Nitschke, Łukasz
Remote voting using smart cards with display. (English) Zbl 1240.94083

Summary: Internet voting is one of the most desired elements of modern democracy. It would make
the voting process more convenient, less expensive, and it could also be a democracy enhancing factor.
Unfortunately, almost all contemporary protocols for Internet voting have an inherent flaw – they neglect
susceptibility of the voter’s PC to cyber attacks. Another issue is providing verifiability and disabling
massive vote selling. This paper presents a protocol which does not suffer from any of these disadvantages
and can be integrated with traditional elections. The protocol is based on blind signatures and mixnets
and is designed to be run by secure devices with an integrated display. As a result, implementation costs
rise; however, with the advent of e-paper displays, such devices, in the form of smart cards, are expected
to become commodity items in the near future.

MSC:
94A60 Cryptography
68M11 Internet topics
68M12 Network protocols
91B12 Voting theory

Keywords:
internet voting; remote voting; cyber attack; verification; protocol