Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

Dialog with Experts 2020

Management Summary

1. Background and approach

Under the Federal Council's mandate of 26 June 2019, the Federal Chancellery FCh in collaboration with various cantons conducted an expert dialog. The purpose of the dialog was to provide the task-force of the Confederation and the cantons with a basis for drafting recommendations. The FCh discussed various issues concerning internet voting with 23 experts from the academic research community and the industrial sector[1], with the dialog being focused on technical matters. Most of the experts were from a field of exact science, three of them had a background in social science.

To start, the FCh sent out a questionnaire to the experts on 14 February 2020 containing around 60 questions.[2] Based on the answers, the FCh then conducted a moderated online discussion in writing from 5 May to 17 July based on the responses. The moderator provided the experts who participated with a summary of each discussion block. The summaries of the discussion blocks and of the answers to the questionnaire are contained in the main document entitled 'Summary of the Expert Dialog'.

2. 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.

3. Providing a secure system

3.1 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.

3.2 Standardizing 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.

[1] See list of mandated experts at www.bk.admin.ch > Political rights > E-Voting.
[2] See Questionnaire at www.bk.admin.ch > Political rights > E-Voting.

3.3 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.

3.4 Greater diversity as a basic condition for reliability

The experts are of the opinion that the diversity of components that are important for verifiability (i.e. control components and verifiers) is a basic condition for a system's trustworthiness: Defects in individual components would not have an impact on verifiability if other components function properly (exponential increase in security). Software is one of the elements of 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.

3.5 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.

4. Commissioned examinations and public scrutiny

4.1 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.

4.2 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 (BBP) with financial compensation. The BBP 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 BBP.

In addition to a BBP, 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.

4.3 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.[3] However, they consider disclosure under an open source licence to be more promising.

4.4 Dealing with non-conformities

Ideally, commissioned and public examinations should take place far enough in advance so that non-conformities 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 non-conformity, 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.

5. Experts' assessment of the dialog

The experts consider the dialog a milestone and believe it yielded valuable results. They suggest it should be seen as a starting point for a permanent exchange.

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