Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh
Political Rights Section

Vote électronique

Catalogue of measures by the Confederation and cantons

Approved by the Vote électronique Steering Committee (SC VE): 4 August 2023

Contents

1. Background

As part of the redesign of online voting trials, the Confederation and the cantons have adopted a final report containing a comprehensive catalogue of measures.[1] With the redesign of the trials, the cantons will be able to resume trials and establish stable trial operations with the latest generation of online voting systems. The first stage of the redesign comprised numerous measures, many of which were implemented when the related legislation was revised in July 2022. This involved the partial revision of the Political Rights Ordinance (PoRO; SR 161.11) and the total revision of the Ordinance of the Federal Chancellery (FCh) on Electronic Voting (OEV; SR 161.116).[2]

With the revision of the federal legislation, the security of e-voting systems was strengthened by introducing more precise and stricter security and quality requirements for the systems, their operation and development. Only the use of completely verifiable e-voting systems that have been examined by independent experts on behalf of the Confederation will be authorised. E-voting may be used by a maximum of 30% of the cantonal electorate and 10% of the national electorate. The key aim of the redesigned trials is to continuously improve e-voting systems and their operational modalities. Security is to be continuously enhanced and strengthened. Findings from the practical use of e-voting are to be continuously incorporated. This principle is also taken into account in the licensing procedure. As stated in Article 16 paragraph 2 OEV, the FCh may in exceptional cases exempt a canton from meeting individual requirements when authorising an e-voting system. The canton must justify the exceptions, describe any alternative measures and announce how it intends to rectify the non-conformity. If action is required, the e-voting system can only be used if the risks involved in using it are nevertheless sufficiently low.

The source code and documentation of Swiss Post's new e-voting system with complete verifiability have been disclosed since 2021. Since then, the system and its operation have been examined in various stages by independent experts and – as part of a bug-bounty programme and a public intrusion test – by the public, and have been fundamentally improved by Swiss Post. This system is used in the cantons of Basel-Stadt, St Gallen and Thurgau in resumed trials based on the PoRO.

The examination commissioned by the Confederation in particular identified a further need for action with regard to some aspects that are designated as non-conformities, as well as aspects where further improvements are needed to ensure greater compliance with the requirements. In order to address the known need for action and to address and highlight necessary further improvements of e-voting, the Confederation and the cantons have drawn up this joint catalogue of measures (see Measure A.8 in Section 2.2). The catalogue of measures is regularly reviewed, adapted and published. The implementation of measures is scheduled as far as possible. The costs incurred in implementing the measures are analysed and mapped in the joint financial planning of the Confederation and cantons. The measures are implemented with the financial support of Digital Public Services Switzerland.

[1] See Vote électronique Steering Committee final report (SC VE) of 30 November 2020 on the redesign and relaunch of trials; available at www.bk.admin.ch > Political rights > E-voting > Reports and studies.

[2] Federal Council press release of 25 May 2022; available at www.bk.admin.ch > Political rights > E-voting > Media releases.

2. Catalogue of measures

2.1 Pending measures

The following table includes the status of pending measures according to the SC VE's decision of 4 August 2023. Information that has been adjusted is shown in italics.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
A.	**Further development of the systems**				
A.4	Deploy manufacturer-independent components (verifier / control components)	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Study and request for online control components to SC VE: 2024 Conditional implementation: 2028	Online control components study: Cantons with FCh involvement	Planned
A.5	Weaken trust assumptions in the printing process and in the software that generates cryptographic parameters	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Extension / adaptation of the cryptographic protocol; set schedule for implementation: 2023 / 2024 Request to SC VE: 2025 Conditional implementation: 2025 / 2026	Issues to be clarified for requirements: FCh Implementation: Cantons, system provider	Planned
A.6	Enhance the foundations for additional verification mechanism whose effectiveness is not based on current trust assumptions	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Study: 2025 Request to SC VE: 2025	Study: FCh with cantons' involvement	Planned
A.10	Reduce dependencies on external software in the Swiss Post system	Integrating external software into the online voting system may make sense, especially for security reasons. This is especially the case when the software is widely used throughout the world and is continuously scrutinised and improved. The more the software is examined, the lower the probability that attackers could succeed in infiltrating harmful code into the system unnoticed. Swiss Post has already implemented a process to minimise the risks associated with the use of external software. This measure will further reduce Swiss Post's dependence on external software, namely on external software libraries on the Java Script client. External libraries will only be used with good reason.	Ongoing; Java-Script client: 2nd quarter 2023 (to be used from National Council election 2023)	Cantons, system provider	*In progress* *Java-Script client: Completed*

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
A.11	Disclose source code of software for generating PDF files for printing voting cards	Art. 11 OEV requires software to be disclosed. This helps to reveal any errors or weaknesses. In fulfilment of Art. 11 OEV, the cantons have already disclosed the software that generates the raw data for printing the voting cards. The raw data contains the codes for voting and verification by the voters providing individual verifiability in accordance with Number 2.5 of the OEV annex. The cantons of BS and TG use Swiss Post's Voting Card Printing Service (VCPS) software to convert the raw data into print-ready PDFs. This software is not disclosed. The software for generating the PDF files for printing the voting cards is to be disclosed at some point in the future. Given the scope of functionality, the operational precautions and examinations of the source code, it has been concluded that the risk involved in not requiring disclosure at this time is sufficiently low. See Annex for additional information on this measure.	2024	Cantons, system provider	*Planned*
A.12	Further develop symbolic proof of cryptographic protocol compliance	Computer-aided proof of compliance is provided based on symbolic models. Number 2.14.1 of the OEV annex requires such proof of compliance to demonstrate that a cryptographic protocol meets the requirements for verifiability, voting secrecy and authentication. Swiss Post has created a symbolic model and uses the ProVerif programme to provide proof. So that ProVerif can produce a result within a useful period of time, system properties are usually presented in a simplified form, which by nature conflicts with the substance of a proof. On the basis of examinations carried out on the Swiss Post system, it was concluded that the models available are of good quality and that the proof delivers valuable evidence of compliance of the cryptographic protocol. As a next step, the substance of the proof is to be further increased as far as is reasonable in the ongoing improvement process during trials. The models will be enhanced with the goal of capturing the system properties as realistically as possible: - Authentication is modelled as far as is reasonable based on the specification and considered in the symbolic proofs (see also Measure A.9). - Further additions are examined and subsequently either implemented or reason given for non-implementation (see recommendations 4.1 and 4.2.1 in the University of Surrey examination report dated 17.10.2022[3]).	Authentication: 2nd quarter 2023 (to be used from National Council election 2023) Remaining points: 2025	Cantons, system provider	*Authentication: Completed* *Remaining points: Planned*

[3] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		Furthermore, additional evidence is provided, where appropriate, that the models are suitable for detecting non-conformities (see recommendation 4.2.3 in the University of Surrey examination report dated 17.10.2022).			
A.13	Do not apply SGSP[4] problem as a hardness assumption	Number 2.14.1 of the OEV annex requires cryptographic proofs of compliance to demonstrate that a cryptographic protocol meets the requirements for verifiability, voting secrecy and authentication. In proofs of compliance cryptographic protocols are brought into relation with elementary cryptographic problems. If the proof is correctly established, i.e. if the relations are established correctly, and if the security assumptions hold, namely that the elementary cryptographic problems are 'hard to solve' and are thus de facto unsolvable, a protocol may be considered secure in the sense of the OEV. Number 2.14.3 of the OEV annex specifies that proof of compliance may be provided under generally accepted security assumptions. Swiss Post's cryptographic protocol uses a construction that is related to the so-called SGSP problem in the cryptographic security proof. This is an elementary cryptographic problem that has strong similarities with the DDH[5] problem, which is generally accepted as a hardness assumption. Despite its relationship to the DDH problem, little research has been done into the SGSP problem. Swiss Post is adapting its cryptographic protocol so that its compliance does not depend on the de facto insolvability of the SGSP problem. See Annex for additional information on this measure.	2025 / 2026 (together with Measure A.5)	Cantons, system provider	*Planned*
A.14	Remove the scope of eligibility to vote as a mandatory criterion for the formation of counting districts	The technical design of the Swiss Post system does not allow votes cast by voters with different eligibility to be mixed and tallied together. For example, the results of votes cast by Swiss voters abroad on federal proposals must be counted separately if these voters are not entitled to vote on cantonal or communal proposals on the same ballot. The more votes mixed and tallied in one batch, the greater the protection of voting secrecy. Federal requirements do not prescribe to the cantons a minimum size for the counting districts, and this also applies to e-voting. The solution chosen by Swiss Post thus meets the requirements of federal law. However, in the case of cantons in which the votes of the Swiss voters	2025 / 2026 (together with Measure A.5)	Cantons, system provider	*Planned*

[4] Subgroup Generated by Small Primes.

[5] Decisional Diffie-Hellman.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		abroad are processed decentrally, more flexibility in the formation of counting districts is desirable. In particular, the technical design should not pose any barrier. For proposals at federal level, the cantons are to be given the option of mixing and counting the votes of Swiss voters abroad together with the votes of other voters in the same commune. Swiss Post is adapting its system accordingly.			
A.15	Increasingly base application of crypto-primitives on design principles of object-oriented programming	Consistent application of design principles for implementation facilitates maintainability and counteracts mistakes. The crypto-primitives in the Swiss Post system are a collection of algorithms that perform basic cryptographic operations. Implementation is based on the principles of object-oriented programming. It is published under an open source licence. On the basis of the examinations carried out on the Swiss Post system, it was concluded that even more benefit could be obtained from the design principles of object-oriented programming in some areas. Improvements could be made in the naming of classes and interfaces, the consistent application of semantic criteria in the formation of hierarchies (class inheritance, interface implementation) and the definition of suitable methods at a high abstraction level and their efficient use. Adjustments are to be made in the following areas (see also Section 3.2.1 in the Bern University of Applied Sciences BFH examination report of 23.02.2023[6]): - Implementation of algebraic groups - Implementation of tuples, vectors and matrices - Interface 'hashable' as a basis for calculating cryptographic hashes The recommendations do not have to be strictly observed provided the objectives underlying the comments in the examination report are achieved by other means.	2025	Cantons, system provider	*Planned*
A.16	Swiss Post to examine ways to reduce the complexity of the system and simplifies it appropriately	Essentially, the simpler the design, the earlier errors can be detected and corrected. At the same time, by their very nature secure e-voting systems have a certain degree of complexity. The systems should be as complex as necessary and as simple as possible. In general, the Swiss Post system does not have an unnecessarily complicated design. Nevertheless, Swiss Post will examine ways of simplifying the system further, provided that this is possible without	Simplified authentication: 2nd quarter 2023 (to be used from National Council election 2023)	Cantons, system provider	*Authentication with reduced complexity: Completed* *The proposed solution for authentication will be discussed and possibly amended in conjunction with Meas-*

[6] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		compromising the security features implemented and that the simplifications are reasonable. See also Section 1.4 'Potential for Simplifications' in the BFH examination report dated 23.02.2023.[7] Simplifications are introduced in the following areas in particular: - Voter authentication is now achieved by means of a series of rounds of exchanged messages. Although the certificates used do not meet the federal requirements, their use does not affect system compliance. Messages and certificates for which no substantial added value is documented will not be used. These simplifications will be made together with the completion of the authentication specification (see also Measure A.9). - In addition to the vote cast, elements necessary to generate the verification codes are sent to the online system as part of the voting data. These elements are sent in encrypted form, although this is not actually necessary (see also Section 5.1.4 of the Swiss Post Voting System – System Specification Version 1.2.0[8]). Unnecessary encryption should be avoided.	Unnecessary encryption in the voting data should be eliminated and further simplifications introduced as needed: 2025 / 2026 (together with Measure A.5)		*ure A.25. Assessing the trade-off between the security benefits introduced due to the proposed solution and the risks that inherently come along with it is of particular interest. On the one hand, the solution provides an additional safeguard addressing the case where datasets are maliciously sent to the servers. On the other hand, voters that use a device with an operating system set to the wrong time might not be able to cast a vote before adjusting the time. At the price of waiving the mentioned security benefit, the complexity could be additionally reduced, which in return would be beneficial for security as well (see explanations in description of this measure).* *Elimination of unnecessary encryption in the voting data and introduction of further simplifications as needed: Planned*
A.17	The Confederation, cantons and the system provider Swiss Post harmonise their terminology	The Confederation, cantons and Swiss Post sometimes use different terms for the same thing (concepts, objects, etc.). At the same time, there are clear similarities in the content of their documentation. The use of different terms can make it difficult to understand the various documents. The Confederation, cantons and Swiss Post will create a grid showing the terms used by the respective actors. They will consider the possibility of making the grid available to the public as an aid to understanding the published documents. Based on the grid, the Confederation, cantons and Swiss Post will decide on possible standardisations and draw up proposals for such. The aim is to use terminology as consistently as possible in any documents	Grid and plan: 2024	FCh with involvement of cantons, system provider	*Planned*

[7] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

[8] Available at https://gitlab.com/swisspost-evoting > E-voting > E-voting documentation > System.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		created or modified, in preparation for Release 2.0 of the Swiss Post system.			
A.18	The cantons document links between their operating instructions, the cryptographic protocol and OEV requirements	The cryptographic protocol defines the operations to be carried out for all system participants on the basis of the trust model in Number 2 of the OEV annex. Some operations need to be performed by humans, for example setting passwords (see Section 4.2.2 Swiss Post Voting System – System Specification Version 1.2.0[9]). Furthermore, Number 3 of the OEV annex specifies additional requirements for the operation of components whose correct functioning is crucial to meet security objectives ('trustworthy components'). For example, the OEV requires there to be sufficient entropy when selecting random values (No 3.2 OEV annex). With this measure, the cantons place an emphasis on documenting the links between their operating instructions and the cryptographic protocol as well as the requirements of the OEV. This helps to ensure that the main steps are performed correctly in the long term, namely when changes are made to the cryptographic protocol or the OEV.	2025	Cantons with support of system provider and FCh	*Planned*
A.19	The Confederation and the cantons examine the use of verification features by the voters and, if necessary, define measures to encourage their use	The OEV requires there to be a variety of ways in which voters can check whether an attack has taken place and to react. They can check: - that the vote was correctly registered (No 2.5 OEV annex); - whether a vote has been maliciously cast on behalf of the person entitled to vote (No 2.5 OEV annex); - whether the correct software with the correct encryption parameters is run on the user platform (No 2.7.3 OEV annex); - the authenticity of the website used for voting (No 8.10 OEV annex). In addition, Number 8 of the OEV annex contains minimum requirements for providing information and instructions for voters. The verification features are only effective if voters make use of them. If voters report the negative results of their checks, the agencies involved have an indication of possible systematic attacks. They, too, have an interest in ensuring that voters make sufficient use of the checking options. The use by voters of the checking options can be assessed during the trials and any necessary improvements made to design and communication.	Investigation and definition of any measures necessary: 2025	FCh with involvement of cantons, system provider	*Planned*

[9] Available at https://gitlab.com/swisspost-evoting > E-voting > E-voting documentation > System.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		The Confederation and the cantons investigate the use of verification features by the voters and, if necessary, define measures to encourage their use.			
A.20	In a public examination, ballots can be set up based on the eCH files	On the basis of the disclosed source code, people can set up the Swiss Post system in their own infrastructure and simulate ballots with predefined test files. Under the Swiss Post's bug bounty programme, there is a reward for reporting deficiencies which are of relevance. Swiss Post is looking into suitable measures to ensure that interested parties have more flexibility in simulating ballots, e.g. making it easier to conduct ballots based on the eCH files containing the parameters defining a ballot (voting proposals, lists and candidates, eligible voters).	First improvements: 2nd quarter 2023 (to be used from National Council election 2023) Further improvements: 2024	Cantons, system provider	*Initial measure: Completed except for user instructions; Swiss Post and the cantons are considering further improvements*
A.21	Implement the specified 'dispute resolver'	Swiss Post has specified the so-called 'dispute resolver' to eliminate possible inconsistencies in the control components with regard to the issue of which votes are to be counted (see also explanations on Measure A.24 in the Annex). This must now be implemented so that the cantons and Swiss Post can use it immediately if necessary. The probability of inconsistencies may be considered as low. With no dispute resolver implemented, any inconsistency would mean that the necessary functionality would have to be implemented at short notice, taking into account the necessary transparency and traceability. As a result, it might take days to resolve the inconsistency. The risk associated with not implementing the dispute resolver for the time being may be considered sufficiently low.	2024	Cantons, system provider	*Planned*
A.22	Adjust auditors' tasks so that they do not perform operational tasks	During configuration of a ballot, the cryptographic parameters for the ballot are set by the canton. This is an operational task and is therefore not part of the auditors' actual area of responsibility. The operations required for this are time-consuming. With the aim of optimising the processes, the cantons and Swiss Post have assigned one of the particularly time-consuming tasks to the auditors as defined in Article 2 paragraph 1 letter h OEV. For this work, the auditors use the laptop assigned to them. This way, this task can be carried out in parallel with other tasks. Since the laptop used by the auditors is kept by the competent cantonal office and is operated under the same conditions as the laptop that would normally be intended for this step, the solution is considered equivalent from a security point of view. This measure is intended to ensure that auditors do not perform any operational tasks. In particular, when developing Measure A.5, it	2025 / 2026 (together with Measure A.5)	Cantons, system provider	*Planned*

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		should be ensured that the performance of operational tasks is not, or not solely, dependent on the correct functioning of the auditors' laptop. See Annex for additional information on this measure.			
A.23	Enhance development process, in particular Secure Development Lifecycle	The SCRT examination report of 02.11.2022 on Swiss Post's development process[10] contains suggestions for improvements in security precautions in software development. Swiss Post has already started to implement these suggestions as part of an ongoing improvement process. This measure specifies that the recommendations from the examination reports are to be addressed and that the current status of the security precautions be submitted to the FCh for periodic examination. The results will be made available for an initial review in 2024.	Ongoing; Implementation and availability for initial review: 2024	Cantons, system provider	*In progress*
A.24	Further improve the conclusiveness of cryptographic proof of conformity and increase its substance	Number 2.14.1 of the OEV annex requires cryptographic proofs of compliance to demonstrate that a cryptographic protocol meets the requirements for verifiability, voting secrecy and authentication. In proofs of compliance, cryptographic protocols are brought into relation with elementary cryptographic problems. If the proof is correctly established, i.e. if the relations are correctly established, and if the security assumptions hold, namely that the elementary cryptographic problems are 'hard to solve' and are thus de facto unsolvable, a protocol may be considered secure in the sense of the OEV. The examination report by Haines, Pereira and Teague of 13.02.2023[11] indicates that the conclusiveness of the proof and thus the reasoning as to why the cryptographic protocol was correctly associated with the elementary problems needs further improvement. In order to improve the conclusiveness of the proof, some of the arguments put forward need to go further. In some cases, erroneous or misleading arguments that are already provided in sufficient depth must be corrected. In general, the substance of the proof need not be considered to be fundamentally too low. However, it would be greater if further system elements that are currently excluded from the security proof were considered. Going forward, these system elements should be included in the proof as far as is reasonable. See Annex for additional information on this measure.	2024	Cantons, system provider	*Planned*

[10] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

[11] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
A.25	Further improve the quality of the specification and the software	Adherence to quality criteria in the specification and the software plays an important role in preventing errors or shortcomings, or at least in identifying and eliminating them at an early stage. The OEV sets various requirements with regard to quality, such as traceability, completeness, consistency, commonality and self-descriptiveness (see No 25 OEV annex). Swiss Post has succeeded in substantially improving the quality of its system's specification and source code. Nevertheless, improvements are still to be made. Examples of points subject to improvement are found in the examination reports;[12] some are mentioned here in the Annex. Improvements are made on an ongoing basis (continuous improvement process). The purpose of this measure is to help ensure that the currently known need for improvement in quality is addressed and remedied as far as possible by 2025. As part of this work, Swiss Post is to provide the FCh and the cantons with a material description of the planned improvements so that they can be discussed and, if necessary, adjusted before implementation, and any ambiguities and differences can be clarified, if necessary with the involvement of external experts. This reviewed description is also to be included in the FCh's independent examination in accordance with Article 10 paragraph 1 OEV. The risks associated with the quality improvements required may be considered sufficiently low. See Annex for additional information on this measure.	Improvements: ongoing Description of planned improvements still pending: ongoing, by 1st quarter 2024 at the latest Address currently known improvements required: 2025	Cantons, system provider	*In progress (see added information in the measure's description in the Annex)*
A.26	*Strengthen the means to detect votes not cast in conformity with the system as per Art. 2 para. 1 let. o No 1 OEV*	*Art. 2 para. 1 let. o OEV defines under which conditions a vote may be considered to be «cast in conformity with the system». One of the conditions states that a vote must comply with a predetermined way of completing a ballot paper in a vote or election. In order to refer to a vote that satisfies this condition, in the context of this measure, the term «valid vote» is used.* *The user interface of the Swiss Post system only allows to furnish and cast valid votes. However, it is not possible to prevent cases where skilled people furnish a non-valid vote, e.g. using third party software, and attempt to cast it using their voting card. As the voting servers detect non-valid votes right after transmission, such attempts fail. However, there is one exception: Votes at elections to the National Council*	*Checks in compliance with No 10 OEV annex: 2025* *Verification in compliance with Art. 5 para. 3 let. a OEV as well as No 2.6 OEV annex: 2024*	*Cantons, system provider*	*New*

[12] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		that represent a vote for a party list but represent no vote for any candidate are non-valid and should accordingly be detected upon transmission. This is not done and voters can finalize the process of casting such a vote by entering their confirmation code. Although such votes are identified and documented at tallying, this system behavior stands in conflict with No 10 OVE annex which requires that votes not cast in conformity with the system shall not be stored in the electronic ballot box in the first place. *In accordance with Art. 5 para. 3 let. a OVE and No 2.6 OVE annex, votes are to be verified with regard to their validity during the tallying phase. In particular, using their verifier[13] as a tool, auditors have to be able to verify that the result has been computed solely on the basis of valid votes. This functionality has not been fully implemented (see Haines, Pereira and Teague examination report of 31.07.2023; section 5.2.3, first paragraph). Yet, the verifier allows to detect cases of votes that correspond with the exception discussed above. In particular, auditors are able to ascertain that such votes have been processed and recorded correctly and that they have not been considered in any way at computing the result. Conversely, non-valid votes that are not detected due to the incomplete verifier functionality are detected upon transmission and thereby prevented from being cast.* *In conclusion, all cases of non-valid votes are detected either upon transmission or at tallying, thus being kept from being considered when computing the result. The risk that emerges from addressing the discussed issues only at a later stage may be considered to be sufficiently low.* *This measure shall ensure that during the phases of casting and tallying all checks and verifications are performed as per the requirements of the OEV.*			

B.	Effective control and oversight				
B.6	Renew crisis management and conduct crisis simulation exercises	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh, cantons, system provider	In progress

[13] *For more information on the terms «auditors» and «verifier», see first paragraph in the explanations on Measure A.22 in the Annex to this document.*

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
B.8	Further develop the plausibility checks for e-voting results	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch: Initial discussions Study standardised method: by 2023	Cantons	In progress; first discussions: *Completed*
B.10	Revision of processes, roles and tasks long term	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Long term	Working group on the future of Vote électronique (AG Zukunft VE)	In progress
B.11	Continuously improve the cantons' risk documentation	The risk assessments carried out by the cantons in 2022 reflect the situation after the implementation of the OEV requirements. They were drawn up in accordance with the FCh's guidelines on risk assessments. Risk documentation is to be continuously improved, with more documentation of the considerations leading to an assessment in order to increase traceability. Based on its discussions with the cantons and their existing documentation, the FCh concludes that the cantons have systematically and sufficiently assessed their risks. The purpose of this measure is solely to improve the documentation in order to increase the traceability of the cantons' risk management.	Ongoing; Implementation of first improvements: 2024	Cantons	*In progress*
B.12	Improve accessibility and traceability of Swiss Post's risk documentation	On accessibility: When applying to the FCh for authorisation, the cantons must submit their risk assessments and, if applicable, those of their service providers (such as the system operator) (Art. 15 para. 1 let. a OEV). They must demonstrate and justify that the security risks are sufficiently low (Art. 4 paras 1 and 2 OEV). Swiss Post conducts its risk assessment according to its internal directives, at several levels: Group, IT and e-voting. Because of the classification of the contents, the documentation can only be viewed on site at the Swiss Post premises. Accessibility is thus difficult for the FCh and does not allow for flexibility. Swiss Post and the cantons are looking at ways of creating a form of access for the FCh that meets the needs and constraints of all stakeholders. Access must ensure the traceability of the various risk assessments. On traceability: After consulting Swiss Post's threat and risk documentation, the FCh has concluded that appropriate processes have been implemented for risk owners to take responsibility for identifying, assessing and documenting risks. These processes ensure that risks are under control; however, the documentation submitted to the FCh could be improved. It will be adapted and supplemented to provide the FCh	Determine the form and timetable for improving accessibility and traceability: 3rd quarter 2023	Cantons, system provider	*In progress*

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
		with a consolidated overview of all risks and threats (developmental or operational, technical or organisational) in sufficient detail.			
B.13	Improve possibilities for independent investigation of incidents	The system provider, Swiss Post, controls the availability of information required by the cantons to investigate incidents (reports with selected statistics; investigation reports can be ordered). This could lead to problems when investigating errors irregularities that fall within the remit of Swiss Post. The cantons examine the extent to which it is necessary and possible to have more direct access to the information relevant to such investigations. During the trial phase, they develop competencies to investigate incidents and based on needs identified during ballots. In view of the trial phase conditions (in particular the limit on the electorate), Swiss Post's control of information is acceptable until such time as the improvement measures are implemented. The trial phase also allows for competencies to be developed.	Initial assessment of the situation: 2024, thereafter definition of measures	Cantons, system provider	*Planned*
B.14	Revise legislation to remove ambiguities	Federal legislation pertaining to e-voting, revised in 2022, was applied for the first time in view of the resumption of trials in 2023. Various questions have arisen for the first time in the application of the legislation. It has become apparent that clarity could be improved in some areas by adapting the wording of the OEV or by adding to or clarifying the explanations. For example, an inconsistency in the legislation meant that the partial non-fulfilment of a requirement had to be pointed out in an examination report, although the solution chosen by the cantons is preferable from a security point of view (see Section 8, item 15.4 in the SCRT examination report of 17.02.2023 on infrastructure and operation in the cantons[14]). The purpose of the trials is to provide a framework in which lessons can be learned and adjustments made in order to increase clarity, also in the legislation. Adjustments will be made as soon as the legislation is due to be revised again in the further course of trials.	Next revision of legislation	FCh	*Planned*
C.	**Increasing transparency and trust**				
C.6	Increase public involvement	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Concept: 2023	FCh with involvement of the cantons and system provider	In progress

[14] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
C.7	Provide additional documentation that contributes to the formation of opinion on trustworthiness and security	Both voters without a relevant background and experts alike typically have initial doubts and questions regarding the trustworthiness and security of electronic voting. Transparency is essential for stakeholders to form informed opinions and for a fruitful, fact-based public debate to take place. The Confederation, cantons and Swiss Post have disclosed documents in their respective areas of responsibility and have also drawn up information containing explanations on online voting for voters. Based on the experience already gained, the forthcoming trials are intended to provide more information as to which issues actually concern voters and indicate what communication by the authorities and their service providers should involve in order to meet voters' needs and expectations. Needs assessment: - In consultation with the cantons, the FCh conducts workshops with independent members of the public. - The FCh and the cantons, in cooperation with their service providers, evaluate feedback received in the course of the trials. The FCh and the cantons provide the public with further documentation on their respective areas of responsibility as required.	FCh workshops: 2023 Provision of documents: ongoing and as required	FCh and cantons	*In progress*

D.	**Closer cooperation with the academic community**				
D.1	Draw up a concept for the scientific monitoring of the trials and for the dialog with external experts	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Concept: 2023	FCh with involvement of the cantons	In progress
D.2	Involve independent experts	See description in catalogue of measures in SC VE final report dated 30.11.2020.	In each individual measure	FCh with involvement of the cantons	Ongoing
D.3	Develop a concept to set up an academic committee	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Concept: 2023	FCh with involvement of the cantons	In progress

2.2 Completed measures

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
A.	**Further development of the systems**				
A.1	Draw up precise criteria for source code quality and documentation quality	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	Requirements: FCh Implementation: Cantons, system provider	Completed (see Nos 24 and 25 OEV annex; Implemented by cantons and system provider)
A.2	Improve quality assurance in development of e-voting systems	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	Requirements: FCh Implementation: Cantons, system provider	Completed (see Nos 17 and 24 OEV annex; Implemented by cantons and system provider)
A.3	Use a proven and traceable build and deployment method	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	Requirements: FCh Implementation: Cantons, system provider	Completed (see No 24.3 OEV annex; Implemented by cantons and system provider)
A.7	Improve bases for detection (monitoring) and investigation of incidents (IT forensics)	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Definition of requirements and improvement process: Relaunch	Requirements: FCh Improvement process: System provider, cantons	Completed (see No 14 OEV annex; Ongoing improvements by cantons and system provider)
A.8	Create a joint plan for implementing measures for the Confederation and cantons	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh, cantons	Completed (see this catalogue of measures, which is regularly reviewed, adapted and published)
A.9	Complete system specification for voter authentication	Specifications serve as an instruction guide for system development. They also form the basis for assessing the system's conformity with the legal requirements. The system must not be underspecified (No 2.13.2 OEV annex). In the online voting system of Swiss Post,[15] voters are authenticated before casting their ballot in accordance with Number 2.8 of the OEV annex, but this authentication is not fully specified. Voter authentication specification will be completed with this measure and taken into consideration in the proofs of conformity required by Number 2.14 of the OEV annex as far as is reasonable. On the basis of the specified parts of the system, the examinations carried out and the explanations provided by Swiss Post, it was concluded that the risks associated with the incomplete specification may be considered sufficiently low. See Annex for additional information on this measure.	2nd quarter 2023 (to be used from National Council election 2023)	Cantons, system provider	*Completed*

[15] The action required as identified in this catalogue of measures relates to the Swiss Post system version, which was used for the first time in June 2023.

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
B.	**Effective control and oversight**				
B.1	Adapt responsibilities in the examination of the system and the underlying processes	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh	Completed (see Art. 27*l* PoRO and Art. 10 OEV in conjunction with No 26 OEV annex)
B.2	Develop an examination concept to assess conformity of the system and the underlying processes	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh with cantons and system provider	Completed (see audit concept for independent examinations at www.bk.admin.ch > Political rights > E-voting > Examination of systems)
B.3	Develop and apply a process to deal with non-conformities	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh with cantons and system provider	Completed (Process of dealing with non-conformities has been defined by the FCh in conjunction with the cantons and system provider)
B.4	Revise and improve risk assessment guidelines	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh with cantons and system provider	Completed (see FCh guidelines at www.bk.admin.ch > Political rights > E-voting > Federal legislation)
B.5	Draw up and implement a new process for the risk assessment of completely verifiable systems	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh, cantons, system provider	Completed (see Art. 4 OEV; All actors have assessed their risks; FCh risk assessment is published)
B.7	Integrate e-voting into the Confederation's critical infrastructure	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh (lead), cantons and system provider	Completed
B.9	Amend authorisation process	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh with cantons' involvement	Completed (see FCh guidelines at www.bk.admin.ch > Political rights > E-voting > Federal legislation)

C.	**Increasing transparency and trust**				
C.1	Restrict electorate permitted for completely verifiable systems	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh	Completed (see Art. 27*f* PoRO)
C.2	Draw up more detailed requirements for disclosing the source code	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	Requirements: FCh Disclosure: Cantons, system provider	Completed (see Art. 27*l*^{bis} PoRO and Arts 11 and 12 OEV; Published by cantons and system provider)
C.3	Run a bug bounty programme	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	Requirements: FCh Run by: Cantons, system provider	Completed (see Art. 27*l*^{ter} PoRO and Art. 13 OEV; Implemented by cantons

No	Measure	Description	Timeframe implementation	Responsibilities	Implementation status
					and system provider; see Community-Programm | Evoting-Community (post.ch))
C.4	Publish examination reports relevant to authorisation	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	FCh, cantons, system provider	Completed (see Art. 10 para. 4 OEV; Published by FCh, cantons and system provider)
C.5	Publish e-voting results in federal ballots	See description in catalogue of measures in SC VE final report dated 30.11.2020.	Relaunch	Requirements: FCh Publication: Cantons	Completed (see Art. 27*m* para. 3 PoRO; To be published by the cantons after the ballots)

Annex: Additional information on individual measures

No	Measure
A.9	**Complete system specification for voter authentication**

Voter authentication takes place in two stages. For each stage, voters enter a confidential code, which appears on their voting card:

1. Initial authentication takes place after the first confidential code has been entered. If it is successful, the online system sends a confidential voting parameter to the voter's device. Without this parameter, the user platform cannot transmit a vote that is accepted by the online system (authentication takes place based on the voting data).
2. By entering a second confidential code, voters confirm that they have checked that their vote has been correctly transmitted by means of the individual verifiability verification codes with a positive result. The code entered can also be considered an authentication credential, by means of which the voter is authenticated (see explanations of 25 May 2022 on No 2.12.8 OEV annex[16]).

In the Swiss Post system, which is to be used for the first time in June 2023, initial authentication of the first stage is not specified.

Based on the present system specification it can be observed that system security relates to the confidential parameter actually being confidential in the following way:

Assuming an attacker had access to the parameter, they would still not be able to cast a vote, as the second confidential code needs to be entered. Also, verifiability in accordance with Numbers 2.5 and 2.6 of the OEV annex would not be compromised if the parameter was accessed. Both of these observations can be derived from the cryptographic proof of conformity in Number 2.14.1 of the OEV annex. Access to the parameter could aid attempts to infer the content of votes cast in encrypted form. For the requirement in Number 2.7 of the OEV annex dedicated to voting secrecy to be met, access must not be possible. On the positive side, an attacker would have to obtain additional information collected in the online system during voting in order to benefit from their knowledge of the confidential parameter. However, for compliance with Number 2.7 of the OEV annex to be met, it must not be possible to draw any conclusions about the content of the votes cast from access to the entirety of the data maintained in the online system.

On maintaining secrecy of the confidential parameter: The confidential parameter sent in the first stage is only available to the online system in encrypted form. The same applies to other values in the online system that would allow decryption of the confidential parameter. Decryption is only possible if the first confidential code is known. Accordingly, the user platform sends this code in an altered form that does not allow decryption. This means that attackers who come into possession of the encrypted values in the online system are still unable to decrypt the confidential parameter. These observations are not supported by a specification, but solely by statements made by Swiss Post and observations of the source code. The completion and examination of the specification will allow a more structured analysis of the source code and thus help to achieve even greater certainty that the requirements resulting from Number 2.7 of the OEV annex are met.

No	Measure
A.11	**Publish source code of software for generating PDF files for printing voting cards**

The cryptographic protocol, which is needed to meet the requirements of individual verifiability, preservation of voting secrecy and voter authentication, can only be effective if the codes for the voting cards remain confidential and are correctly included in the PDF files.

On the basis of a security assessment conducted and the following considerations, it may be concluded that a decision not to disclose VCPS for the time being involves a sufficiently low risk:

- The cantons concerned undertake to carry out random checks during operation to ensure that the correct codes have been transferred to the PDF.

[16] Available at www.bk.admin.ch > Political rights > E-voting > Federal legislation.

- VCPS is operated on a laptop subject to Number 3 of the OEV annex, meaning operation is specially protected. In particular, it is operated without a network connection.
- Apart from the raw data for printing, no critical data according to Article 2 paragraph 1 letter v OEV is kept on the laptop.

No	Measure
A.13	**Do not apply SGSP problem as a hardness assumption**

The difficulty of solving the SGSP problem cannot be quantified conclusively on the basis of the DDH problem. As a result, the SGSP problem may only be considered to be at most as difficult to solve as the DDH problem. At the same time, no approach is known that describes a more efficient (albeit impractical) way of solving the SGSP problem than for the DDH problem, let alone one that points to a practicable way.

The conformity of the cryptographic protocol with the requirements for verifiability according to Numbers 2.5 and 2.6 of the OEV annex as well as authentication according to Number 2.8 of the OEV annex is not based on the SGSP problem. Attackers who managed to penetrate the online system, access the necessary data and solve the SGSP problem would be able to infer the content of the votes cast in encrypted form. This would mean that the cryptographic protocol would violate Number 2.7 of the OEV annex, according to which no conclusions about the content of the votes cast may be drawn from any of the data in the online system.

The following consideration leads to the conclusion that there is a sufficiently low risk in temporarily maintaining the SGSP problem as a hardness assumption: If a viable solution to the SGSP problem were to exist at all from a mathematical point of view, it is highly likely that a considerable amount of effort would have to be invested in finding it and also in applying it. In addition, there would be the effort of obtaining the data necessary for the attack; these are generated from the voting records in the online system. At the same time, there would be little benefit, if any, given the restricted electorate until the measure is implemented.

No	Measure
A.22	**Adjust auditors' tasks so that they do not perform operational tasks**

The auditors should detect cases where votes have been manipulated, deleted or illegitimately counted (see No 2.6 OEV annex). To do this, they evaluate cryptographic evidence that they receive along with the ballot result by means of the verifier, software openly available under an open source licence. They conduct the examination on a dedicated laptop.

In the Swiss Post system, the auditors also carry out an examination during the configuration phase; this needs to be correctly conducted for the requirements for individual verifiability according to Number 2.5 of the OEV annex, for the protection of voice secrecy according to Number 2.7 and for authentication according to Number 2.8 to be met. This examination is an operational task which is essentially the direct responsibility of the cantonal body in charge of e-voting. The cantonal body has its own laptop (so-called setup component) as a technical aid.

Since the auditors' laptop does not process any data whose confidentiality is a condition for fulfilling the above-mentioned requirements, and since the same modalities apply to the operation of the setup component and the auditors' technical aid, the solution chosen by the cantons and Swiss Post may be considered equivalent from a security perspective. The explanatory report on the 2022 total revision of the OEV also states that auditors may be used for tasks for which the setup component would otherwise be intended (see explanations on No 2.1 OEV annex).[17]

In the long term, operational tasks should also be carried out with the necessary precautions taken. At the same time, it should be possible to grant the auditors more independence, if this is desired and made possible by cantonal law. Operational tasks should therefore be carried out directly by the cantonal electoral office. The auditors, meanwhile, should uncover any operational errors as their task.

[17] Available at www.bk.admin.ch > Political rights > E-voting > Federal legislation.

No	Measure
A.24	**Further improve the conclusiveness of cryptographic proofs of conformity and increase their substance**

The cryptographic proofs of compliance serve to convince the readership – first and foremost the persons responsible for maintaining the proof – that the cryptographic protocol meets the requirements for verifiability, voting secrecy and voter authentication. Although inconclusiveness in the proof does not automatically mean that the cryptographic protocol has a vulnerability, let alone a vulnerability that can actually be used for an attack, before any other analyses are made such inconclusiveness must be considered a potential indication of a possible vulnerability. It is therefore important to consider inconclusiveness and eliminate it, either by improving just the proof or, if necessary, the cryptographic protocol as well. Swiss Post has substantially improved the proofs of compliance. The aim of this measure is to continue the work until the proof may be considered conclusive throughout.

The examination report by Haines, Pereira and Teague of 13.02.2023[18] gives examples with faulty or misleading arguments in the proof (see Sections 2.5.1 and 2.5.2 of the report). These are examples of inconclusiveness that can easily be remedied simply by adjusting the reasoning in the proof. They do not indicate weaknesses in the cryptographic protocol, which therefore does not need to be adapted. Nevertheless, it is worth making the adjustments to the proof. This way, people reading the proof do not have to spend time on problems that others have already analysed. Rather, they can specifically check the proof for new inconclusiveness and thus help to ensure that any need for improvement in the cryptographic protocol is discovered and addressed at an early stage.

In Section 2.5, the same examination report states that the reasoning within the proof would have to be made in greater detail on some points so that it could be understood and any errors or gaps in the reasoning identified. Without such explanations, the usefulness of the proof in such cases may be severely limited. Under this measure, the reasoning behind the proof should be extended on the points concerned.

The proof is also to take additional system elements into account. When proof of security is provided, it is usual to present system properties in a simplified form, which by nature conflicts with the substance of a proof. However, currently certain functions that are particularly important in the implemented security properties of the cryptographic protocol are not taken into account. In order to be able to ascertain in a structured manner that these functions bring the promised benefit and at the same time do not introduce any vulnerability into the protocol, they should be taken into account in the proof. This applies in particular to the following system elements:

- Before counting, the votes are mixed and decrypted on five different control components in accordance with Article 2 paragraph 1 letter d OEV in conjunction with Numbers 2 and 3 of the OEV annex. Each control component changes the order as well as the encryption of the votes without changing the votes (the encryption is changed, not the content of the encryption). After mixing, each control component performs partial decryption and passes the mixed and partially decrypted votes to the next control component. The first four of the total of five control components are located with Swiss Post. The private key for partial decryption is stored on them. The requirements in Number 3 of the OEV annex apply to the secrecy of the private keys; in particular, all components involved must be physically monitored by two persons at all times. The fifth control component is the laptop operated by the cantons; this is also subject to the requirements of Number 3 of the OEV annex. However, the private key for the fifth partial decryption and thus the definitive decryption of the votes is not stored on this laptop. Instead, the private key is derived from a long password that is split between two groups of people at the canton. Splitting the password between two groups of people prevents the fifth partial encryption from losing its effect if a single person were to pass on the password needed for decryption. Because of their importance for security, the functions used to calculate the private key from the two parts of the password are now to be considered in the proof. In particular, it should be shown that, under the trust assumptions for the protection of voting secrecy specified in Number 2.7 of the OEV annex, one of the two password parts alone is not sufficient to carry out the fifth partial decryption.
- Before mixing and partial decryption, each control component checks that all preceding control components have processed the votes correctly. To do this, they firstly check mathematical proofs that show that the preceding control components did not change any votes during mixing and partial decryption. Secondly, they check that the list of votes that the first control component has

[18] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

mixed and partially decrypted is correct. The four above-mentioned control components at Swiss Post are the same machines that generate the verification codes from the transmitted votes to meet individual verifiability requirements specified in Number 2.5 of the OEV annex and which store the votes until they are tallied. When they check whether the first control component has correctly mixed and partially decrypted the votes, they compare the votes with their own list of votes to be counted. If a control component indicates an inconsistency between its own list and that of the first control component, an investigation must take place to identify the correct list to be tallied. A tool known as a dispute resolver is used within this investigation. The cryptographic proof of security should now take into account the possible use of the dispute resolver and show that the correct list of votes to be counted can be found under the trust assumptions for individual verifiability in accordance with Number 2.5 of the OEV annex.

In addition to these two points, there are further system elements where it should be checked whether consideration of the cryptographic proof of compliance might be appropriate or at least an informal justification provided as to why this is not the case (see Section 2.1.3 of the examination report by Haines, Pereira and Teague of 13.02.2023).

At present, there is no concrete evidence that the inconclusiveness or the system elements not considered in the proofs are concealing weaknesses in the cryptographic protocol. Improvements in the proofs will provide further insight into any weaknesses and into improvements that may be required. The cryptographic protocol was also considered for compliance independently of the examination of the proofs. Considering that the electorate will be limited until this measure is implemented, the risk associated with the provisional need for action on the cryptographic proofs may be considered sufficiently low.

No	Measure
A.25	**Further improve the quality of the specification and the software**

In the points mentioned below, a need for improvement is identified; this is to be remedied on an ongoing basis and at the latest by the time Measure A.5 is implemented. The list is largely based on the results of the independent examination commissioned by the FCh.

In principle, all criticisms made here or in the examination reports concerning the quality of the specification and the software must be addressed, unless Swiss Post demonstrates that they are unjustified. In cases in which Swiss Post proposes alternative options for improvements that address a criticism raised to the same extent, the alternative improvements proposed may be implemented.

- The specification documents should express more clearly how the variables generated by and passed among protocol participants are to be used in the course of the protocol. In particular, it should be made clearer which variables are passed when the algorithms specified in pseudocode are called. In addition, it would be worth formulating more stringently the principles applied to checking the validity of the transferred variables. From the principles it should be perfectly clear which variables must be checked for validity and in which cases, against what basis and for what reason, as well as which variables may be changed in which cases and those which may never be changed. Any divergence from the principles should be clearly stated and justified. The principles should also regulate the use of context variables, namely those that must be and remain unchangeable during a ballot (see also Section 3.1.2 in the BFH examination report of 23.02.2023[19]). The validity checks and other principles that can be derived from the specification should be implemented in the source code in as uniform a form as possible and should be easy to find.
- The software is under-specified at certain points, i.e. the specification documents do not make it sufficiently clear what form implementation in the source code or the operational steps should take. For example, greater explanation is required regarding the minimum entropy required at choosing the passwords for the fifth partial decryption (see Measure A.24). The procedure for continuing the ballot after an inconsistency has been resolved thanks to the dispute resolver (see Measure A.24) is not sufficiently clear. Further examples can be found in the BFH examination report of 23.02.2023 in Section 2.4.1 (Election Use Cases), Sections 3.4.1, A.4.1 (3rd part), A.4.2 and B.4, as well as in Section 2.2 of the examination report by Haines, Pereira and Teague of 13.02.2023. *The following issues will be addressed by 2024: Haines, Pereira and Teague examination report of 31.07.2023 (Section 2.4), BFH examination report of 30.06.2023 (Section 2.1 [reference to the specification of Miller-Rabin], Section 2.4, Section 3.2.1, Section A.4).*

[19] Available at www.bk.admin.ch > Political rights > E-voting > Examination of systems.

- Further explanations of conscious decisions on system design and any risks associated with these decisions can contribute to a goal-oriented improvement process and should be provided at least where common standards, obvious practices or explicitly made recommendations are not applied. See, for example, the examination report by Essex of 21.11.2022 (Section 5, 'Clarify design choice of Bayer-Groth mixnet'), the examination report by Essex of 13.02.2023 (Sections 2.2, 2.3 and 2.4), the Haines, Pereira and Teague examination report of 13.02.2023 (Section 3.1) and the BFH examination report of 23.02.2023 (Sections 2.2.7 and 3.1.1, individual points in Section A.3.1, Section A.3.2 in the 1st, 7th and 8th sections, Sections B.3.2 and B.3.6). *The following issues will be addressed by 2024 or the lack of implementation will be justified: subsequent work on Measure A.16, Haines, Pereira and Teague examination report of 31.07.2023 (Section 2.1, Section 2.2.1, Section 2.2.2, Section 2.3, Section 3.1.2 [Nos 1 and 3], Section 5.1, Section 5.2.2, Section 5.2.3 [on strengthening «consensus»], BFH examination report of 30.06.2023 (Section 2.1 [Miller-Rabin instead of Baillie-PSW as well as «further potential improvements»], Section 3.1, Section 3.2.2 [«two comments»], Section A.2.2, Section A.3.1), Essex examination report of 01.08.2023 (Section 3, Section 4, Section 6.2 [issue 11], Section 7.1 [issues 13, 14], Section 8). The following issues will be addressed by 2025: BFH examination report of 30.06.2023 (Section 3.2.1, Section 3.2.2, Section 3.2.2 [«unminify»]).* In particular, the explanations should also be included in the material description of the planned improvements (see main part of this document on this measure). On this basis, it should be possible to discuss and re-assess whether it would be reasonable to design the system, in the individual points, according to a common standard, an obvious practice or a recommendation that has explicitly been proposed.
- The notation should be made more precise in order to counteract errors or misunderstandings, and minor errors should also be corrected; see for example the examination report by Essex of 21.11.2022 (Section 5, 'Implied modular reduction in subscript' and 'Improper quotation marks') and the BFH examination report of 23.02.2023 (Sections 3.1.5 and 3.2.2 [Algorithm 3.1, Algorithm 3.8, Algorithm 3.9 and Algorithm 3.12], Section 3.2.3 [Algorithm 4.11 and Algorithm 4.13] and others in Sections 3.2.5, 3.2.7, 3.2.8 and 3.3.1). *The following issues will be addressed by 2024: BFH examination report of 30.06.2023 (Ziff. 3.3), Essex examination report of 01.08.2023 (Section 6.1 [issue 9]).*