Summary of the feasibility study

An online voting system would consist of an online voting application, a front-end system and a back-end system. The online voting system would utilise Suomi.fi e-Identification, the voting register and the election information system. As the highest electoral authority, the Ministry of Justice would be the owner of the system, and the Legal Register Centre would be responsible for the procurement, implementation and maintenance of the online voting system.

If a decision is made to launch the procurement process of an online voting system, policies regarding the following matters should be outlined first:

- Would voting a second time be made possible in the online voting application?
  - This could make it more difficult to pressure voters or sell votes and help safeguard the secrecy of the ballot.
  - This would jeopardise the secrecy of online votes in the ballot box, as the vote and the voter's details would need to be stored together.
- Would it be possible to replace an online vote by a vote on paper during the advance voting period or on the actual election day?
  - This would make it more difficult to guarantee the secrecy of the ballot, as the vote and the voter's details would need to be stored together.
- Would voters be given any receipt of the vote they have cast, how would the receipt be provided and what kind of information would it contain?
  - A receipt would make it possible to breach the secrecy of the ballot and sell votes.
  - A receipt would make it more difficult to guarantee the secrecy of the ballot, because votes would need to be traceable.
- What action would be taken if suspicion of a mistake or a problem in the online voting system occurred?

Enough time and expertise should be allocated for the procurement process and for the more detailed definition of the final system. Information security, usability and accessibility are essential features that should be taken into account throughout the process from the very beginning. A transparent and open process helps to gain voters' confidence and makes it easier to identify any possible problems.

As regards identification, a decision-in-principle should be made whether a high assurance of identity – in practice an electronic certificate card – is required or whether a lower (substantial) level of assurance – online bank identifiers and a signature and an encryption key produced by a programme in the user's terminal device – is considered sufficient. The latter option is easier to implement, but the involved risks of misuse are greater. The working group has examined the pros and cons of the different options in this feasibility study. Based on the working group's assessment, the most secure option would be to use high level of assurance in the online voting system, but the challenge is that devices providing a high level of assurance are not widely used.

One of the objectives of the introduction of online voting is to facilitate the voting of certain groups, such as expatriate Finns, but, for the time being, identification abroad still requires Finnish strong electronic identification devices, which the majority of Finns living abroad do not have at their disposal. eIDAS may improve the situation in the future, but this requires several years of work. Cross-border utilisation of personal identity codes in the Nordic countries and the Baltic region will be examined in the next few years.

Guaranteeing end-to-end verifiability and secrecy of the ballot at the same time is technically a very challenging task. Voters should be able to ensure that their vote is counted as cast. Viable online voting systems do already exist, but none of them fulfils the necessary requirements as such and risks would continue to exist even after further development. The remaining uncertainties would need to be compensated for through legislation and

procedures. Irrespective of the technical solutions selected, the secrecy of the ballot could be at risk when voting would take place without the authorities' supervision.

Blockchains enable maintenance of a list of transactions or a log that can be audited and is difficult to forge. However, a straightforward way of using blockchains to solve the key problems related to online voting was not identified in the study.

Online voting technology and the development of the structures required for the system are not yet at a level that would enable a sufficiently secure implementation and introduction of the system. There are still open questions in terms of verifiability and the secrecy of the ballot. It is not expected that the key risks related to online voting would be solved in the next few years.

Thus, the working group does not recommend the introduction of online voting in Finland, as the risks involved in the project currently outweigh the benefits. However, technological developments and the digitalisation of democracy should be closely monitored also in future and the current election information system developed to meet the new requirements resulting from changes in the operational environment.