure and operation examination	Entity responsible: Canton Client: System provider Supplier: Accredited body	*System provider's infrastructure for ISO 27001 certification* Entity responsible: Canton Client: System provider Supplier: Accredited body in accordance with ISO 27001
		Infrastructure of system provider and canton to meet VEleS requirements Entity responsible: FCh Client: FCh Supplier: Cryptography experts and system operation experts
5.4 Control components examination	Entity responsible: Canton Client: System provider Supplier: Accredited body	Entity responsible: FCh Client: FCh Supplier: Cryptography experts and development experts
5.5 Protection audit against attempts to hack infrastructure	Entity responsible: Canton Client: System provider Supplier: Accredited body	Entity responsible: FCh Client: FCh Supplier: Security experts
5.6 Printing press examination	Entity responsible: Canton Client: Canton Supplier: Accredited body	Entity responsible: FCh Client: FCh Supplier: Cryptography experts and system operation experts

The system provider will thus continue to be responsible for audits relating to system operation in its data centres (ISO 27001 certification in accordance with Section 5.3 of the annex to the VEleS). No further certification by bodies accredited by the Swiss Accreditation Service (SAS) will be required in future. The Confederation is responsible for examinations to check compliance with the requirements relating to the system and the underlying processes. Independent experts will be commissioned to conduct the examinations.

The FCh will amend the VEleS annex for the relaunch.

Dialog with the academic community

The experts stressed that independent examinations should be commissioned by an independent committee or by the Confederation. Certification only makes sense as part of system auditing (ISO 270001 certification). The authorities should focus on independent examinations by persons with the necessary expertise. In examinations e-voting systems, appropriate expertise is of greater value than certification. Cryptographers should also be involved in scrutinizing the source code and the system operation. There should be a comprehensive approach to examinations in order to avoid gaps. Moreover, there should be a particular focus on public scrutiny.

Impact of measure and SC VE general assessment

The effectiveness of the examinations can be ensured if the Confederation commissions the bulk of the examinations going forward in addition to drawing up the examinations concept (Measure B.2). These are important and expedient aspects.

The examination costs are to be borne by the entity responsible. Adapting the responsibilities thus has a considerable financial impact on the Confederation. The cantons remain responsible for auditing the system provider's infrastructure (ISO 27001 certification); costs for further certification by an SAS-accredited body are no longer incurred. The cantons assume that this will not result in any direct cost savings for the cantons (the change in responsibility requires more comprehensive preparation on the part of the system provider, while the staffing required to carry out the examinations remains unchanged).

Adapting the responsibilities has an impact on the processes between the Confederation, cantons and system provider and on the authorisation procedure (see Measure B.9). The FCh will provide the cantons with the examination reports on an ongoing basis and give its feedback on the examination results. The cantons will thus have the necessary information for assessing any authorisation application made to the Confederation. The FCh will ensure that the cantons are involved in the examinations and will exchange information with the cantons on a regular basis.

No	Measure	Timeframe implementation	Responsibilities
B.2	Develop an examination concept to assess conformity of the system and the underlying processes	Relaunch	FCh with cantons and system providers

Objective and description of measure

Responsibilities for system and process examinations will be aligned with Measure B.1. A new examination concept will be developed to reflect these new responsibilities, to ensure that examinations are carried out without gaps and to achieve greater overall effectiveness. The examination concept will ensure that the security requirements are thoroughly inspected.

The examination concept will include the following aspects:

- Clear definition of examination depth for the different areas: the scope of the individual examination areas and the duration of the examination result’s validity are defined.
- Permeability between examined areas: permeability between the examined areas ensures a consistent and complete examination.
- Qualified and independent experts will be appointed to conduct the examinations.
- The examination reports will be published (see Measure C.4).

System examinations should be conducted at an early stage so that there is enough time before the system goes into operation to eliminate non-conformities and to re-examine (see Measure B.3, dealing with non-conformities).

The examination concept will be drawn up by the FCh. The examinations conducted before the relaunch of trials will be based on the new examination concept. The FCh can invite external experts to be involved in drawing up the examination concept.

Dialog with the academic community

See explanations under Measures B.1.

Impact of measure and SC VE general assessment

See explanations under Measures B.1. Drawing up an examination concept has minor financial implications for the Confederation. Costs may be incurred for the use of external experts. This measure has no financial impact on the cantons.

No	Measure	Timeframe implementation	Responsibilities
B.3	Develop and implement a process to deal with non-conformities	Relaunch	FCh with cantons and system providers

Objective and description of measure

Non-conformities such as defects in the system and underlying processes may be discovered at any time. If non-conformities are discovered or suspected shortly before or during the e-voting process, it is extremely important to have a set procedure for dealing with them. A non-conformity does not necessarily mean that the system cannot be used. Non-conformities must be assessed in terms of their impact on risk, and consideration must be given to whether the risk associated with a non-conformity can be minimised by other measures. Having a process for dealing with non-conformities will ensure that, in the event of an incident, there is as much clarity as possible and that e-voting can be conducted in conformity with the requirements of the VEleS.

Before the resumption of trials and in collaboration with the cantons and the system provider, the FCh will develop a process for dealing with proven and suspected non-conformities, defining the following aspects:

- Defining non-conformities: the type of non-conformity that triggers the process is determined.
- Setting criteria: criteria are set that can be applied in dealing with non-conformities. The non-conformities are assessed in terms of their impact on the risks. Here the risks that result from a system withdrawal must also be considered. In principle, the e-voting system is more likely to be usable when non-conformities do not relate to the system but to the surrounding processes. If the system can be used despite detection of a non-conformity, provision should be made for the non-conformity to be rectified and this should possibly be included in the plan of measures to be taken by the Confederation and the cantons (cf. Measure A.8).
- Determining actors and roles: The roles and cooperation between the Confederation, cantons, system provider and possible other actors is to be determined. Independent experts may be invited to advise on dealing with non-conformities.

Dialog with the academic community

The experts stressed the importance of having a clearly defined process for dealing with non-conformities. They agree that not every non-conformity should necessarily mean that e-voting must be stopped. Minor risks can be accepted. However, the risks must be appropriately assessed, and in some cases this is difficult to do. Alternatively, the severity of the non-conformity can be taken as the decision criterion. A comparison with risks that are already accepted may be helpful. Further factors to consider are the de facto loss of voting rights by a part of the Swiss electorate abroad and the fact that if e-voting is not used, there will be greater use of postal voting, which also entails risks. The more extensively a non-conformity affects a system and the surrounding processes, the sooner it must be remedied. As a principle, errors in the cryptographic protocol or its implementation in the source code should not be accepted.

Impact of measure and SC VE general assessment

Defining how to deal with non-conformities is seen as an important measure. All actors benefit from a clearly defined decision-making process containing the main criteria for dealing with non-conformities. Implementation of this measure has no financial consequences for the cantons. Costs may be incurred by the Confederation in employing external experts.

No	Measure	Timeframe implementation	Responsibilities
B.4	Revise and improve risk assessment guidelines	Relaunch	FCh with cantons and system providers

Objective and description of measure

The existing bases and requirements for risk assessment will be revised and improved. The risk assessments by the FCh, cantons and system provider (see Measure B.5) are to be conducted on the basis of guidelines. The guidelines will contain the basic risk assessment concept and the allocated responsibilities. The actors will still be free to choose the risk assessment method they wish to apply. The guidelines will contain the following main aspects:

- Catalogue of information assets

- Catalogue of threats (based on the list of threats in Section 3.1 of the annex to the VEleS)
- Catalogue of risk minimisation measures
- Responsibilities with regard to protection of information assets

The guidelines will cover, among other things, the length of encryption keys, multiple votes cast through different voting channels, vote buying, long-term privacy and reliance on a single provider.

The guidelines will be drawn up by the FCh in conjunction with the cantons, system providers and IT experts. They will be published prior to the trials relaunch in order to enhance transparency and build trust. Moreover, the public will have the opportunity to give feedback. The guidelines should be reviewed periodically and adapted where necessary.

Dialog with the academic community

The development of a set of guidelines as a basis for risk assessments was discussed. In the view of the experts, this set of guidelines should be drawn up by the Confederation (in conjunction with the cantons, system providers and, if necessary, external experts) in order to provide a uniform basis for risk assessment and comprehensive risk coverage. The actors will still be free to choose the risk assessment method they wish to apply. The guidelines should name threats, propose risk-minimising measures and define responsibilities. They should be published so that external experts can give their feedback.

Impact of measure and SC VE general assessment

The guidelines can be used to develop an effective and uniform basis for the design of risk assessments, helping all actors to assess the risks. This facilitates processes. The measure entails minor costs for the Confederation and has no immediate financial consequences for the cantons. The guidelines are to be drawn up before the implementation stage (Measure B.5).

No	**Measure**	**Timeframe implementation**	**Responsibilities**
B.5	Draw up and implement a new process for the risk assessment of completely verifiable system	Relaunch	FCh, cantons, system providers

Objective and description of measure

The risk assessments previously envisaged will be restructured. In future, all actors (FCh, cantons, system provider), not just the cantons, will draw up a risk assessment for their own area of responsibility. The responsibilities and the procedure are based on the guidelines in Measure B.4. The risk assessments will reflect the current situation in each case and the latest developments and findings will be incorporated into the assessment on an ongoing basis. The risk assessments are to be reviewed at least annually and whenever significant changes are made to the system. In addition, before each ballot, it will be ascertained whether specific risks have arisen and whether existing risks have increased. If risk-minimising measures cannot be implemented immediately, they are to be recorded in the set of measures (Measure A.8). Independent experts will be employed to assess the risks.

The FCh will amend the VEleS. Risk assessments from all actors must be available before trials are relaunched.

Dialog with the academic community

The experts are in favour of each actor (FCh, cantons, system providers) drawing up a risk assessment for its area of responsibility. They agree that risks should be assessed regularly using a systematic and comprehensive methodology. The risk assessments should be reviewed at least annually and in response to significant changes in the system. Ideally they will be reviewed in advance of each ballot (every three months). However, this is a tall order, and it might make sense to adopt a longer interval after a few years. The choice of method plays a secondary role. The risks arising from dependence on third-party suppliers and manufacturers (supply chain risks) were rated by half of the experts as particularly difficult to manage. A majority believes it would be useful to set up an expert committee to support the risk management process. The experts discussed the various pros and cons of publishing the risk assessments, and advise against publishing a detailed risk assessment immediately. However, it could be useful to publish graphs, statistical data and governance information and to clearly state the conditions under which a detailed risk assessment could be subsequently published.

Impact of measure and SC VE general assessment

Effective risk management can be ensured by each actor assessing and addressing those risks that are within their area of responsibility. The guidelines under Measure B.4 regulate the division of responsibilities and establish a common basis for assessing risks. It is important to establish continuous dialog and consultation between the various actors so that they can benefit from each other's experience (such as the experience of the Canton of Fribourg with the use of the risk-assessment method Octave Allegro). When identifying and assessing risks, the Confederation and the cantons can benefit from the advice of external experts.

Implementing this measure may incur additional costs for the Confederation and cantons, but these can be met with existing resources. There may be some minor costs involved in commissioning external experts.

No	Measure	Timeframe implementation	Responsibilities
B.6	Renew crisis management and conduct crisis simulation exercises	Relaunch	FCh (lead), cantons, system providers

Objective and description of measure

Effective and functioning crisis management is an important aspect in implementing a trustworthy and secure e-voting system. The Confederation and cantons have until now set out in a crisis agreement the details of how information, cooperation and communication will be managed if there is an incident in the e-voting process. This practice will be renewed to take account of developments in e-voting and to improve the efficacy of crisis management. To this end, a new crisis agreement will be drawn up. This will take the form of a framework agreement and have the following features:

- Trilateral agreement: The crisis agreement will be concluded between the FCh, the user cantons and the system provider.
- Processes, roles and tasks: The crisis management processes and the roles and tasks of the actors involved will be defined.
- Communication: The crisis agreement will contain a communication process between the actors involved (internal communication) and a process for coordinating communication to the outside (external communication). A suitable communication platform will be created for communication between the actors involved.
- Exercises: Crisis simulation exercises will take place at regular intervals (tbd) in order to improve processes and cooperation in crisis management.
- In the crisis agreement, the crisis scenarios will be adapted to the new risk assessments for completely verifiable systems. Existing structures at federal, cantonal and system provider level will be retained as far as possible in the crisis management arrangements.

The new crisis agreements are to be developed and signed before trials are relaunched. The first exercises may take place after relaunch.

Dialog with the academic community

The experts stressed that clearly defined processes and action and communication plans are key to crisis management. They also proposed that, in addition to the competent federal agency, the cantons concerned and the system provider, other federal agencies (GovCERT / MELANI), communications specialists and independent (technical) experts should be involved in crisis management.

Impact of measure and SC VE general assessment

This measure is necessary in order to adapt existing crisis management arrangements to the current situation and to enable a continuous improvement process. The implementation of this measure has a minor financial impact on the Confederation. Implementing crisis management and conducting crisis simulation exercises will not incur additional external costs for the cantons concerned.

No	Measure	Timeframe implementation	Responsibilities
B.7	Integrate e-voting into the Confederation’s critical infrastructure and regular exercises	Relaunch	FCh (lead), cantons and system providers

Objective and description of measure

Critical infrastructures as defined in the National Critical Infrastructure Protection Strategy will receive increased support from the Reporting and Analysis Centre for Information Assurance (MELANI) and the National Computer Emergency Response Team (GovCERT). This support would be valuable in analysing threats and investigating e-voting incidents. The purpose of this measure is to define cooperation on e-voting between the FCh, cantons, system provider and GovCERT / MELANI in order to ensure a prioritised approach to dealing with incidents. Crisis management will also take account of this cooperation.

Dialog with the academic community

The issue of e-voting as part of critical infrastructure was not explicitly discussed with the experts. The latter see the cooperation with GovCERT / MELANI as being advantageous.

Impact of measure and SC VE general assessment

This measure has no financial implications for the Confederation or cantons.

No	Measure	Timeframe implementation	Responsibilities
B.8	Further develop the plausibility checks for e-voting results	Relaunch: Initial discussions Study standardised method: 2022	Cantons

Objective and description of measure

Under the current law, plausibility checks of ballot results using e-voting must be conducted (Art. 27*i* para. 1 PoRO). The purpose of the plausibility checks is to obtain indications of unintended mistakes in the presentation of the results and manipulation of the results that may have occurred. To this end, statistical methods can be used insofar as the available data permits (Section 3.2.8 of the annex to the VEleS). The cantons conduct plausibility checks of e-voting results in various ways. There is to be more intensive discussion among the cantons and with the FCh so that experiences and approaches to problem-solving can be shared and best practices developed. The possibility of devising a standardised statistical method and the form this might take is being considered. The introduction of a standardised procedure would provide a further instrument for obtaining indications of mistakes or manipulation. The method must be applicable to the specific circumstances in each canton. The e-voting results of federal ballots should be published so it can be seen that plausibility checks of the results has been made (see Measure C.5). What information can be published in future regarding the cantons' plausibility checks should also be looked at. This will allow public scrutiny of the authorities' plausibility checks of e-voting results.

Initial discussions among the cantons and with the FCh on current practice is to take place before the relaunch of trials. The clarifications on a standardised method and the examination of what information should be published in relation to the cantons' plausibility checks going forward are to take place by 2022.

Dialog with the academic community

The topic of a standardised statistical method for plausibility checks was discussed. There is currently no such method but the experts believe that one could be developed. They do not believe that statistical methods can detect manipulations, but plausibility checks can provide indications of irregularities; based on these indications, investigations into possible manipulations can be carried out. However, the absence of indications is not a guarantee that manipulation has not taken place.

Impact of measure and SC VE general assessment

The plausibility checks already required in the cantons need to be developed further. When implementing this measure, the effects on the other voting channels as well as the efforts already underway in various cantons to improve plausibility checks of ballot results in general must be taken into account.

This measure has no financial consequences for the Confederation. The financial impact on the cantons depends on whether and which plausibility methods are developed, but it is likely to be inconsiderable.

No	Measure	Timeframe implementation	Responsibilities
B.9	Amend authorisation procedure	Relaunch	FCh with cantons' involvement

Objective and description of measure

The implementation of a range of measures for the resumption of trials makes it necessary to adapt the procedures in the authorisation procedure. The measures to reorganise the responsibilities for independent examinations (Measure B.1) and the adaptation of the transparency requirements (Measures C.2 and C.3) affect this in particular. In addition, the involvement of independent experts in the authorisation process and ongoing risk management must be taken into account. The current authorisation process framework set out in the PoRO (licensing by the Federal Council, authorisation by the FCh) will still apply in the new trials.

The FCh will amend the authorisation procedure in implementation of this measure. It is currently revising its set of requirements for the authorisation procedure. In addition, the FCh will examine the extent to which the Federal Council's authorisation decision can be divided into a system-related and a canton-specific part.

Dialog with the academic community

The design of the authorisation process was not explicitly addressed in the dialog with the academic community. In the assessment of e-voting systems, great importance is attached to the involvement of competent and independent persons and specialist bodies.

Impact of measure and SC VE general assessment

The authorisation process needs to be adapted in particular to take account of the newly designed independent examinations. It is essential that the FCh and the cantons concerned agree at an early stage to coordinate processes. As stated under Measure B.1, the FCh will ensure that the cantons are involved in the examinations. It will be in regular contact with the cantons. Dividing the authorisation decision into a system-related and a canton-specific part is intended to create a certain degree of planning security for cantons applying for a authorisation to use a system that has already been approved. If they use the same version of the system as other cantons, they can be sure that the general system part meets the federal requirements.

Implementation of this measure has no financial consequences for the Confederation or cantons.

No	Measure	Timeframe implementation	Responsibilities
B.10	Revision of processes, roles and tasks long term	Long term	Working group on the future of Vote électronique (AG Zukunft VE)

Objective and description of measure

The responsibilities, roles and tasks of the Confederation, cantons and system providers have a direct influence on the (security-related) design of e-voting systems. They are to be reviewed over the long term and set out in a strategy. This will allow more thorough changes to the responsibilities, roles and tasks to be discussed. The Confederation and cantons can draw up measures that take into account the changed situation regarding the number of system providers, governance and funding requirements for e-voting. The current distribution of tasks, competences and responsibility reflects the federalist division of tasks in the field of political rights. Processes, roles and tasks must be developed and defined in such a way that security is continuously ensured and improved. This should take account of the technical competencies and human resources available at the federal and cantonal levels, as well as dependence on the system provider.

The working group on the future of Vote électronique (AG Zukunft VE), which has been proposed by the Swiss Conference of Cantonal Chancellors to deal with long-term issues, will be responsible for defining any issues to be dealt with and for implementing the measure. The working group will look at whether and for what tasks in the field of political rights more centralised e-voting structures could be of benefit in the future. This work is to be embedded in the overarching e-government strategy and structure, and will encompass all aspects of e-democracy, above and beyond e-voting. A draft mandate for the AG Zukunft VE has been drawn up by the cantons; the Swiss Conference of Cantonal Chancellors will decide the next steps to be taken.

Dialog with the academic community

The review of processes, roles and tasks was not discussed in the dialog with the academic community as a separate topic but in the context of individual measures (such as independent examinations).

Impact of measure and SC VE general assessment

Implementation of this measure has no financial consequences for the Confederation or cantons.

C. Increasing transparency and trust

No	Measure	Timeframe implementation	Responsibilities
C.1	Restrict electorate permitted for completely verifiable systems	Relaunch	FCh

Objective and description of measure

In accordance with the Federal Council's decision of 26 June 2019, the transfer to regular operation will be postponed for the time being and trial operations will continue. Only completely verifiable systems will be used in future. To make clear that e-voting trials are still being conducted, the previous restrictions on which voters may vote online will still apply, even though completely verifiable systems will be used.

The FCh will amend the legal provisions to restrict the voter groups permitted to use e-voting in the trials of completely verifiable systems. Limits will be 30 per cent of the cantonal electorate and 10 per cent of the national electorate. As in previous trials, the cantons are responsible for ensuring compliance with the cantonal limits (voter registration procedure, use in pilot communes or only for Swiss voters abroad). Swiss voters abroad will still not be considered when the limits are calculated. The limits will apply in the next phase of trials so that experience can be gained with completely verifiable systems and trust can be built up as e-voting is gradually introduced.

Dialog with the academic community

Various positions are held in the discussion about limiting the number of voters. A majority of the experts is in favour of applying limits in the trials in order to minimise risk. Opinions are divided into two roughly equal groups over whether limiting the number of voters also helps to strengthen trust. One group believes that keeping the trials small-scale helps to build up acceptance and trust long term. The second group is of the opinion that limiting the number of voters does not affect trust and that it may even erode trust, as limiting the number of voters may suggest that the system is not reliable. In any case, limits should be a temporary measure only.

Impact of measure and SC VE general assessment

This measure is an effective instrument because it emphasises that trials are still being conducted and e-voting is being introduced gradually. By continuing the previous practice of limiting the number of voters using e-voting, trust in the system can be strengthened. The limits of 30 per cent of the cantonal and 10 per cent of the national electorate shall apply in the first phase of the new trials. The limit may be increased or removed entirely once the completely verifiable systems have been shown to be reliable in stable trial operation.

Implementation of this measure has no financial consequences for the Confederation. The Confederation will ensure the national electorate limits are observed in the authorisation procedures with the applicant cantons. The cantons must implement measures to ensure the cantonal limits are observed. Depending on the choice of instrument, this could lead to medium-scale costs (e.g. for the introduction of an application procedure). Cantons that have planned to roll out e-voting for the whole of their electorate and have not implemented measures to limit the number of voters may incur additional costs.

The limits on voter numbers may mean that some cantons are unable to introduce e-voting, for example if the national limit has already been met or if they wish to offer e-voting to all their voters, not just some. In practice, it is unlikely that the proposed limits will lead to such constraints. As soon as such constraints are observed, the measure will be reviewed.

No	Measure	Timeframe implementation	Responsibilities
C.2	Draw up more detailed requirements for disclosing the source code	Relaunch	Requirements: FCh Disclosure: Cantons, system providers

Objective and description of measure

Experience with disclosing Swiss Post's source code showed that there is a need for action in this area. The requirements for the published documents must be updated to contain details of the following:

- Disclosure of the source code, software documentation and files with relevant input parameters;
- Publication of aids and supplementary documentation so that competent persons can efficiently compile, execute and analyse the system in their own infrastructure;
- Publication where possible of documentation on infrastructure, third-party software and operating processes. This should contain, as a minimum, a summary of the key elements.
- The presentation of the disclosed documents is in line with standard practice.

The terms of use should state the following:

- Access to the source code is provided free of charge and anonymously. Persons wishing to access the published information will not be required to give proof of their identity.
- The source code may be used for ideational and in particular scientific purposes. This includes exchanging information about any errors detected and the right to publish. This right is explicitly granted by the owner.
- Persons complying with the terms of use will not be prosecuted. Persons violating the terms of use will only be prosecuted if the source code or parts of it are used commercially or productively. The terms of use refer to this limitation of liability.
- It is sufficient to refer to the terms of use in the licence agreement. If possible, there should be no requirement for users to give a declaration of intent.

The FCh will revise its requirements before the tests are resumed. The SC VE would like to see future systems and system components published under an open source licence (OSL). Furthermore, the current system provider Swiss Post is looking at whether it is also possible to place already developed source code components of its completely verifiable system under an OSL.

Dialog with the academic community

The experts stress that transparency is a very important basis for effective public scrutiny. Disclosing the source code and its documentation with the lowest possible access barriers is an important instrument in this respect. Various options for improving the existing source code disclosure provisions were discussed. There should be no requirement to sign a non-disclosure agreement.

The experts believe that disclosing the source code under an OSL would be more beneficial than publishing it under a proprietary licence. With an OSL, the objectives of transparency, public scrutiny, public trust, and building a community of professionals can be more effectively achieved. Disclosure under a proprietary licence could also lead to these objectives being reached, but not to the same extent. The experts also recommend open source publication because it allows the cryptographic elements to be used and further developed in other applications. The development and security of e-voting systems could benefit from such a re-use.

Many of the experts advocate disclosing the source code and documentation at an early stage. A pre-release version could be published before the final version, which will be used productively. At the same time, it was pointed out that the published documentation should be of good quality and that updates should be made clear. The experts are also in favour of publishing all documents necessary to understand how the system functions and is operated. It should also be possible for individuals to test the system on a private computer.

Impact of measure and SC VE general assessment

The disclosure of the source code for public scrutiny is important and the development of an appropriate community of experts should be promoted. Action needs to be taken regarding disclosure of the source code. Before trials are resumed, the requirements on the documents to be published and on the terms of use will be specified and adapted as described in the measure.

Independent of the source code disclosure and how this is done, there is still the question of whether an e-voting system source code should be published under an open source licence (OSL). In simple terms, such a licence allows third parties to use the source code, to modify it and to use it for their own purposes (including productive use). The SC VE would like to see future systems and system components published under an open source licence (OSL). However, publication of Swiss Post's system source code under an OSL is not a prerequisite for use of its system. Furthermore, the current system provider Swiss Post is looking at whether it is also possible to place already developed source code components of its completely verifiable system under an OSL.

The disclosure of the source code can lead to high costs, but implementing this measure should not have any direct additional financial consequences for the Confederation and the cantons.

No	Measure	Timeframe implementation	Responsibilities
C.3	Run a bug bounty programme	Relaunch	Requirements: FCh Run by: Cantons, system providers

Objective and description of measure

In order to involve independent experts and subject the system to public scrutiny, a bug bounty programme will be run for the disclosed source code and e-voting system documentation. This should meet the following requirements, among others:

- The system provider runs an ongoing bug bounty programme. The programme is to be launched in advance (around three months) of the submission of a definitive application for an basic licence from the Federal Council.
- There will be a financial reward for any errors detected according to their severity. The amount of the reward will be based on the 2019 PIT.
- Participants can analyse the source code in their own infrastructure based on the system in operation. To be entitled to remuneration, it is sufficient to identify vulnerabilities by means of the source code; a successful attack does not have to take place.
- There are three elements to the bug bounty programme:
  - Search for errors in the disclosed documentation or source code (static test)
  - Search for errors by analysing the executable system in a private infrastructure (dynamic test)
  - Attacks on the provider's infrastructure (internet test). The aim of this test is solely to infiltrate the infrastructure. Denial-of-Service (DoS) and social engineering attacks may be excluded from the bug bounty programme. Attacks on infrastructure may be prohibited in justified cases (e.g. during a ballot).

Responsibilities and handling of notifications:

- The system provider will be responsible for the bug bounty programme. It will run the programme and receive and categorise notifications. It will justify its decisions to the participants concerned and publish all confirmed findings. In addition, the system provider undertakes to remedy errors.
- The FCh will establish the basic conditions for the bug bounty programme.
- The Confederation and the cantons will receive unrestricted access to the notifications and to the system provider's responses. A summary of the notifications and the measures taken as a result of these notifications must be submitted in the authorisation procedure.

The terms of use should include the following:

- It is possible to participate anonymously. Participants must only be required to disclose their identity for a reward to be paid out in the bug bounty programme.
- Participants may publish information about errors or suspected errors. In this they may be required to respect a deadline (see below).
- Participants may be required to observe the following rules in a spirit of 'responsible disclosure':

- Errors must be reported immediately.
- Errors may not be publicly disclosed immediately; any embargo set by the FCh, cantons and system provider must be respected.
- Information on suspected errors must be handled responsibly. Participants may not unnecessarily publicise any security vulnerabilities that are in the process of becoming apparent. Information about vulnerabilities will only be shared and discussed with people who are presumed to be able and willing to deal with the issue and who will do so responsibly.

- There shall be no sanctions for violations of responsible disclosure. The terms of use refer to this limitation of liability.
- For the internet test: The fact that the system provider consents the test taking place protects participants from prosecution unless the attacks do not form part of the test.

The FCh, in consultation with the cantons, will adapt the statutory provisions to provide for a bug bounty programme before the resumption of trials. In consultation with the cantons and the system provider, it will define the basic framework conditions of the bug bounty programme in a catalogue of requirements. An escalation option for participants who disagree with the system provider's decision should also be considered.

The internet test is to be conducted on the productive system before the resumption of trials. Then a decision can be made on further steps to be taken based on the test findings. There are two options: the internet test will either be regularly repeated on the productive system or will be run permanently on a parallel system.

Dialog with the academic community

The experts consider public scrutiny to be very important. Vulnerabilities should be disclosed and a response given to inputs from the public. The experts recommend implementing an ongoing bug bounty programme with financial rewards. This should not be restricted to successful attacks on the provider's infrastructure but also involve identifying errors in the system documentation and source code. Attacks on the system provider's back-end infrastructure, physical intrusion, DoS and social engineering attacks will not form part of the bug bounty programme, but can be tested in other ways, e.g. commissioned penetration testing. The Confederation or an independent committee will be responsible for defining the objectives and the conditions.

Impact of measure and SC VE general assessment

A programme to identify errors can contribute to the ongoing improvement of the system. The bug bounty programme will strengthen public scrutiny, and could help building a community of specialists and increasing public trust. The FCh will establish the basic conditions for the bug bounty programme. The system providers will, for the time being, be responsible for defining the details of the bug bounty programme, categorising errors and determining the size of the financial rewards. This will be done in consultation with the NCSC, the FCh and the cantons. Care must be taken to ensure that appropriate financial rewards are given and that reported vulnerabilities are dealt with effectively and credibly.

Cost estimates for the internet test options (not incl. financial rewards):

- bug bounty programme with ongoing error search (static and dynamic test) and a recurring internet test:
  - One-off costs: CHF 230,000-290,000
  - Recurring costs (average): CHF 55,000-70,000 / year
- bug bounty programme with ongoing error search (static and dynamic test) and an ongoing internet test:
  - One-off costs: CHF 255,000-360,000
  - Recurring costs (average): CHF 550,000-650,000 / year

The FCh is of the opinion that the costs should be borne primarily by the cantons. Co-financing by the Confederation for the running of the programme should be examined, as should contributions by other federal agencies.

No	Measure	Timeframe implementation	Responsibilities
C.4	Publish examination reports relevant to authorisation	Relaunch	FCh, cantons, system providers

Objective and description of measure

The Confederation, cantons and system providers ensure there is sufficient transparency regarding examination results that are relevant to authorisation. This will allow for peer review and help to create trust and build a community of professionals. This measure regulates the following aspects:

- Reports, supporting documents and certificates produced as part of the examinations in accordance with point 5 of the Annex to the VEleS must be published; the entity commissioning the examination report is responsible for publication.
- The published reports must be clear and comprehensible. If reference is made in the reports to further documentation, this should also be made public. If additional documents cannot be made public, a summary of the relevant aspects of the unpublished documents should be provided in order to ensure that the examination reports are comprehensible.
- If good reason is given, in some exceptional cases it may not be necessary to publish the examination reports, for example if publication would increase a risk or reasons of data protection or internal security policies speak against it.
- Any response by the examined entity to the published examination report should also be published.

The FCh will amend the legal provisions before the resumption of trials.

Dialog with the academic community

The experts agree that transparency is the prerequisite for effective public scrutiny. The majority of the experts also recommend publishing examination reports. However, care must be taken to ensure that the examination reports are of high quality and comprehensible, otherwise publication could lead to a loss of trust.

Impact of measure and SC VE general assessment

It is necessary to create greater transparency with regard to examination reports that are of relevance to the authorisation procedure. The target audience for the published reports is primarily specialists and, less directly, the general public. The intended publication of the examination reports should be borne in mind during the process of appointing experts; publication should be discussed with them when they are appointed. The implementation of this measure may have a significant financial impact on the contracting authority, primarily on the Confederation.

No	Measure	Timeframe implementation	Responsibilities
C.5	Publish e-voting results in federal ballots	Relaunch	Requirements: FCh Publication: Cantons

Objective and description of measure

It is important to create transparency for the public with regard to e-voting results. The cantons should therefore publish the e-voting results of federal ballots. In this way the public can compare the results of e-voting with the overall result and conduct plausibility checks. This will generate greater trust in e-voting. In addition, publication of the e-voting results will provide data and information that could provide an interesting basis for research.

The FCh will adapt the VEleS so that e-voting results can be published down to communal level. Provision should be made for exceptions to ensure that voting secrecy is guaranteed at all times.

Dialog with the academic community

The majority of the experts are in favour of e-voting results being published. The main reasons for this are transparency and trust. They also point out that by publishing the results, system vulnerabilities can be identified immediately. Voting secrecy and data protection must be ensured at all times.

Impact of measure and SC VE general assessment

E-voting results are to be published. The cantons are concerned that publishing the results in detail down to commune level may prove problematic. The legal bases should provide for exceptions so that voting secrecy is preserved at all times.

Implementation of this measure has no financial consequences for the Confederation; for the cantons, a minor financial impact is projected.

No	Measure	Timeframe implementation	Responsibilities
C.6	Increase public involvement	Concept: Relaunch	FCh with involvement of the cantons and system providers

Objective and description of measure

The public is to be invited to be more involved in the establishment of e-voting. Various measures proposed in the redesign process will promote transparency and the creation of a community of experts. In addition, the Confederation, cantons and system providers will develop a concept on how to involve the general public to a greater extent. This will include proposals for active communication. Events and information activities will be run on an ongoing basis with a focus on the general public as well as on politicians, experts and interest groups. The activities may include:

- holding and participating in information and discussion events (conference for politicians, parties, associations and academic community; E-VoteID Conference in Bregenz);
- running idea competitions (e.g. for social engineering attacks) and hackathons;
- operating an information platform.

An initial version of this concept will be drawn up before the relaunch of trials, with the FCh taking the lead. The planned activities will take place on an ongoing basis. If possible, the first activities should already take place before the relaunch of trials. For example, the Canton of St Gallen has already begun developing an information platform where interested persons can obtain general information about e-voting.

Dialog with the academic community

The experts underline the importance of transparency and public communication. The method of communication be adapted to the target audience (specialists or general public). Specific technical events such as hackathons and idea competitions are considered suitable instruments to interest and involve specialists in e-voting. For the general public, meanwhile, it is necessary to choose an approach that promotes the understanding of and trust in e-voting, for example citizen science projects and workshops.

Impact of measure and SC VE general assessment

It is very important to strengthen transparency and communication with the general public, politicians and interest groups, as well as to create a community of experts. Drawing up a concept involves minor costs for the Confederation and none for the cantons. However, implementation may result in costs for the Confederation and cantons.

D. Stronger connection with the science community

No	Measure	Timeframe implementation	Responsibilities
D.1	Draw up a concept for the academic monitoring of the trials and for the dialog with external experts	Concept: 2021	FCh with involvement of cantons

Objective and description of measure

The e-voting trials are to be scientifically evaluated and monitored on an ongoing basis. In addition, the Confederation and the cantons will maintain an ongoing dialog with the academic community and the competent specialist entities. They will submit questions, respond to comments, actively participate in discussions and provide the necessary infrastructure and resources for discussion. The Confederation and cantons will also commission academic studies in areas where greater depth of understanding is required.

The Confederation and the cantons, in collaboration with representatives of the academic community, will draw up a concept for the monitoring process and the dialog with external experts for the period 2022–2025, to include the funding involved. The FCh will take the lead in the concept development.

Dialog with the academic community

The experts emphasise that constant dialog and cooperation between the authorities and the academic community are key to the further development of e-voting. They stress in particular the importance of involving independent experts in the conception and development of the system, in public and commissioned testing and in risk assessment, and the need to promote research and the creation of a community of specialists. In addition to technical issues, the dialog with the academic community should also increasingly address social science aspects. To provide a holistic view and thus improve voting security as a whole, the security discussion should include not only e-voting but also the other voting channels.

Impact of measure and SC VE general assessment

Continuous scientific monitoring is essential to ensure security and the scientifically sound development of e-voting. In drawing up the concept, the objectives and expectations of scientific monitoring must be clearly established. In particular, the responsibilities of the Confederation and the cantons as well as funding for the monitoring process must be defined. Developing the concept involves few costs for the Confederation and cantons; implementation will have a financial impact depending on the mode and the degree of the community's involvement.

No	Measure	Timeframe implementation	Responsibilities
D.2	Involve independent experts	In each individual measure	FCh with involvement of cantons

Objective and description of measure

In their work, the Confederation and the cantons will involve independent experts and specialist entities from relevant academic disciplines as well as other organisations where this makes sense and offers added value, in particular with regard to the measures defined in the redesign of trials:

- Definition and commissioning of independent examinations by the FCh
- Design and implementation (of e-voting service and related processes run by cantons and their partners)
- Assessment of authorisation applications and esp. of examination results
- Review of Confederation's security requirements
- Development of concepts for improvement measures and their scheduling in the action plan
- Development of bases for risk assessments
- Assessment of individual risks
- Development of measures aimed at encouraging participation of independent experts
- Workshops / seminars
- User friendliness/ ergonomics
- Finding and assessing solutions to distributed printing

The form of involvement will be discussed with regard to the respective areas of responsibility. The involvement of suitable federal agencies in some tasks may also be considered.

Dialog with the academic community

See explanations of individual measures and of Measure D.1.

Impact of measure and SC VE general assessment

See explanations of individual measures and of Measure D.1. This measure has essentially no financial implications for the Confederation or cantons. The costs involved will be listed with each individual measure.

No	Measure	Timeframe implementation	Responsibilities
D.3	Develop a concept to set up an academic committee	Concept: 2022	FCh with involvement of cantons

Objective and description of measure

An academic committee will be set up to advise the Confederation and cantons. The committee will advise on cooperation with the academic community (see Measures D.1 and D.2) and will also be able to perform individual tasks itself. Consideration needs to be given to how it can be integrated into existing system assessment processes as well as to how it might support the cantons. The committee's tasks and composition are to be defined. A concept for the years 2022–2025 is to be drawn up by the Confederation and cantons with the FCh as lead.

Dialog with the academic community

In addition to the comments made under Measure D.1, the experts advocate the creation of an academic committee charged with advising the authorities. The committee could have a supervisory function but would not take on any regulatory tasks. The idea was also put forward of setting up a citizens' advisory board, which could take on the task of promoting public information, public trust-building and user-friendliness.

Impact of measure and SC VE general assessment

Besides the general expert supervision of the trials, the creation of an academic advisory body is advocated to support the Confederation and the cantons in an advisory capacity. Any concept should establish the advisory body's tasks, the question of possible financial compensation and responsibility for the costs. Developing the concept has no financial implications for the Confederation and cantons.

4. Overall assessment and further steps

4.1 Summary of main features and implementation schedule

Implementing the above measures will meet the identified need for action in resuming e-voting trials in the medium to long term. A continuous improvement process is necessary to ensure the quality and security of systems, the efficacy of controls and processes, and the strengthening of trust in e-voting. This should entail closer dialog with the academic community and greater involvement of independent specialists and of the public. Various measures must be implemented and legal provisions amended before trials can be relaunched. This will be the first stage of improvements, while the implementation of the medium to long-term objectives will be an ongoing process. The main features of the measures can be summarised as follows:

Further development of the systems

– Ensure the quality of the system by defining quality criteria more precisely and establish clear development and deployment processes	Relaunch; ongoing improvement process
– Ensure the forensic readiness of the systems used by means of effective detection and investigation of incidents	Relaunch; ongoing improvement process
– Create a joint, public planning instrument by the Confederation and the cantons for the ongoing implementation of security-related measures	Relaunch; ongoing monitoring
– Improve verifiability by introducing greater diversity and independent individual components	Medium term; consolidation up to two years after relaunch

Effective control and oversight

– Ensure efficacy of independent system examinations	Relaunch
– Set up a regulated process to deal with identified and suspected non-conformities	Relaunch
– Introduce improvements in risk assessment and crisis management	Relaunch; ongoing improvement process
– Further develop plausibility checks	Ongoing, first stage by 2022
– Adapt and revise processes in authorisation procedure, as well as roles and tasks	Relaunch and long-term revision

Increasing transparency and trust

– Limit number of voters in trials	Relaunch
– Create greater transparency and easier access to system information, examination reports and findings	Ongoing
– Promote creation and involvement of a community of specialists and of the public (politicians, specialists, interest groups and general public) for ongoing public scrutiny	

Stronger connection with the science community

– Ongoing support by academia and involvement of independent experts	Cross-sectional topic, ongoing implementation
– Set up an academic committee to support and advise the Confederation and cantons	Medium term

4.2 Cost implications for the Confederation and cantons

4.2.1 Measures for the relaunch and the first stage following relaunch

Some of the measures for relaunching trials have no or only minimal direct cost implications for the Confederation and cantons. It may be assumed that the Confederation and the cantons can meet these costs in accordance with their responsibilities. However, the following measures, also foreseen for the relaunch or the first stage after relaunch, have a greater financial impact:

- Manufacturer-independent verifier and control components (Measure A.4): According to initial estimates, implementation of the first stage (drawing up a study on independent online control components) will incur low to medium costs for the cantons.
- Weakening of trust assumptions in the printing process (Measure A.5): According to initial estimates, adapting the cryptographic protocol in the first stage will incur high costs.[19] The cantons must bear these costs under the current division of responsibilities. The cantons cannot bear these costs alone; co-funding with the Confederation is to be considered.
- Public bulletin board (Measure A.6): According to initial estimates, implementation of the first stage (drawing up a study) will incur medium costs for the Confederation.
- Independent system examinations (Measure B.1): This measure has considerable financial consequences for the Confederation, which in future will be responsible for commissioning these examinations – with the exception of ISO 27001 system provider certification – and will thus also bear the costs incurred. The Confederation is able to fund these independent examinations provided the required budget is approved.
- Bug bounty programme (Measure C.3): An initial cost estimate by Swiss Post suggests that running a bug bounty programme will incur medium to high costs (depending on its form).[20] In addition, there is the cost of rewarding error notifications. According to the division of responsibilities, these costs are to be met by the cantons. However, the cantons cannot bear these costs alone; co-funding with the Confederation is to be considered.

4.2.2 Medium- to long-term developments

The measures are important to ensure the security and trustworthiness of e-voting and are thus central to its future. Funding for the medium- to long-term developments is not secured. Funding is critical in particular for the three measures listed below. For these measures, studies and in-depth investigations are planned as a first step, and these are expected to incur low to medium costs. Subsequent implementation, however, will incur high costs.

- Manufacturer-independent verifier and control components (Measures A.4): The cost of using manufacturer-independent online control components is very high. According to current responsibilities, this is to be borne by the cantons. However, the cantons are unable to bear the estimated costs.[21] Co-funding with the Confederation is to be considered.
- Weakening of trust assumptions in the printing process (Measure A.5): The cost of implementation is high. According to current responsibilities, this is to be borne by the cantons. However, the cantons are unable to bear the estimated costs.[22] Co-funding with the Confederation is to be considered.
- Public bulletin board (Measure A.6): Initial estimates suggest that implementation would incur high costs.[23] Responsibility for funding is yet to be decided.

[19] One-off costs of CHF 850,000-1 million.

[20] Cost estimate for bug bounty programme with recurring internet test: One-off costs of CHF 230,000-290,000 and recurring costs of CHF 55,000-70,000 / year. Bug bounty programme with ongoing internet test: One-off costs of CHF 255,000-360,000 and recurring costs of CHF 555,000-650,000 / year.

[21] Control components: One-off costs of CHF 1.8-2.2 million and recurring costs of CHF 600,000-800,000 / year. Verifier: One-off costs of CHF 0.9-1 million and recurring costs of CHF 200,000 / year.

[22] One-off costs of CHF 700,000-900,000 and recurring costs of CHF 100,000 / year.

[23] One-off costs of CHF 600,000 and recurring costs of CHF 200,000 / year.

4.2.3 Guaranteeing funding long term

Funding options

Ensuring the security of e-voting involves high costs and even higher costs can be expected in the future. Funding must be guaranteed long term. If the cantons are unable to bear the costs of materially important measures, new funding options must be considered.

The following funding options will be investigated:

- eGovernment Switzerland's implementation plan has budgeted CHF 250,000 annually for e-voting up to 2023. This is to fund individual projects and studies; however, it is not enough to fund medium- and long-term developments. The possibility of increasing funds earmarked for e-voting in the eGovernment Switzerland implementation plan and of funding individual projects from other eGovernment Switzerland funds will be examined.
- New funding sources in the cantons.
- New funding sources in the Confederation.

In addition, all the actors involved should, where possible, exploit synergies in implementing the measures. To achieve this, cooperation with existing structures will be strengthened. For example, the potential for exploiting existing resources at the National Cyber Security Centre (NCSC) and the interfaces with existing processes at the FCh, in the cantons and at Swiss Post can be examined.

View of the cantons

For the cantons it is clear that e-voting systems can only be implemented if they are secure. The cantons' ability to fund e-voting is limited. In many of the cantons the political pressure on the resources earmarked for e-voting has risen and may continue to rise if it is not possible to implement a productive e-voting system for some time yet. The cantons feel it is unrealistic to request further funds. Moreover, in the coming years only very few cantons will be able to offer e-voting. The few cantons that intend to do so are unable to bear the costs of the measures defined for the relaunch.

Until now, the cantons were able to bear the costs involved. Going forward, it may be assumed that Swiss Post will pass on the cost of implementing new requirements to the cantons. The price per voter is of relevance to the cantons; any additional costs incurred by Swiss Post can only be met if a larger number of voters is approved for e-voting and more cantons become involved.

When deciding on the implementation of measures, the cantons' limited room for manoeuvre with regard to funding must be taken into account. The funding question must be one of the factors in deciding whether a measure is implemented. Alternative funding solutions must be found for those measures requiring more money than the cantons can provide. The possible extent of co-funding by the Confederation should be examined.

View of the FCh

Guaranteeing security is central to the use of a trusted electronic voting channel. In this, the authorities and system providers will be increasingly confronted with high costs. However, the FCh believes that it is precisely those measures that are associated with high costs that bring considerable security gains. These are, in particular, public scrutiny, the involvement of academics and improved security and verifiability based on scientific findings. Implementing these measures is thus central to the development of e-voting. This assessment is also in line with the outcome of the dialog with the academic community. Since these measures cannot be fully funded from current federal and cantonal budgets, new funding solutions must be sought. The FCh believes that the Confederation and cantons should strive to implement these measures and should already commit to ensuring the necessary funding is obtained.

5. Conclusions

This SC VE final report containing a set of measures for the redesign of e-voting trials meets the objectives defined by the Federal Council. The measures set out the focus of the work to be carried out in the short, medium and long term by the Confederation and the cantons over the next few years. The implementation timeframe and responsibilities are also defined. The focus is on continuous improvement of the system and no longer on a seal of quality in the form of certification. The security, trust and acceptance of e-voting are to be continuously improved with the involvement of experts from academia and industry. The Confederation and cantons will continuously monitor the measures and adapt them where necessary.

In a first stage, measures for the resumption of trials will be implemented and the statutory provisions adapted accordingly. In parallel to this, work will be carried out on implementing the medium- to long-term measures. This will allow the cantons to go ahead with running the trials. Continuing the trials in some cantons will prevent the loss of existing resources and know-how as well as investments already made by the cantons and Swiss Post as system provider. It also allows all actors to gain valuable experience in the use of completely verifiable systems. A number of the measures, such as retaining the limit on the numbers permitted to use e-voting, underline the trial nature of the operations. The motto 'security before speed' will continue to apply. In a second stage, work will be carried out on implementing the medium- to long-term measures.

Ensuring the security of the systems used is top priority. The measures to redesign the e-voting system include a more precise definition of safety requirements, more effective control and supervision with the involvement of the academic community, and an improvement in risk management. The Confederation and the cantons also want to increase public trust in e-voting by increasing transparency and seeking greater cooperation with the public and the academic community. The existing community of experts in the field of e-voting is to be enlarged. The academic community is seen as playing an important role. Independent experts will be increasingly involved in developing basic principles, monitoring the trials and, in particular, examining the systems. There will also be greater opportunity for public scrutiny. The information on the system used (in particular documentation and source code) will be published, thus making the documents required for scrutiny publicly available. Examination reports and the results of votes cast via e-voting channel will be published. In this way, voters and experts will be able to form their own picture and provide feedback to the authorities at any time. This feedback will contribute to the further development and ongoing improvement of e-voting.

Transparent communication with the public plays an important role in generating public trust in e-voting. The Confederation and the cantons must inform the public about security issues. This is an important task in technically complex areas such as e-voting. The Confederation and cantons therefore want to improve public information and communication and implement measures accordingly.

It is essential that the background for the use of e-voting is assessed on an ongoing basis and in the light of current developments. By implementing a range of measures and amending the statutory provisions, it should be possible to continue e-voting trials. Ongoing developments and continuous improvements are important aspects in ensuring the security and credibility of e-voting. Long-term funding must be secured so that these ongoing developments and continuous improvements are possible. The amount of federal and cantonal funding currently earmarked is insufficient. The Confederation and cantons therefore need to look at other funding options.

Appendix: Catalogue of measures

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
A.	**Further development of the systems**				
A.1	Draw up precise criteria for source code quality and documentation quality	Specification of existing quality criteria that the source code and its documentation must meet. By setting clear criteria the high quality of the e-voting systems can be assured. Furthermore, this should make it easier for tests to be carried out by all actors, including the public. Furthermore, the quality assurance process in the software development should also take account of these criteria.	Relaunch	Requirements: FCh Implementation: Cantons, system providers	Confederation: none Cantons: none
A.2	Improve quality assurance in development of e-voting systems	Specification of quality assurance requirements in the development of e-voting systems. The following goals are to be attained: – Traceability and review of adjustments – Continuous traceability in both directions between the individual elements of the documentation (protocol, specification, architecture, etc.) and the source code – Integrate the results of test processes into the development process – Ensure conformity with legal requirements and maintain this throughout the entire life cycle	Relaunch	Requirements: FCh Implementation: Cantons, system providers	Confederation: none Cantons: none
A.3	Use a proven and traceable build and deployment method	The system provider is further required to use a method for system deployment that ensures traceability from source code to installation in the production phase (build and deployment). The following goals are to be attained: – The build and deployment method ensures that the deployed software conforms to the published, tested and approved version (traceability). – Moreover, the build and deployment method will help prevent the manipulation of system components as much as possible. – It must be ensured that the development tools and libraries used for the software do not introduce significant vulnerabilities into the system that expose it to attack. A process is being developed for dealing with non-conformities (see Measure B.3).	Relaunch	Requirements: FCh Implementation: Cantons, system providers	Confederation: none Cantons: low

[24] Estimates of additional costs (external costs or additional resources) for the Confederation and cantons are shown. Costs incurred by the system provider are shown in the cantonal costs, insofar as they are passed on.

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
A.4	Deploy manufacturer-independent components (verifier / control components)	The FCh and cantons draw up more detailed specifications for the use of manufacturer-independent components. Priority is given to developing bases for manufacturer-independent control components used to generate verification codes and store votes until counted (online control component). The SC VE intends to deploy manufacturer-independent online control components for about five years after relaunch provided the necessary funds are available. A critical mass of active cantons is needed to share the financial burden; a sufficient number of cantons must agree to meet the costs to be borne by the cantons. A further proviso is that no significant reasons against implementation arise unexpectedly at a later date. As a first step, a study will be carried out to establish who should be responsible for awarding contracts, conducting system maintenance, conducting operational processes and handling any technical issues, and how these aspects should be carried out. The study will also clearly state the implications for the cantons in terms of both operational processes and costs. In addition, it will propose a clear implementation plan (according to an initial assessment by the cantons, implementation will take between three and five years). The study will provide a basis for making the decision regarding implementation. The cantons are responsible for organising the study. Once the study has been completed, the FCh and the cantons will submit a proposal to the SC VE on further action to be taken.	Study and request for online control components to SC VE: up to 2 years after relaunch Conditional implementation: c. 5 years after relaunch	Online control components study: Cantons with FCh involvement	<u>Online control components study</u> Confederation: none Cantons: low to medium <u>Estimation of possible implementation following study</u> Confederation: Co-funding to be considered Cantons: very high Control components: - One-off: CHF 1.8-2.2 million - Recurring: CHF 600,000-800,000 / year Verifier: - One-off: CHF 0.9-1 m - Recurring: CHF 200,000 / year
A.5	Weaken trust assumptions in the printing process and in the software that generates cryptographic parameters	The trust assumptions in the printing process and in the software that generates cryptographic parameters should be weakened. Using manufacturer-independent software, it should be possible to determine that cryptographic parameters, and in particular the verification codes, have been generated randomly. To achieve the desired entropy, at least four control components must be used to generate private values. Randomly selected polling cards are to be scrutinised to determine whether the values have been correctly printed with regard to the checked values. The SC VE intends to adapt the parameter generation as well as the printing process within about four years after the relaunch provided the necessary funds are available. A critical mass of active cantons is needed to share the financial burden; a sufficient number of cantons must agree to meet the costs to be borne by the cantons. A further	Extension / adaptation of the cryptographic protocol: One year after relaunch Request to SC VE: up to two years after relaunch Conditional implementation: c. 4 years after relaunch	Issues to be clarified for requirements: FCh Implementation: Cantons	<u>Consolidation and adaptation of the cryptographic protocol</u> Confederation: low; Co-funding to be considered Cantons: high Adaptation of cryptographic protocol: CHF 850,000 to CHF 1 million <u>Estimation of possible implementation following consolidation</u> Confederation: Co-funding to be considered

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
		proviso is that no significant reasons against implementation arise unexpectedly at a later date. In a first step, the FCh and cantons will draw up more detailed proposals; the cantons will have the cryptographic protocol adapted and work with Swiss Post to define their processes. An initial assessment of the time required showed that implementation (including adaptation of the cryptographic protocol) would take a good three years. There will be more detailed planning of the implementation in an initial phase. Once completed, the FCh and the cantons will submit a proposal to the SC VE on further action to be taken.			Cantons: high - One-off: CHF 700,000-900,000 - Recurring: CHF 100,000 / year
A.6	Enhance the foundations for additional verification mechanism whose effectiveness is not based on current trust assumptions	The possibilities of an additional verification mechanism will be explored and analysed. It should be examined whether and how an additional instrument to those provided by the manufacturer to assure verifiability can be offered to voters. A public bulletin board could be one such mechanism. With a public bulletin board, voting data could be made public while preserving the secrecy of the vote, and voters could use a second device (e.g. a mobile phone) to determine whether their vote had been correctly received by one or more entities independent of the manufacturer. This would mean that individual verifiability would not depend on the trustworthiness of the printing company or on the control components. As part of their universal verifiability testing, the cantons could establish whether all the votes received by the independent entities were considered in the count. Initially, a study will be developed to examine the benefits of an additional mechanism and of the way that this might be implemented. The study will address technical implementation issues as well as trust-building and acceptance, the latter in consultation with voters. Once the study has been concluded, the FCh and the cantons submit a proposal to the SC VE as to whether and how a public bulletin board could be implemented. Funds must be earmarked for possible future implementation.	Study: One year after relaunch Request to SC VE: up to two years after relaunch	Study: FCh with cantons' involvement	Study Confederation: medium Cantons: none Estimation of possible implementation following consolidation High. Responsibility for funding is yet to be decided. - One-off: CHF 600,000 - Recurring: CHF 200,000 / year
A.7	Improve bases for detection (monitoring) and investigation of incidents (IT forensics)	E-voting systems must allow for effective detection and investigation of incidents - such as suspected vote tampering or system attacks. Before trials are resumed, the existing requirements for gathering evidence must be tightened: Consistent protocols on all system ele-	Definition of requirements and improvement process: Relaunch	Requirements: FCh Improvement process: System providers, cantons	Confederation: none Cantons: none; the costs of implementing measures in the ongoing improvement process are unknown

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
		ments must be drawn up to aid the detection and investigation of incidents. These protocols must be drawn up, transferred and stored in such a way that they cannot be manipulated. The contents and scope of the protocols must be defined in such a way that incident investigations can be carried out effectively. Voting secrecy must be ensured at all times. In a second step, a continuous process for improving methods to detect and investigate incidents will be defined and implemented when trials are resumed. The following aspects in particular should be taken into account: – Open dialog between the Confederation, cantons and system provider. – Regular analyses will be conducted of the suitability of the bases for monitoring and investigation. The scenarios defined in the crisis agreement will be taken into account in these analyses. – Findings from the analyses will influence improvements in the instruments and processes.			
A.8	Create a joint plan for implementing measures for the Confederation and cantons	The Confederation and the cantons have a joint plan for implementing measures going forward. The set of measures reflects the decisions regarding redesign of the e-voting trials and shows which measures are already being implemented in the relaunch and which measures will constitute the further development of e-voting in the medium to longer term. Wherever possible, a time schedule for implementing the measures or for the initial stages should be given. The SC VE will approve and publish the set of measures as a declaration of intent. It will be reviewed regularly to take into account the latest developments in security.	Relaunch	FCh, cantons	Confederation: none Cantons: none
B.	**Effective control and oversight**				
B.1	Adapt responsibilities in the examination of the system and the underlying processes	The responsibilities in the system conformity examination are reviewed in order to ensure the efficacy and credibility of the examination. Independence between the auditing body and the audited entity plays an important role here. The division of tasks between the Confederation and the cantons will be adapted so that the Confederation assumes more responsibility and a more direct role in examining the systems:	Relaunch	FCh	Confederation: high Cantons: none (no cost savings)

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
		– The Confederation is now responsible for examining compliance with the requirements relating to the system and the underlying processes (in accordance with points 5.1, 5.2, 5.3 in sections 5.4, 5.5 and 5.6 of the annex to the VEleS) – The system provider is now only responsible for audits relating to system operation in its data centres (ISO 27001 certification in accordance with Section 5.3 of the annex to the VEleS) Independent experts will be commissioned to conduct the examinations.			
B.2	Develop an examination concept to assess conformity of the system and the underlying processes	An examination concept will be established based on the new responsibilities for examining the system and processes as in Measure B.1. The examination concept will ensure that the security requirements are thoroughly tested. The FCh is responsible for drawing up the concept and can involve external experts in the process. The concept will include the following aspects: – Clear definition of extent of examination in different areas in respect of their scope and duration – Permeability between the different examination areas to ensure consistent and complete examination – Commissioning of qualified and independent experts – Publication of examination reports	Relaunch	FCh with cantons and system providers	Confederation: low Cantons: none
B.3	Develop and apply a process to deal with non-conformities	The FCh will work with the cantons to develop a process for dealing with proven and suspected non-conformities. The aim is to avoid ambiguities as far as possible in dealing with non-conformities and to ensure that the use of e-voting conforms to the provisions of the VEleS. The following aspects are defined in this process: - Type of non-conformities - Criteria used in dealing with non-conformities - Actors and roles	Relaunch	FCh with cantons and system providers	Confederation: low Cantons: none
B.4	Revise and improve risk assessment guidelines	In collaboration with the cantons, system providers and IT security experts, the FCh updates the guidelines serving as the basis for risk assessments as in Measure B.5. The guidelines contain the following main aspects: - Catalogue of information assets	Relaunch	FCh with cantons and system providers	Confederation: low Cantons: none

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
		- Catalogue of threats (based on the list of threats in annex to the VEleS - Catalogue of risk minimisation measures - Responsibilities with regard to protection of information assets The guidelines will cover, among other things, the length of encryption keys, multiple votes cast through different voting channels, vote buying, 'long term-privacy' and reliance on a single provider. The guidelines will be published in order to increase transparency and build trust. Moreover, the public will have the opportunity to give feedback. The guidelines will be reviewed periodically and adapted if necessary.			
B.5	Draw up and implement a new process for the risk assessment of completely verifiable systems	Each actor (FCh, cantons, system provider) will now conduct a risk assessment for their area of responsibility. The risk assessments should follow the guidelines set out in Measure B.4. They will be reviewed and, if necessary, adapted at least annually, in the event of significant changes to the system and specifically before each ballot. If risk-minimising measures cannot be implemented immediately, they should be recorded in the set of measures (Measure A.8). Independent experts are employed to assess the risks.	Relaunch	FCh, cantons, system providers	Confederation: low Cantons: low
B.6	Renew crisis management and conduct crisis simulation exercises	A new crisis agreement will be drawn up to take account of developments in e-voting and to improve the effectiveness of crisis management. This will take the form of a framework agreement and have the following features: - Trilateral agreement concluded between the FCh, the user canton and the system provider - Sets out crisis management processes and processes of the actors involved - Sets out the communication processes between the actors involved and those to coordinate communication to the outside - Stipulates exercises to improve crisis management - The crisis scenarios will be adapted to the new risk assessments for completely verifiable systems. Existing structures at federal, cantonal and system provider level will be retained as far as possible in crisis management design.	Relaunch	FCh (lead), cantons and system providers	Confederation: low Cantons: none

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
B.7	Integrate e-voting into the Confederation's critical infrastructure	Critical infrastructure within the meaning of the National Critical Infrastructure Protection Strategy receives greater support from MELANI and GovCERT. This support might be valuable in analysing threats and investigating incidents. The purpose of this measure is to define cooperation on e-voting between the FCh, cantons, system provider and GovCERT / MELANI in order to ensure a prioritised approach to dealing with incidents. Crisis management will also take account of this cooperation.	Relaunch	FCh (lead), cantons and system providers	Confederation: none Cantons: none
B.8	Further develop the plausibility checks for e-voting results	The cantons conduct the plausibility checks of results from the e-voting system in different ways. There should be more intensive discussion among the cantons and with the FCh so that experiences and approaches to problem-solving can be shared and best practices developed. The possibility of devising a standardised statistical method and what form this would take is being considered. The introduction of a standardised procedure would provide a further instrument for obtaining indications of mistakes or manipulations. The method must be applicable to the specific circumstances of each canton. What information can be published in future regarding the plausibility checks should also be looked at.	Relaunch: Initial discussions Study standardised method: by 2022	Cantons	Confederation: none Cantons: low
B.9	Amend authorisation process	The implementation of a range of measures for relaunching e-voting trials makes it necessary to adapt the procedures in the authorisation process. These include, in particular, the measures to redefine responsibilities for independent examinations (Measure B.1) and the adaptation of transparency requirements (Measures C.2 and C.3). In addition, the involvement of independent experts in the approval process and ongoing risk management must be taken into account. The FCh's catalogue of requirements for the authorisation procedure will be revised. The FCh will also analyse to what extent the Federal Council's basic decision on authorisation can be split into a system-related part and a canton-specific part.	Relaunch	FCh with cantons' involvement	Confederation: none Cantons: none
B.10	Revision of processes, roles and tasks long term	The responsibilities, roles and tasks of the Confederation, cantons and system providers have a direct influence on the (security-related) design of e-voting systems. They are to be reviewed and set out in a long-term strategy. The Confederation and cantons can draw up measures that take into account the changed situation regarding the number of system providers, governance and funding requirements for e-voting.	Long term	Working group on the future of Vote électronique (AG Zukunft VE)	Confederation: none Cantons: none

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
C.	**Increasing transparency and trust**				
C.1	Restrict electorate permitted for completely verifiable systems	The number of voters permitted to use e-voting in the trials of completely verifiable systems is limited. The limits are set at 30% of the cantonal electorate and 10% of the national electorate. Swiss voters abroad do not form part of the calculated limits. The limits may be increased or removed entirely once the completely verifiable systems have been shown to be reliable in stable trial operation.	Relaunch	FCh	Confederation: none Cantons: individual, depending on voter systems in place (e.g. the introduction of a registration procedure may involve mid-range costs)
C.2	Draw up more detailed requirements for disclosing the source code	More detailed requirements for source code disclosure will be specified. Documentation requirements: - Source code, software documentation and files with relevant input parameters must be published. - Publication of aids and supplementary documentation so that competent persons can efficiently compile, execute and analyse the system in their own infrastructure; - Publication where possible of documentation on infrastructure, third-party software and operating processes. - The presentation of the disclosed documents is in line with standard practice. Terms of use requirements: - Access to the source code will be provided free of charge and anonymously. - The source code may be used for ideational and in particular scientific purposes. This includes exchanging information about any errors detected and the right to publish. This right is explicitly granted by the owner. - Persons complying with the terms of use will not be legally prosecuted. Persons violating the terms of use will only be prosecuted if the source code or parts of it are used commercially or productively. The terms of use refer to this limitation of liability. - It is sufficient to refer to the terms of use in the licence conditions; if possible, no declarations of intent by the users should be required. The SC VE would like to see future systems and system components published under an open source licence (OSL). Furthermore, the cur-	Relaunch	Requirements: FCh Disclosure: Cantons, system providers	Confederation: none Cantons: none

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
		rent system provider Swiss Post is looking at which source code components of its completely verifiable system that are already developed can be placed under an OSL.			
C.3	Run a bug bounty programme	A bug bounty programme will be run for the disclosed source code and e-voting system documentation. This should meet the following requirements, among others: - The bug bounty programme is ongoing. - There will be a financial reward for any errors detected according to their severity. The amount of the reward will be based on the 2019 PIT. - There are three elements to the bug-bounty programme: • Search for errors in the disclosed documentation or source code (static test) • Search for errors by analysing the executable system in private infrastructure (dynamic test) • Attacks on the provider's infrastructure (internet test). The bug bounty programme must permit attacks on the provider's infrastructure; DoS and social engineering attacks can be excluded. Attacks on infrastructure may be prohibited in justified cases (e.g. during a ballot) - Responsibilities and handling of notifications: • The system provider is responsible for the bug bounty programme. It runs the programme and receives and categorises notifications. It justifies its decisions to the participants concerned and publishes all confirmed findings. • The FCh establishes the basic conditions. • The Confederation and the cantons receive unrestricted access to the notifications and to the system provider's responses. A summary of the notifications and the measures taken as a result thereof must be submitted in the authorisation procedure. - Terms of use: Participation is anonymous and vulnerabilities may be disclosed: responsible disclosure. Participants must only be required to disclose their identity for a reward to be paid out in the bug bounty programme. The FC defines the requirements in consultation with the cantons and examines any financial contribution to be made. An escalation option	Relaunch	Requirements: FCh Run by: Cantons, system providers	Confederation: Co-funding to be considered Cantons: high Implementation with recurring internet test (not incl. reward): – One-off: CHF 230,000-290,000 – Recurring: CHF 55,000-70,000 / year Implementation with recurring internet test (not incl. reward): – One-off: CHF 255,000-360,000 – Recurring: CHF 550,000-650,000 / year

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
		for participants who disagree with the system provider's decision should also be considered. The internet test is to be conducted on the productive system before the resumption of trials. Then a decision can be made on further steps to be taken based on the findings. There are two options: either the internet will be regularly repeated on the productive system or will be run permanently on a parallel system.			
C.4	Publish examination reports relevant to authorisation	The Confederation, cantons and system providers ensure there is sufficient transparency regarding examination results that are relevant to authorisation. Reports, supporting documents and certificates produced as part of the examinations in accordance with point 5 of the Annex to the VEleS must be published; the published reports must be clear and comprehensible. Any other documents referred to must be published. Publication may not be required in justified cases (e.g. if publication increases a risk, for reasons of data protection, internal security guidelines, etc.). Any response by the examined organisation to the published examination report should also be published.	Relaunch	FCh, cantons, system providers	Confederation: possibly low Cantons: none
C.5	Publish e-voting results in federal ballots	Creates transparency for the public with regard to e-voting results. The cantons will therefore publish the e-voting results of federal elections and votes. In this way the public can compare the results of e-voting with the overall result and conduct plausibility checks. Exceptions may be made in order to ensure voting secrecy.	Relaunch	Requirements: FCh Publication: Cantons	Confederation: none Cantons: low
C.6	Increase public involvement	The Confederation and the cantons will draw up a concept in consultation with the system provider to ensure greater public involvement with a focus on the general public as well as on politicians, experts and interest groups. This will involve proposals for active communication. The possibility of implementing a range of activities is to be considered before relaunch.	Concept: Relaunch	FCh with involvement of the cantons and system providers	Concept Confederation: low Cantons: none Implementation depending on activity; 2021 low costs for Confederation

No	Measure	Description	Timeframe implementation	Responsibilities	Cost estimate[24] *Low (< CHF 50,000)* *Medium (CHF 50,000.- 500,000)* *High (CHF 500,000 - 1 million)* *Very high (> CHF 1 million)*
D.	**Stronger connection with the science community**				
D.1	Draw up a concept for the scientific monitoring of the trials and for the dialog with external experts	The e-voting trials are to be scientifically evaluated and monitored on an ongoing basis. In addition, the Confederation and the cantons will maintain an ongoing dialog with the academic community and the competent specialist entities. They will submit questions, respond to comments, actively participate in discussions and provide the necessary infrastructure and resources for discussion. The Confederation and cantons will also commission academic studies in areas where greater depth of understanding is required. The Confederation and the cantons, in collaboration with representatives of the academic community, will draw up a concept for the monitoring process and the dialog with external experts for the period 2022-2025, including the funding involved.	Concept: 2021	FCh with involvement of the cantons	Confederation: low Cantons: low
D.2	Involve independent experts	In their work, the Confederation and the cantons will involve independent experts and specialist entities from relevant academic disciplines as well as other organisations where this makes sense and offers added value, in particular with regard to the measures defined in the redesign of trials.	In each individual measure	FCh with involvement of the cantons	Estimate according to each individual measure
D.3	Develop a concept to set up an academic committee	An academic committee will be set up to advise the Confederation and cantons. The Committee will advise on cooperation with the academic community (see Measures D.1 and D.2) and will also be able to perform individual tasks itself. The Confederation and cantons draw up a concept for the years 2022-2025.	Concept: 2022	FCh with involvement of the cantons	Concept development Confederation: none Cantons: none