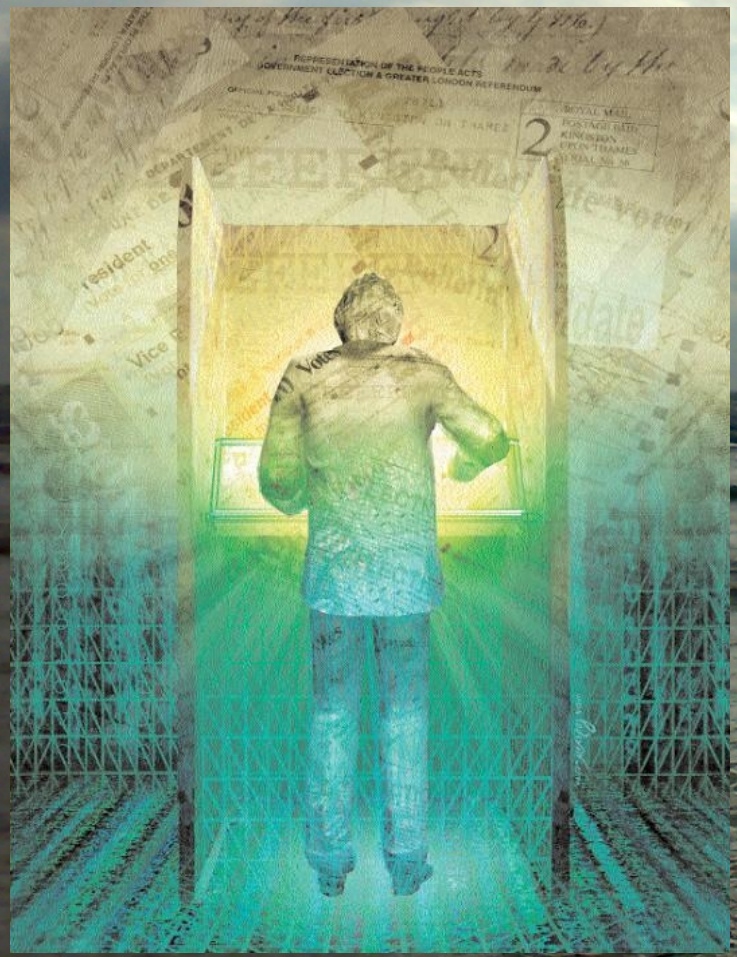
Internetinis balsavimas. Techninės galimybės ir iššūkiai

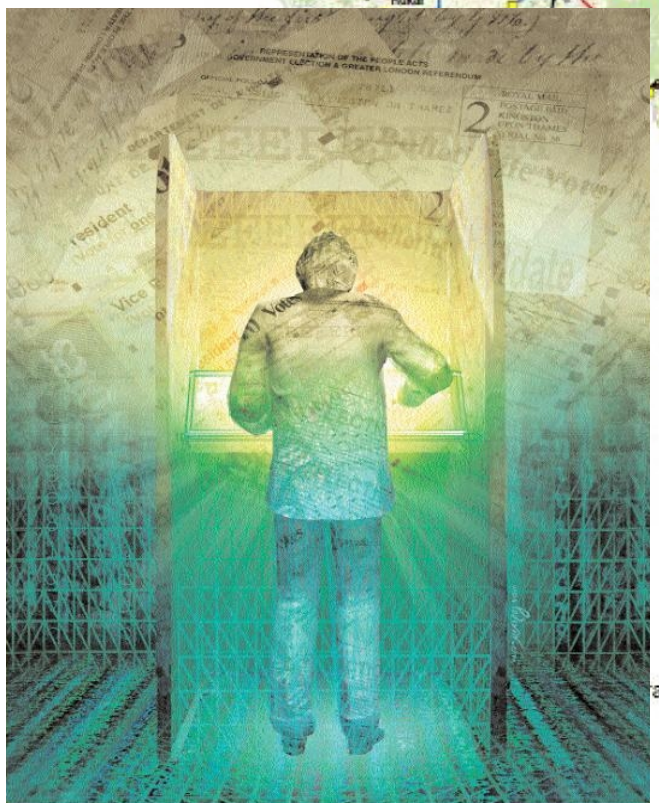
Įžanga seminarui– atvirai diskusijai

Romualdas Krukauskas

VILNIUS

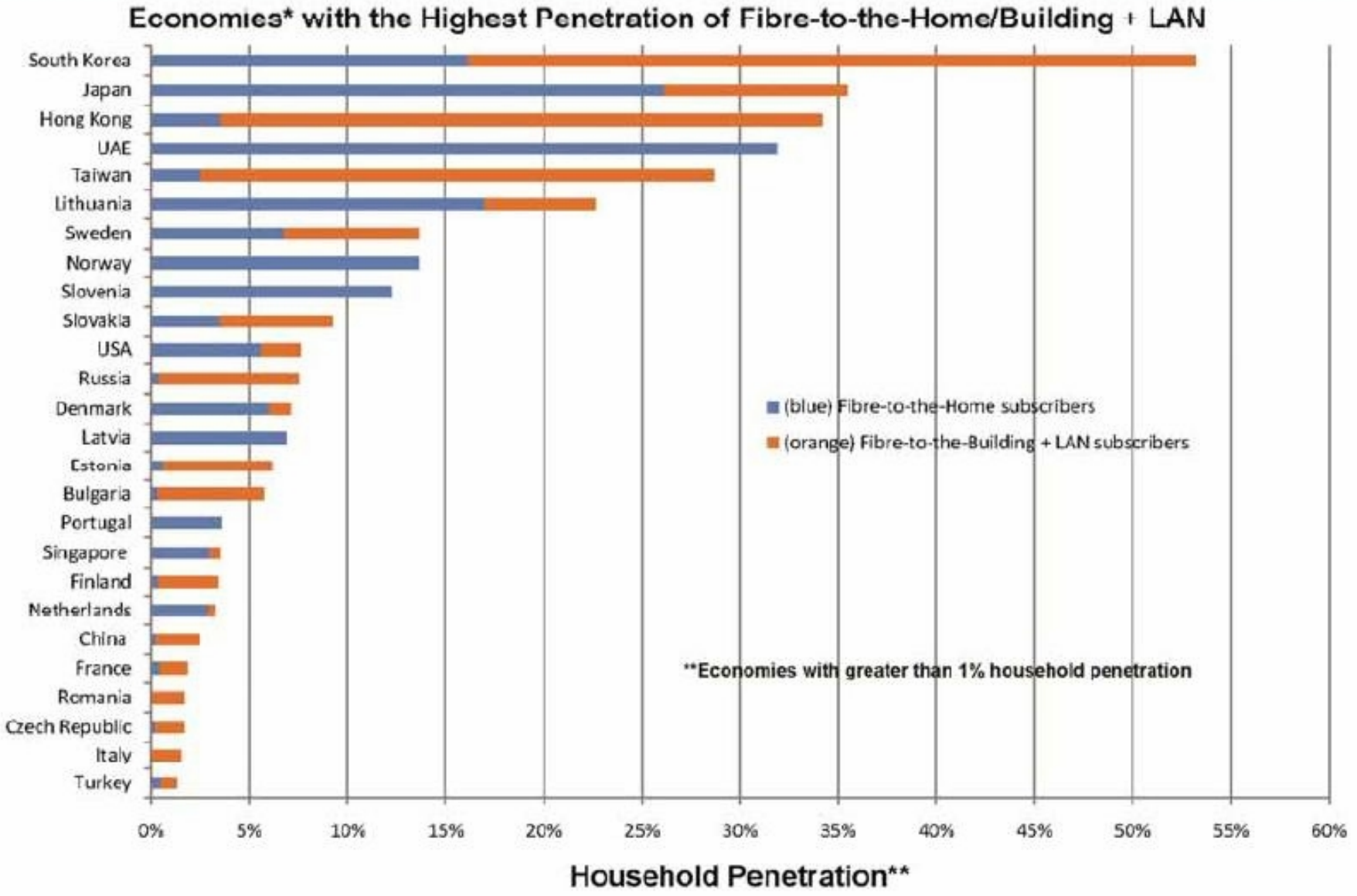
2011 m. gruodžio 22 d.


REPRESENTATION OF THE PEOPLE ACTS
GOVERNMENT ELECTION & GREATER LONDON REFERENDUM
ROYAL MAIL
POSTAGE PAID
KINGDOM
UNITED KINGDOM
2
resident
Vice
Vote



Asociacijos „Šviesolaidžių į namus Europos Taryba“ (Fibre to the Home Council Europe) 2011 m. vasario mėn. ataskaitos duomenimis Lietuva yra penkta valstybė pasaulyje ir pirma valstybė Europoje, pagal turimas šviesolaidines linijas į namų ūkius ir pastatus ("Fiber-to-the-Home/Building (FTTH/B)“.

FTTH Global Ranking – end 2010



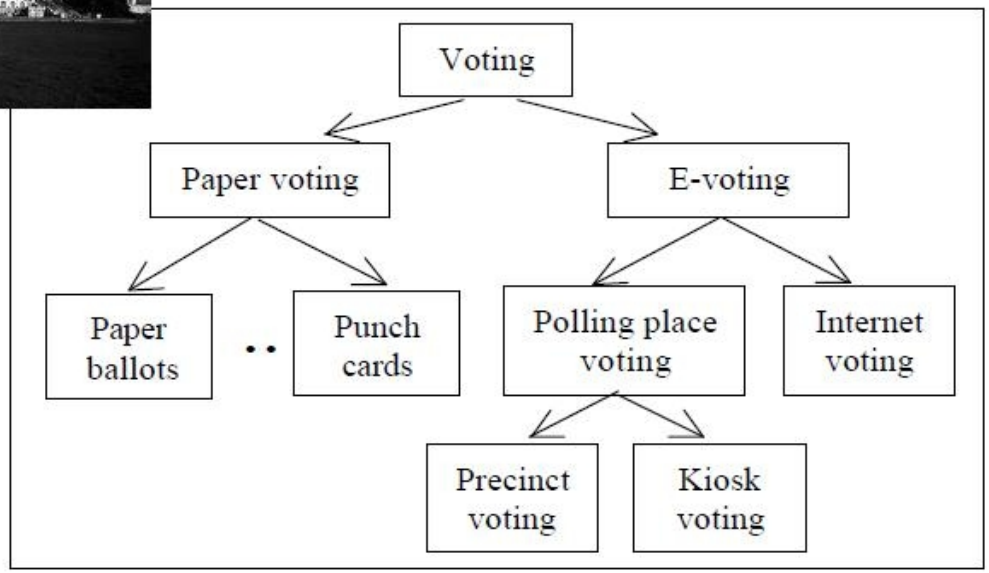
December 2010 Ranking
Source:
Fibre-to-the-Home Council
February 2011

***Economies with at least 200,000 households**

What is electronic voting (system)?

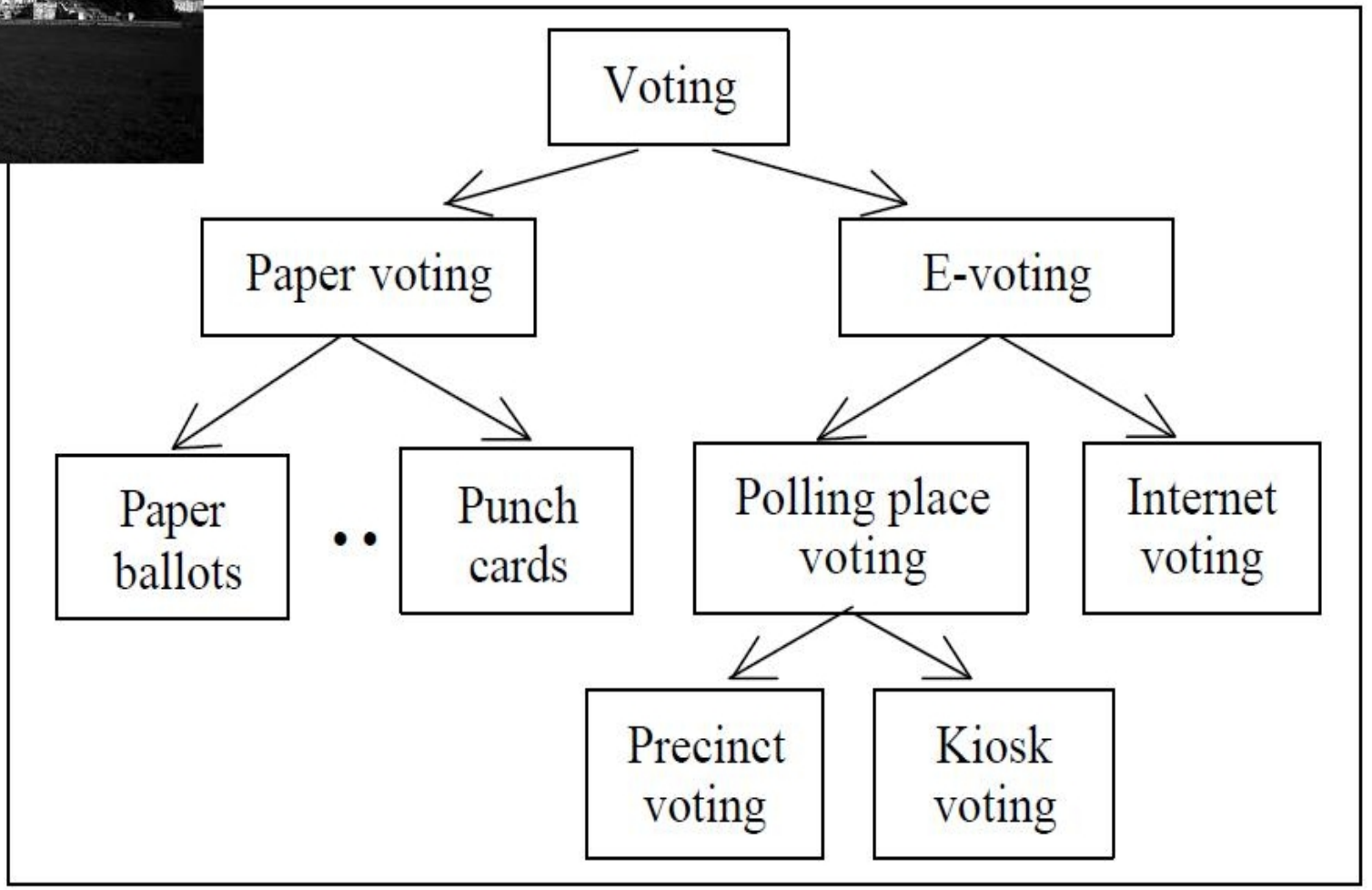
An *electronic voting (e-voting) system* is a voting system in which the election data is recorded, stored and processed primarily as digital information.

Network Voting System Standards, VoteHere, Inc., April 2002

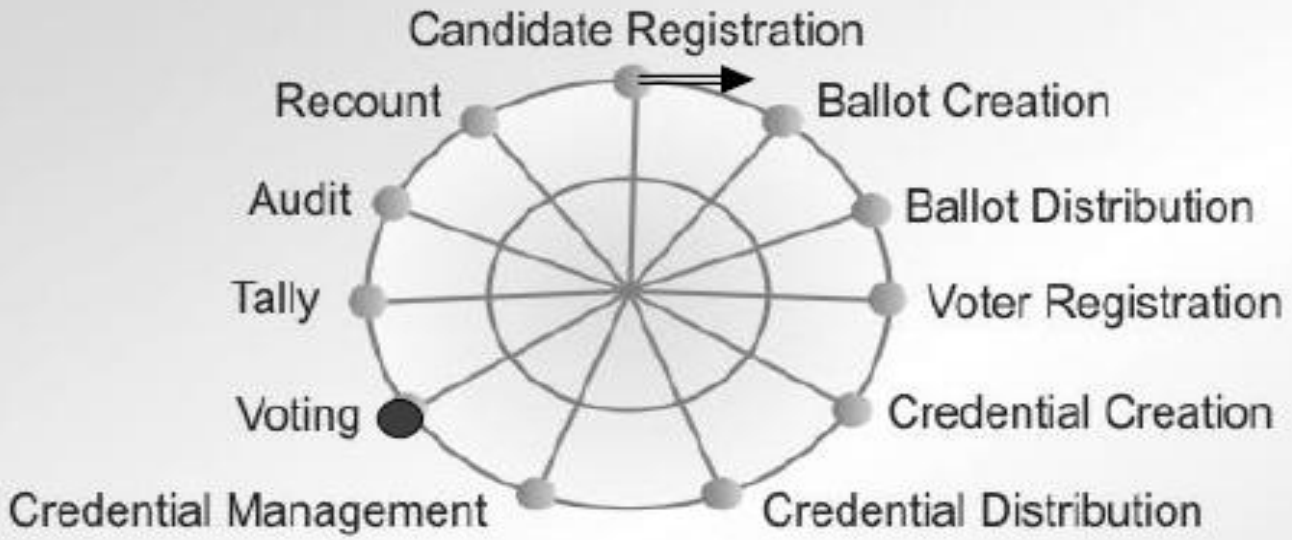


Note: Traditional electronic voting is …132 years old! (T. Edison, *Electrographic Vote Recorder*, US Patent, 1869).

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!

APC0354b

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

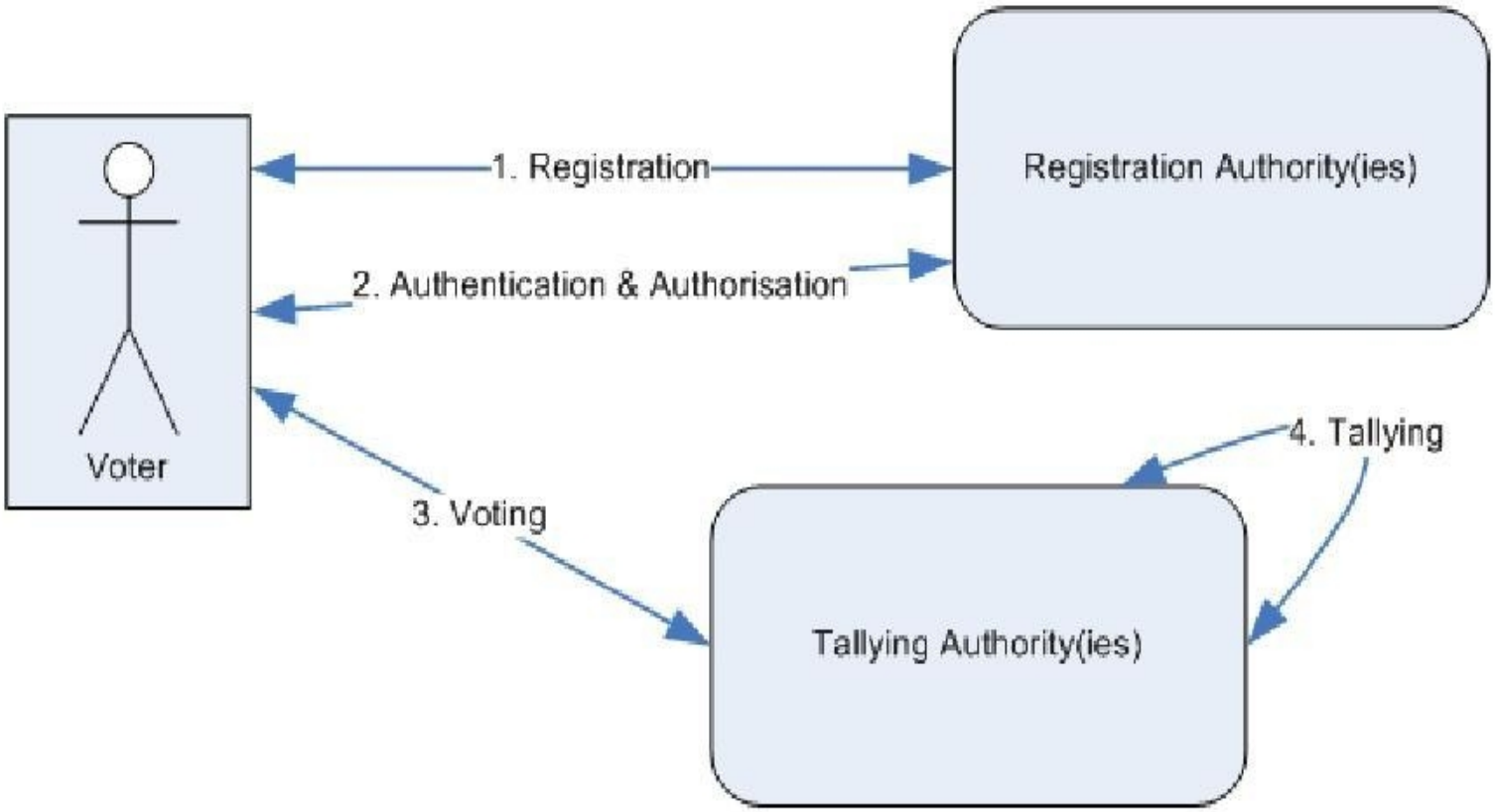


Figure 1: A general e-voting process

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.

Voting systems design criteria*

Secrecy:	No one should be able to determine how any individual voted.
Non-coercibility:	Voters should not be able to prove how they voted.
Flexibility:	Equipment should allow for a variety of ballot question formats.
Convenience:	Voters should be able to cast votes with minimal equipment and skills.
Certifiability:	Systems should be testable against essential criteria.
Transparency:	Voters should be able to possess a general understanding of the whole process.
Cost-effectiveness:	Systems should be affordable and efficient.

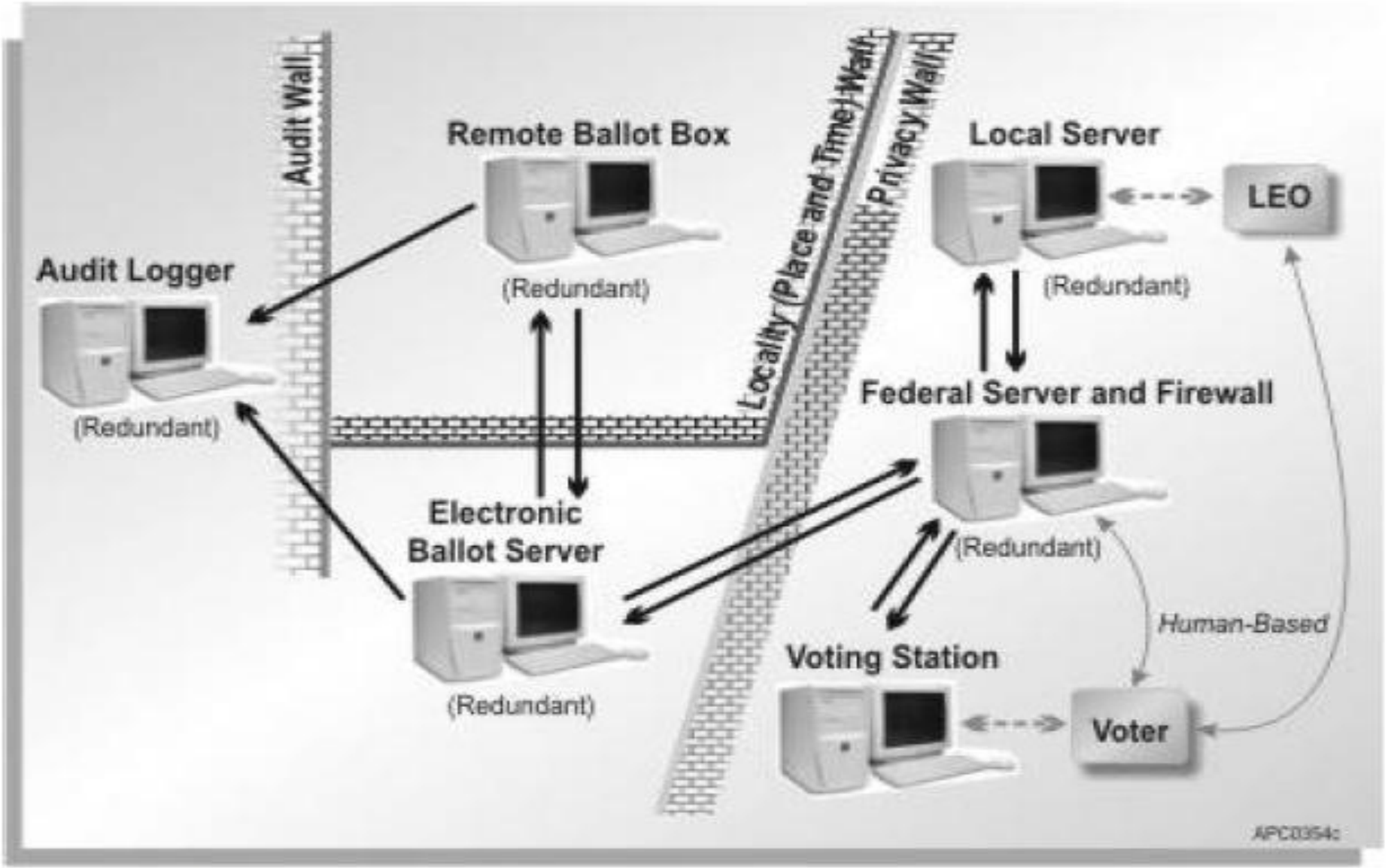
* Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, USA, March 2001.

Voting systems design criteria*

Authentication:	Only authorized voters should be able to vote.
Uniqueness:	No voter should be able to vote more than once.
Accuracy:	Voting systems should record the votes correctly.
Integrity:	Votes should not be able to be modified without detection.
Verifiability:	Should be possible to verify that votes are correctly counted for in the final tally.
Auditability:	There should be reliable and demonstrably authentic election records.
Reliability:	Systems should work robustly, even in the face of numerous failures.

* Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, USA, March 2001.

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.