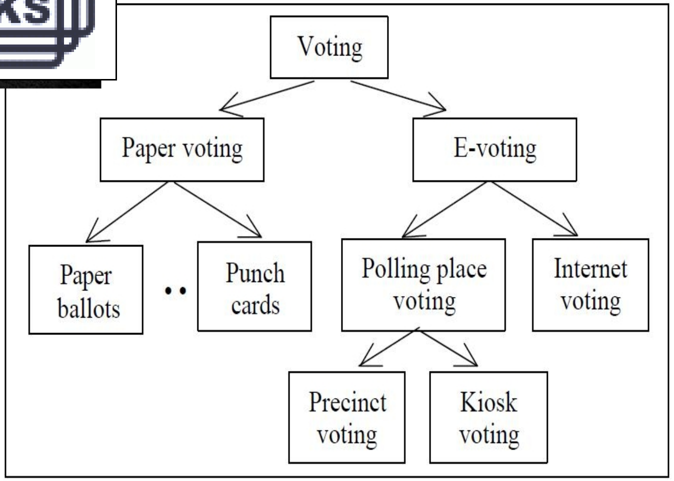
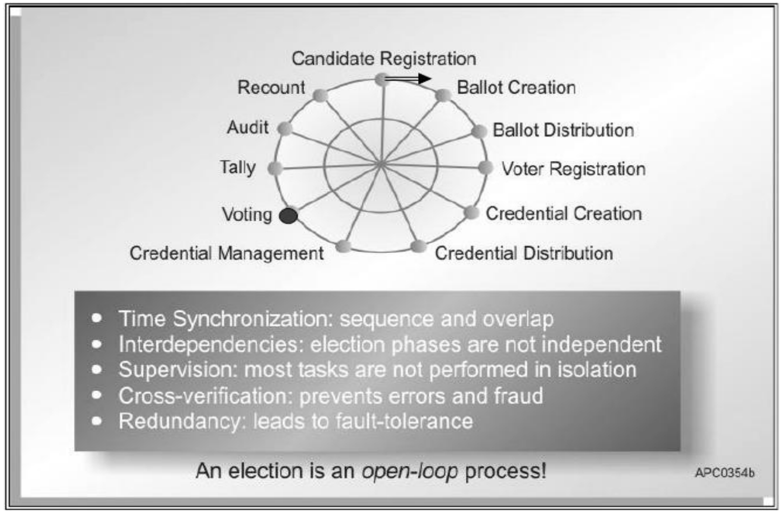
VoteHere, Inc., April 2002



Time-sequence of a typical voting process*



- Time Synchronization: sequence and overlap
- Interdependencies: election phases are not independent
- Supervision: most tasks are not performed in isolation
- Cross-verification: prevents errors and fraud
- Redundancy: leads to fault-tolerance

An election is an *open-loop* process!

* E. Gerck, "Private, secure, and auditable Internet voting", in D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA 2002.

Orhan Cetinkaya, and Deniz Cetinkaya

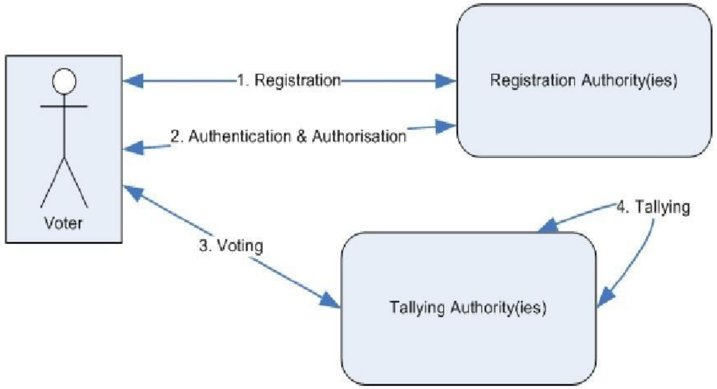
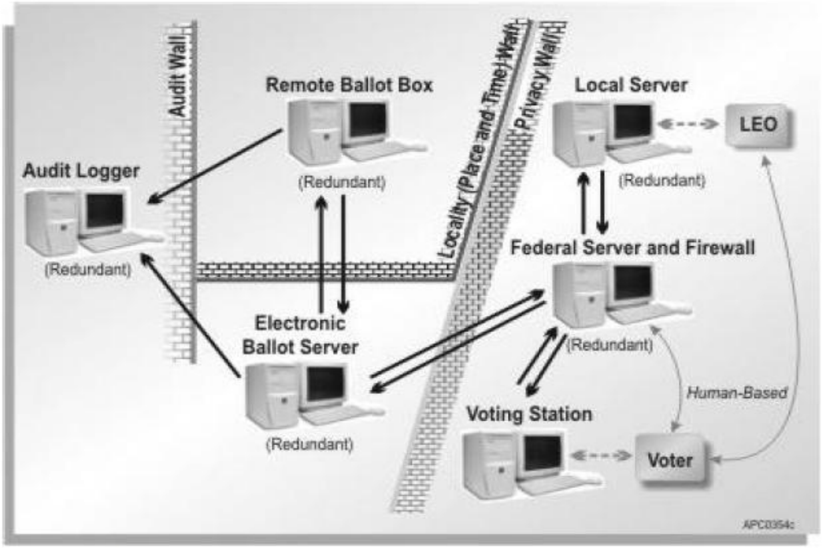


Figure 1: A general e-voting process

In the literature, numerous e-voting protocols have been proposed (Sampigethaya 2006). In those protocols, different requirement sets are defined, and whereas fulfilling these requirements different cryptographic tools and primitives are used. These underlying primitives are mainly blind signatures (Chaum 1982), mix-nets (Chaum 1981) and homomorphic encryption (Benaloh 1994). Before proceeding to the related work about V&V in e-voting protocols, we will briefly describe e-voting requirements.

DVS: An e-voting system architecture*



* E. Gerck, "Private, secure, and auditable Internet voting", in D. Gritzalis (Ed.), *Secure Electronic Voting*, Kluwer Academic Publishers, USA 2002.

Internetinis balsavimas. Techninės galimybės ir iššūkiai, Seminaras – atvira diskusija, VILNIUS , 2011 m. gruodžio 22 d., LIKS