Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery

Political Rights Section

Vote électronique
Federal and cantonal requirements regarding public intrusion tests

According to the decision taken by the Steering Committee Vote électronique on 29th October 2018, the following requirements apply to public intrusion tests:

1. The system providers will allow a public intrusion test to be conducted on their system.

2. The test will cover a minimum of 4 weeks (duration of the voting process).

3. Participants from anywhere in the world can test the system.

4. The participants must be permitted to attack the system. It should be possible to attempt the following: to manipulate votes, to read votes that have been cast, to breach voting secrecy, to disable or circumvent security measures that protect votes and data relevant to security.

5. Participants are permitted to publish their test findings.

6. The system documentation and the source code must be published beforehand on the internet (the provisions of Ordinance on Electronic Voting Art. 7*a* f. apply). The participants will be given a sufficient number of polling cards as test material. These can be sent out electronically.

7. The feedback from the testers goes to a service company appointed by the Confederation and the cantons. This company will evaluate the feedback and provide its assessment as quickly as possible. The system providers will support the service company in doing this.

8. As a requirement for taking part in the test, the system providers may require persons interested in participation to adhere to a code of conduct. This could include the following obligations:

    a. to refrain from making attacks that are excluded from the test;
    b. to report any deficiencies found immediately;
    c. to postpone publication of any description of deficiencies found until the system providers have decided how to deal with the deficiencies.

9. The following are excluded from the test:

    a. load-based attacks that are intended to make voting impossible (distributed denial of service);
    b. attacks using fake messages that are intended to distract voters from the required processes (social engineering);
    c. attacks that are intended to manipulate votes where the attack can be recognised with the aid of individual verifiability;
    d. attacks that are intended to read votes by infecting the devices used for voting with malware;
    e. attacks on the system providers' services that are not connected with e-voting;
    f. attacks on the system for sending out polling cards online.

10. Once the system providers have given their consent to the test, the participants are protected from prosecution, unless their attacks are excluded from the test.