What is Verification of I-votes?

Verification of electronic votes (I-votes) enables to receive more accurate information on the security of the computer that was used to cast the I-vote. Verification makes it possible to detect when the computer is infected with malware that changes the I-vote or blocks the I-voting. According to the Riigikogu Election Act the verification of I-votes shall not be implemented before 2015. The system will be tested first at 2013 local elections. Voters will be able to verify their I-votes with a smart device (mobile phone or a tablet) equipped with a camera and Internet connection. During the 2013 test only Android devices are supported. Support for other platforms will be added by 2015.

The voter selects the candidate „12. Elmar“ and the computer generates a random number „92862847293“. These two pieces of information will be encrypted with the public key of the I-voting system. The resulting encrypted information (cryptogram) is digitally signed by the voter.

The digitally signed cryptogram is sent to the I-voting system server. The server generates a session code „1357“ end returns the code to the voter application.

The random number „92862847293“ and the session code „1357“ are displayed by the voting application as a QR-code. The verification app in the smart device reads the information through the device’s camera.
The verification app sends the session code „1357“ to the I-voting server. The server identifies the I-vote being verified and returns the digitally signed I-vote to the smart device. The voter’s identity is determined from the digital signature.

The I-voting server also sends the list of candidates in the election district of the voter to the verification app. (for example: 1...139, amongst them „12. Elmar“)

The verification app cannot decrypt the I-vote but it knows the random number „92862847293“ and the public key of the I-voting system that the data is encrypted with.

The verification app will now create cryptograms to all the candidates in the candidate list using the random number. Once it finds the cryptogram that matches the I-vote received from the server ((„12. Elmar“), the voter’s choice is confirmed.