Elektronické voľby: utópia alebo realita?

Peter Gaži

Katedra informatiky
FMFI UK, Bratislava
gazi@dcs.fmph.uniba.sk

Úvod do informačnej bezpečnosti
3/5/2011

Obsah

Čo si pod elektronickými voľbami predstaviť?

Prečo máme chcieť elektronické voľby?

Čo by sme mali od elektronických volieb požadovať?

Ako elektronické voľby zrealizovať?

Obsah

Čo všetko spadá pod elektronické voľby?

Pojem elektronických volieb zahŕňa všeličo:

- elektronické sčítanie hlasov
  - dierne štítky
  - optické sčítavacie skenery (marksense)
  - digitálne pero

Čo všetko spadá pod elektronické voľby?

Pojem elektronických volieb zahŕňa všeličo:

- elektronické sčítanie hlasov
  - dierne štítky
  - optické sčítavacie skenery (marksense)
  - digitálne pero
- elektronické odovzdanie (a sčítanie) hlasov
  - vo volebnej miestnosti
    - Direct Recording Electronic (DRE) systémy
  - cez internet
    - Public Network DRE
    - hlasovanie z ľubovoľného počítačaa s pripojením na internet

DRE systémy

- vo volebnej miestnosti
- klávesy/dotyková obrazovka
- výstup: elektronický (alebo aj papierový) súhrn hlasov
- niekedy tiež Voter-Verifiable Paper Audit Trail (VVPAT)

DRE systémy

- vo volebnej miestnosti
- klávesy/dotyková obrazovka
- výstup: elektronický (alebo aj papierový) súhrn hlasov
- niekedy tiež Voter-Verifiable Paper Audit Trail (VVPAT)

- urýchli sčítavanie
- pomoc handicapovaným voličom
- feedback pri nesprávnej voľbe

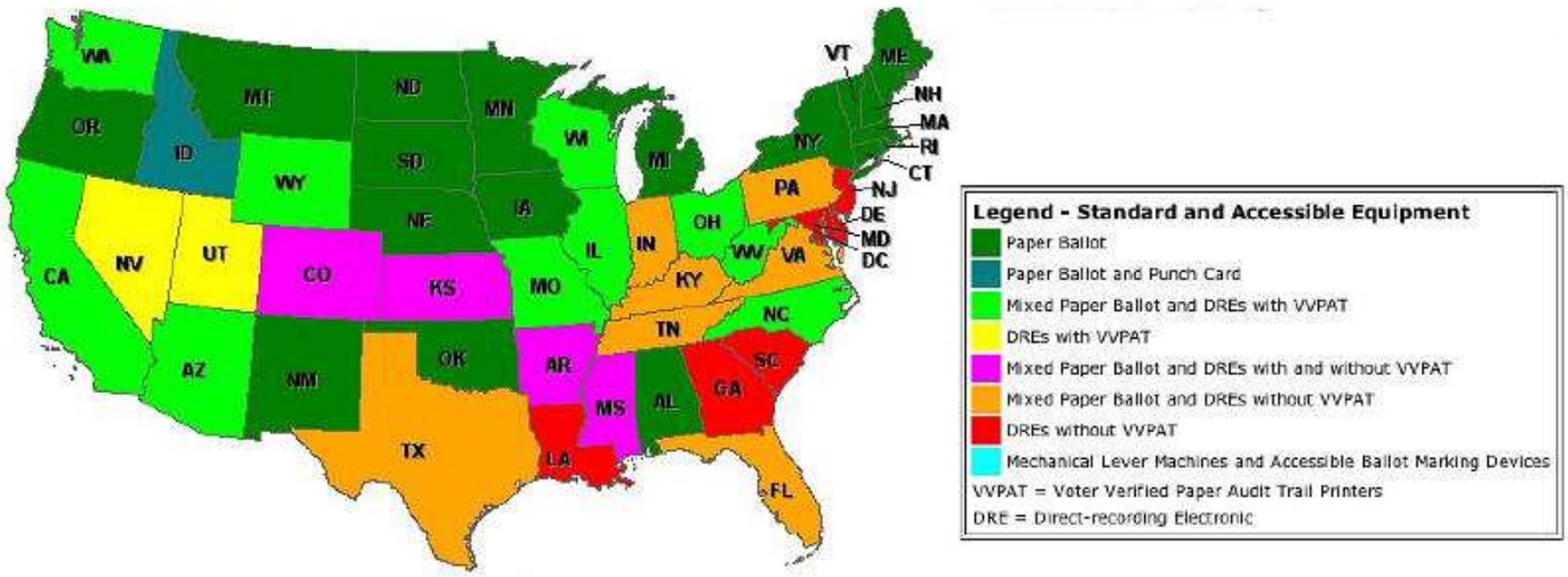
DRE systémy

- vo volebnej miestnosti
- klávesy/dotyková obrazovka
- výstup: elektronický (alebo aj papierový) súhrn hlasov
- niekedy tiež Voter-Verifiable Paper Audit Trail (VVPAT)

- urýchli sčítavanie
- pomoc handicapovaným voličom
- feedback pri nesprávnej voľbe

- notorické problémy s bezpečnosťou
- náklady na bezpečné skladovanie

Skúsenosti s DRE v USA



Zdroj: Verified Voting Foundation

Skúsenosti s DRE v USA (2)

Stovky zaznamenaných incidentov zlyhania DRE systémov:

- Fairfax County, Virginia, 2003: chyba programu spôsobila zmiznutie 100 hlasov
- Franklin County, Ohio, 2004: chyba programu, 3 893 fiktívnych hlasov
- Volusia County, Florida, 2000: podľa DRE systému získal Al Gore -16 022 hlasov
- Boone County, Iowa, 2003: podľa DRE systému odovzdaných 140 000 hlasov, okrsok má 50 000 obyvateľov a menej než polovica bola oprávnená voliť
- ...

\+ presvedčivé útoky z akademickej sféry

Zdroj: Bruce Schneier, Poorvi Vora

Hlasovanie cez internet

- možnosť voľby z ľubovoľného počítača s prístupom na internet

Hlasovanie cez internet

- možnosť voľby z ľubovoľného počítača s prístupom na internet

- všetky spomenuté výhody DRE
- dostupnosť zo zahraničia
- pohodlie

Hlasovanie cez internet

- možnosť voľby z ľubovoľného počítača s prístupom na internet

- všetky spomenuté výhody DRE
- dostupnosť zo zahraničia
- pohodlie

- úplne nové bezpečnostné výzvy
  - autentifikácia?
  - bezpečnosť klientských počítačov?
  - kupovanie hlasov?
  - ...

Skúsenosti s hlasovaním cez internet

- USA
  - 2000: primárky Demokratickej strany v Arizone umožňovali hlasovanie cez internet

Skúsenosti s hlasovaním cez internet

- USA
  - 2000: primárky Demokratickej strany v Arizone umožňovali hlasovanie cez internet
- Estónsko
  - od volieb v októbri 2005
  - prvá krajina s právne záväznými voľbami cez internet

Skúsenosti s hlasovaním cez internet

- USA
  - 2000: primárky Demokratickej strany v Arizone umožňovali hlasovanie cez internet
- Estónsko
  - od volieb v októbri 2005
  - prvá krajina s právne záväznými voľbami cez internet
- Švajčiarsko
  - 3 kantóny umožňujú voliť cez internet (Ženeva, Neuchâtel, Zürich)

Skúsenosti s hlasovaním cez internet

- USA
  - 2000: primárky Demokratickej strany v Arizone umožňovali hlasovanie cez internet
- Estónsko
  - od volieb v októbri 2005
  - prvá krajina s právne záväznými voľbami cez internet
- Švajčiarsko
  - 3 kantóny umožňujú voliť cez internet (Ženeva, Neuchâtel, Zürich)
- Kanada
  - niektoré obce umožnili voliť cez internet v regionálnych voľbách 2010

Skúsenosti s hlasovaním cez internet

- USA
  - 2000: primárky Demokratickej strany v Arizone umožňovali hlasovanie cez internet
- Estónsko
  - od volieb v októbri 2005
  - prvá krajina s právne záväznými voľbami cez internet
- Švajčiarsko
  - 3 kantóny umožňujú voliť cez internet (Ženeva, Neuchâtel, Zürich)
- Kanada
  - niektoré obce umožnili voliť cez internet v regionálnych voľbách 2010
- Holandsko
  - iniciatíva proti DRE zastavila aj vývoj internetových volieb
  - návrat k papierovým voľbám

Obsah

Možné motivácie na elektronizáciu volieb

- zvýšenie volebnej účasti
- nižšia cena
- rýchlejšie spracovanie výsledkov
- nižšia chybovosť
- vyššia bezpečnosť
- vyššie pohodlie

Možné motivácie na elektronizáciu volieb

- zvýšenie volebnej účasti?
- nižšia cena?
- rýchlejšie spracovanie výsledkov?
- nižšia chybovosť?
- vyššia bezpečnosť?
- vyššie pohodlie?

Zvýšenie volebnej účasti?

- case study: Estónsko

rok	online hlasov	z odovzdaných	účasť	typ
2004	-	-	26,8%	E
2009	58 669	14,7%	43,9%	E

Zvýšenie volebnej účasti?

- case study: Estónsko

rok	online hlasov	z odovzdaných	účasť	typ
2004	-	-	26,8%	E
2009	58 669	14,7%	43,9%	E
2002	-	-	52,5%	K
2005	9 317	1,9%	47,4%	K
2009	104 415	15,7%	60,6%	K

Zvýšenie volebnej účasti?

- case study: Estónsko

rok	online hlasov	z odovzdaných	účasť	typ
2004	-	-	26,8%	E
2009	58 669	14,7%	43,9%	E
2002	-	-	52,5%	K
2005	9 317	1,9%	47,4%	K
2009	104 415	15,7%	60,6%	K
2003	-	-	58,2%	P
2007	30 275	5,5%	61,9%	P
2011	140 846	24,3%	63,5%	P

Zvýšenie volebnej účasti?

- case study: Estónsko

rok	online hlasov	z odovzdaných	účasť	typ
2004	-	-	26,8%	E
2009	58 669	14,7%	43,9%	E
2002	-	-	52,5%	K
2005	9 317	1,9%	47,4%	K
2009	104 415	15,7%	60,6%	K
2003	-	-	58,2%	P
2007	30 275	5,5%	61,9%	P
2011	140 846	24,3%	63,5%	P

- Slovensko
  - 34% domácností s prístupom na internet (2007)
  - 16% obyvateľov nakupuje cez internet (2007)

Zdroj: Estonian National Electoral Committee, Štatistický úrad Slovenskej republiky

Nižšia cena?

- priestor na šetrenie
  - tlač volebných lístkov, voličských preukazov, ...
  - distribúcia
  - parlamentné voľby 2006: 46,5 mil. Sk

Zdroj: SITA

Nižšia cena?

- priestor na šetrenie
  - tlač volebných lístkov, voličských preukazov, ...
  - distribúcia
  - parlamentné voľby 2006: 46,5 mil. Sk
- náklady navyše:
  - implementácia, hardvér a softvér (jednorázové)
  - údržba, opravy, modernizácia systému
  - správa systému (noví zamestanci)

Zdroj: SITA

Nižšia cena?

- priestor na šetrenie
  - tlač volebných lístkov, voličských preukazov, ...
  - distribúcia
  - parlamentné voľby 2006: 46,5 mil. Sk
- náklady navyše:
  - implementácia, hardvér a softvér (jednorázové)
  - údržba, opravy, modernizácia systému
  - správa systému (noví zamestanci)

- z krátkodobého hľadiska sa zrejme neušetrí
- strednodobá a dlhodobá úspora závisí od využívanosti elektronického hlasovania

Zdroj: SITA

Rýchlejšie spracovanie výsledkov?

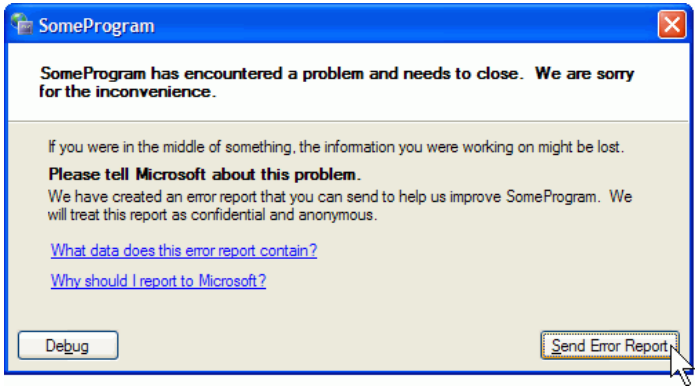
- väčšina modelov by priniesla dramatické zrýchlenie (výsledky dostupné do 1-2 hodín od ukončenia hlasovania)
- týka sa len hlasov odovzdaných elektronicky

Rýchlejšie spracovanie výsledkov?

- väčšina modelov by priniesla dramatické zrýchlenie (výsledky dostupné do 1-2 hodín od ukončenia hlasovania)
- týka sa len hlasov odovzdaných elektronicky

Užitočné len pri veľkom podiele elektronických hlasov, inak sú exit-polly a predbežné čiastočné výsledky presnejšie.

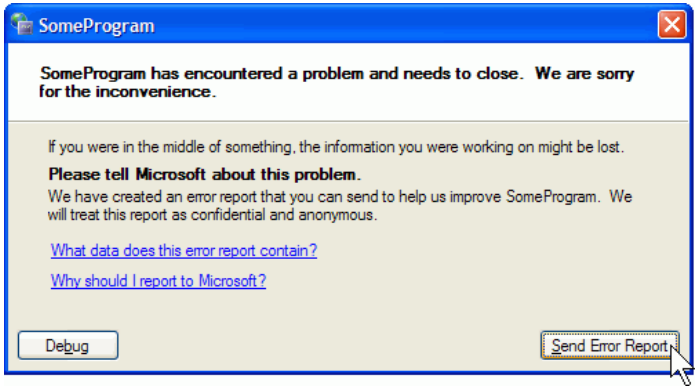
Nižšia chybovosť?



Estónsko: žiadne významnejšie technické problémy

skúsenosti s DRE systémami: veľký priestor na chyby

Nižšia chybovosť?



Estónsko: žiadne významnejšie technické problémy

skúsenosti s DRE systémami: veľký priestor na chyby

Opäť sa prejaví iba pri výraznom podiele elektronických hlasov.

Vyššia bezpečnosť?

- kým bude paralelne prebiehať aj papierová verzia, celková bezpečnosť nemôže vzrásť
  - bezpečnostné slabiny súčasného systému ostanú
  - potenciálne pribudnú slabiny nového systému

Vyššia bezpečnosť?

- kým bude paralelne prebiehať aj papierová verzia, celková bezpečnosť nemôže vzrásť
  - bezpečnostné slabiny súčasného systému ostanú
  - potenciálne pribudnú slabiny nového systému
- prehodnoťme cieľ: aspoň také bezpečné ako papierové voľby

Vyššia bezpečnosť?

- kým bude paralelne prebiehať aj papierová verzia, celková bezpečnosť nemôže vzrásť
  - bezpečnostné slabiny súčasného systému ostanú
  - potenciálne pribudnú slabiny nového systému
- prehodnoťme cieľ: aspoň také bezpečné ako papierové voľby

Čo všetko sa skrýva za slovom "bezpečné"?

Obsah

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný
- súkromnosť

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný
- súkromnosť
  - anonymita: nedá sa zistiť, ako volič hlasoval

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný
- súkromnosť
  - anonymita: nedá sa zistiť, ako volič hlasoval
  - receipt-freeness: volič nevie dokázať ako hlasoval

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný
- súkromnosť
  - anonymita: nedá sa zistiť, ako volič hlasoval
  - receipt-freeness: volič nevie dokázať ako hlasoval
- overiteľnosť

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný
- súkromnosť
  - anonymita: nedá sa zistiť, ako volič hlasoval
  - receipt-freeness: volič nevie dokázať ako hlasoval
- overiteľnosť
  - individuálna: volič vie overiť, že jeho hlas bol započítaný

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný
- súkromnosť
  - anonymita: nedá sa zistiť, ako volič hlasoval
  - receipt-freeness: volič nevie dokázať ako hlasoval
- overiteľnosť
  - individuálna: volič vie overiť, že jeho hlas bol započítaný
  - univerzálna: každý vie overiť, že hlasy boli sčítané korektne

Bezpečnostné požiadavky

Špecifické pre elektronické voľby:

- demokratickosť: práve oprávnení voliči majú práve 1 hlas
- presnosť: práve každý platný hlas je započítaný
- súkromnosť
  - anonymita: nedá sa zistiť, ako volič hlasoval
  - receipt-freeness: volič nevie dokázať ako hlasoval
- overiteľnosť
  - individuálna: volič vie overiť, že jeho hlas bol započítaný
  - univerzálna: každý vie overiť, že hlasy boli sčítané korektne
- férovosť: žiadne čiastkové výsledky pred koncom voľby

Bezpečnostné požiadavky (2)

Všeobecné požiadavky:

- dostupnosť
- robustnosť
- auditovateľnosť
- transparentnosť

Bezpečnostné požiadavky (2)

Všeobecné požiadavky:

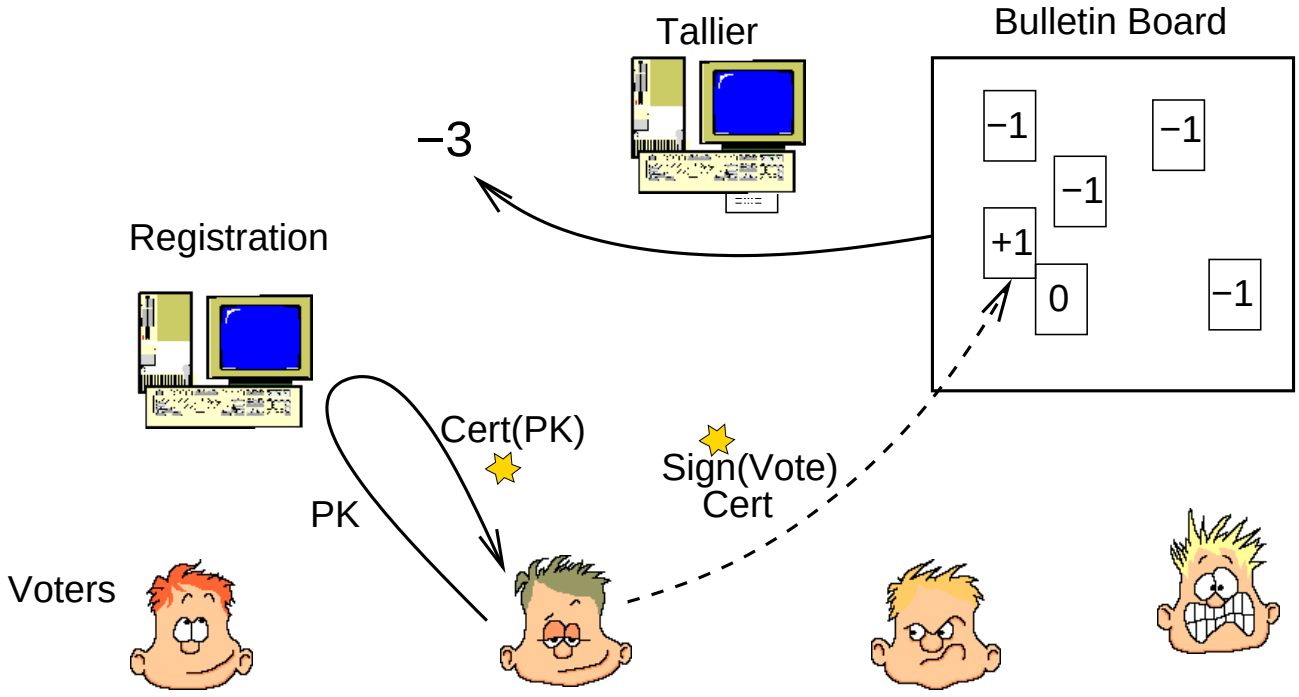
- dostupnosť
- robustnosť
- auditovateľnosť
- transparentnosť

Príjemné doplnkové požiadavky:

- pohodlnosť
- ekonomická výhodnosť
- ...

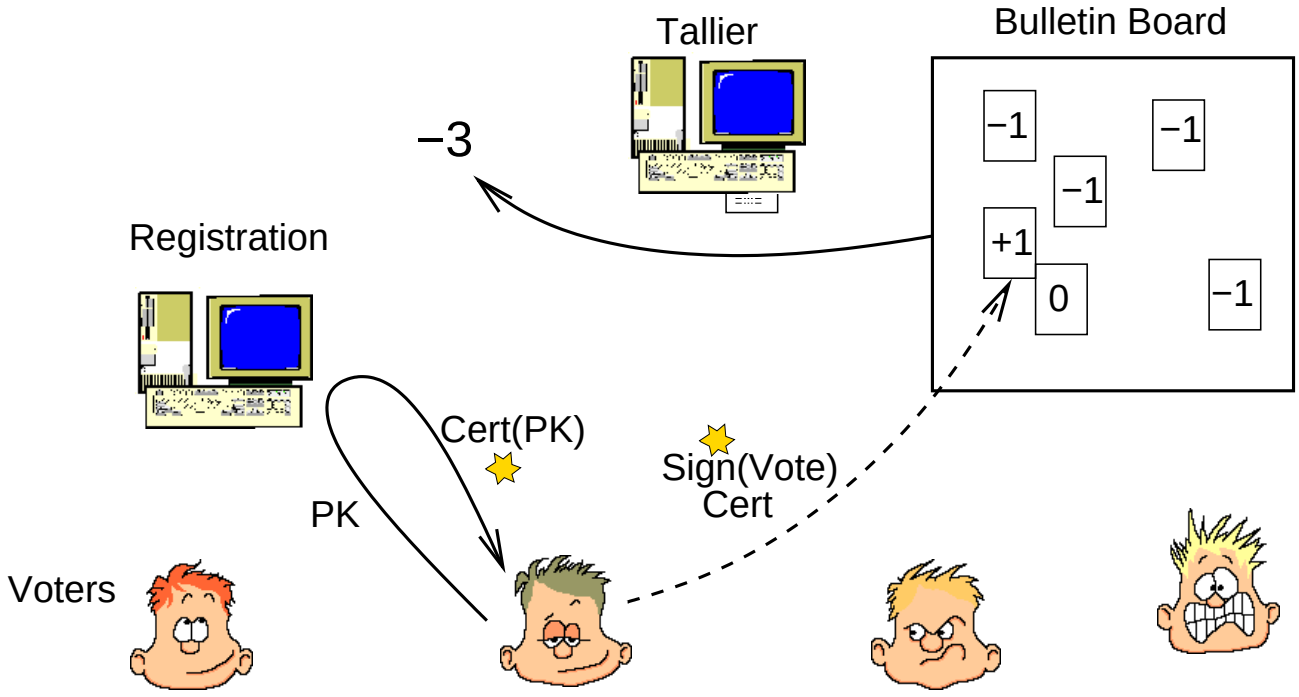
Obsah

Teoretické modely: voľby s anonymným kanálom



Zdroj: M. Hirt

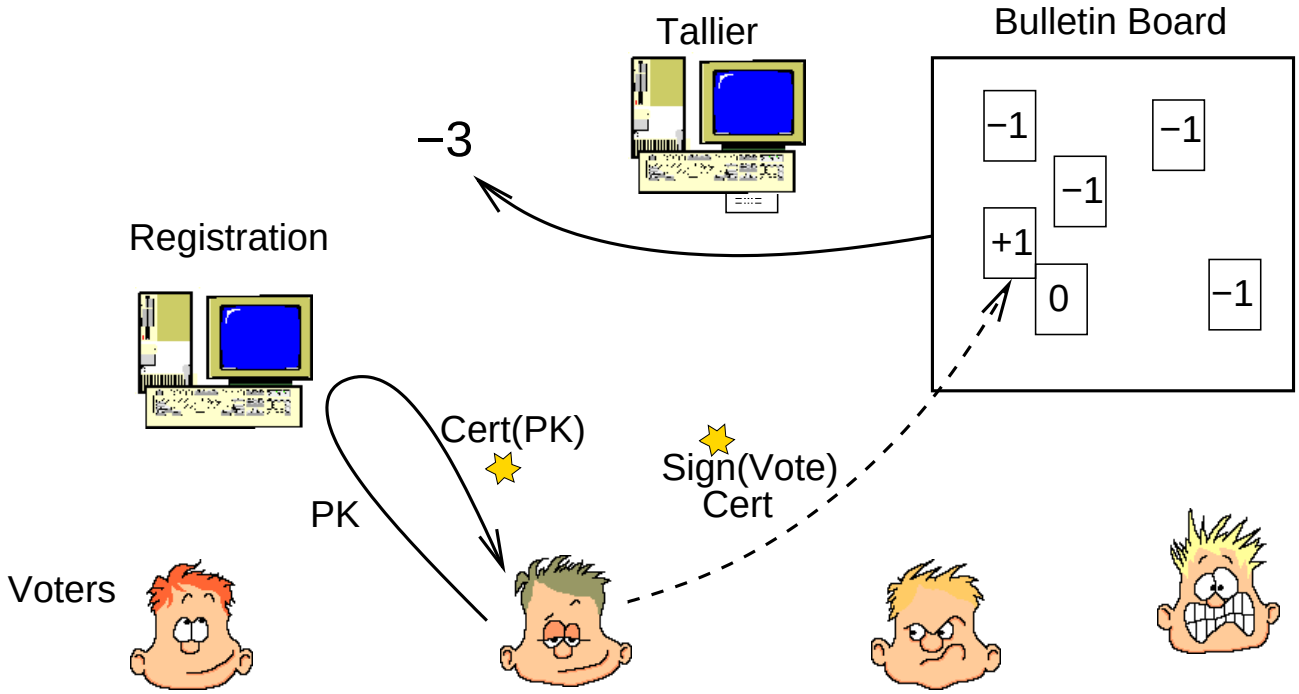
Teoretické modely: voľby s anonymným kanálom



- férovosť vyžaduje niečo navyše
  - Bulletin Board nie je čitateľný počas volieb
  - šifrovanie ďalším pk/sk párom

Zdroj: M. Hirt

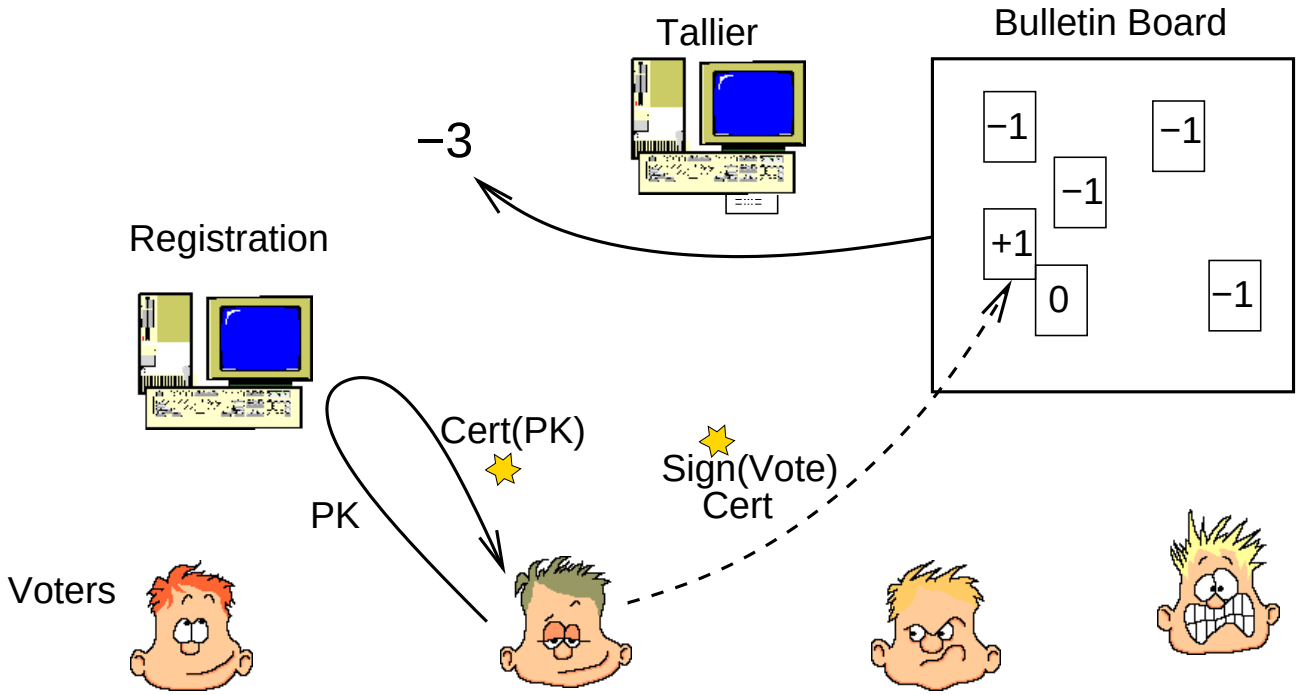
Teoretické modely: voľby s anonymným kanálom



- okamžité výsledky (jednoduché sčítavanie)
- aj zložité hlasovania

Zdroj: M. Hirt

Teoretické modely: voľby s anonymným kanálom

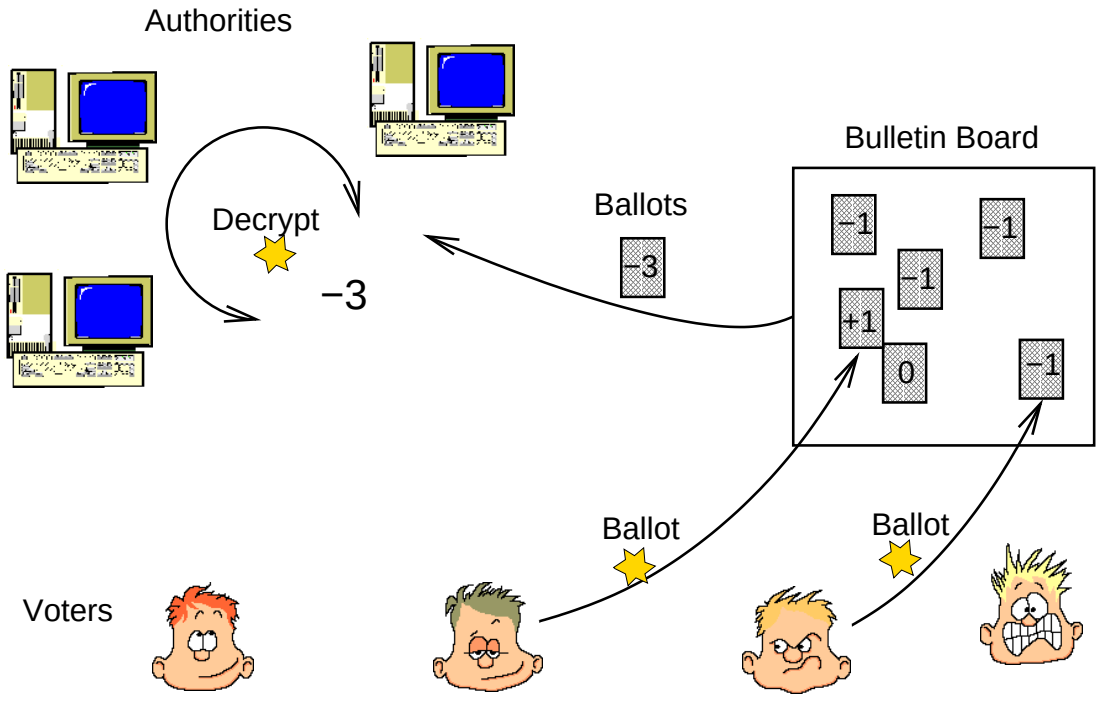


- okamžité výsledky (jednoduché sčítavanie)
- aj zložité hlasovania

- vyžaduje dve fázy

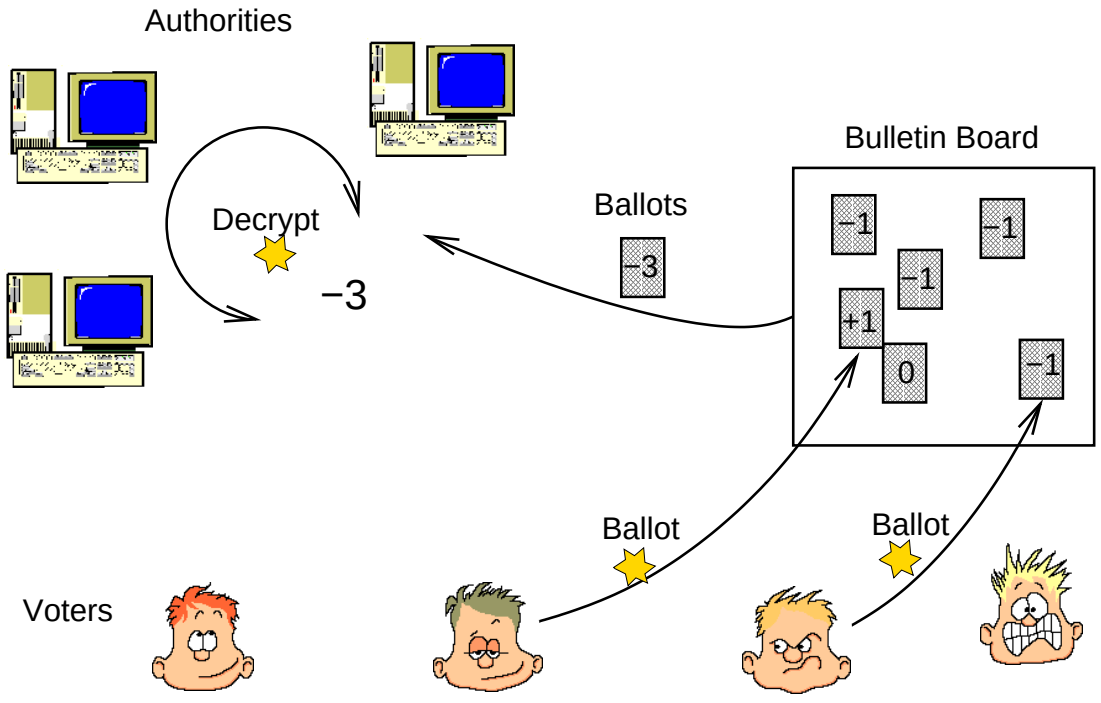
Zdroj: M. Hirt

Teoretické modely: voľby s homomorfným šifrovaním



Zdroj: M. Hirt

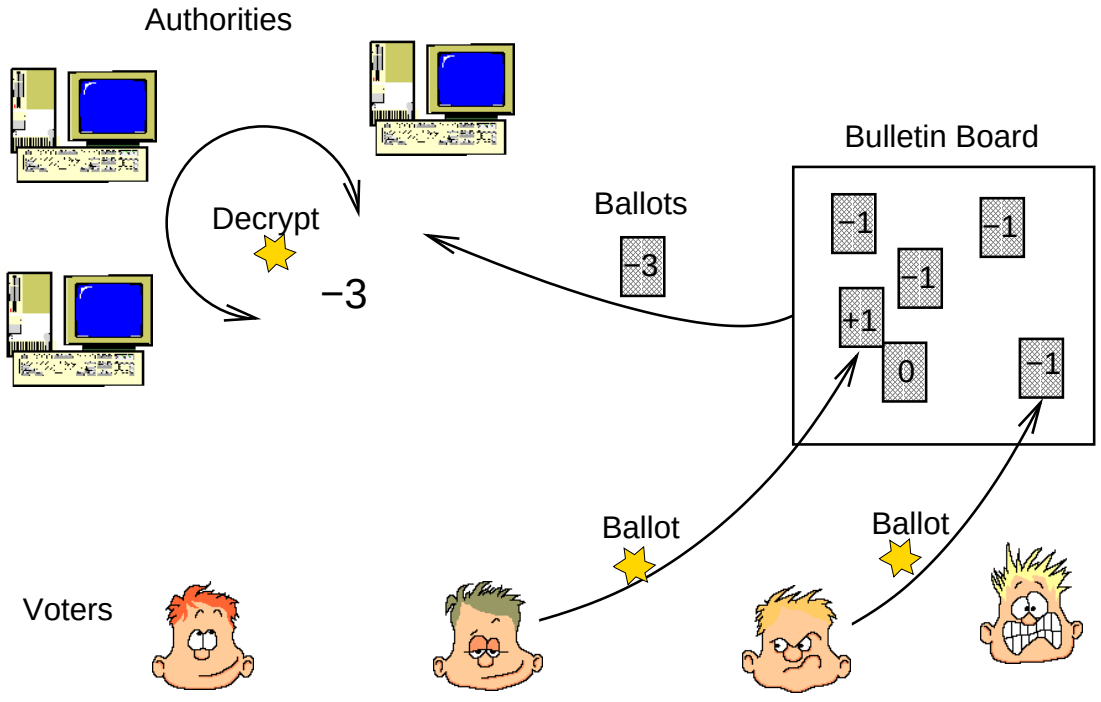
Teoretické modely: voľby s homomorfným šifrovaním



- treba dôkazy platnosti hlasov

Zdroj: M. Hirt

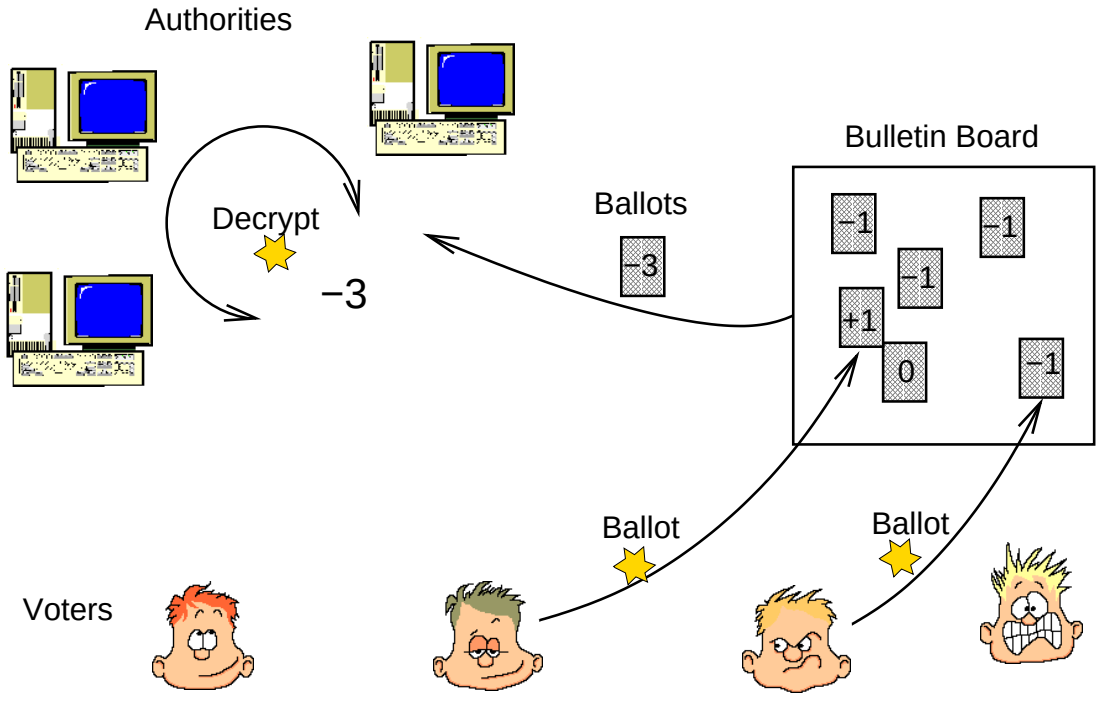
Teoretické modely: voľby s homomorfným šifrovaním



- okamžité výsledky (postupné sčítavanie)
- len 1 fáza
- ľahká overiteľnosť (otvoria sa hlasy namietajúcich)

Zdroj: M. Hirt

Teoretické modely: voľby s homomorfným šifrovaním

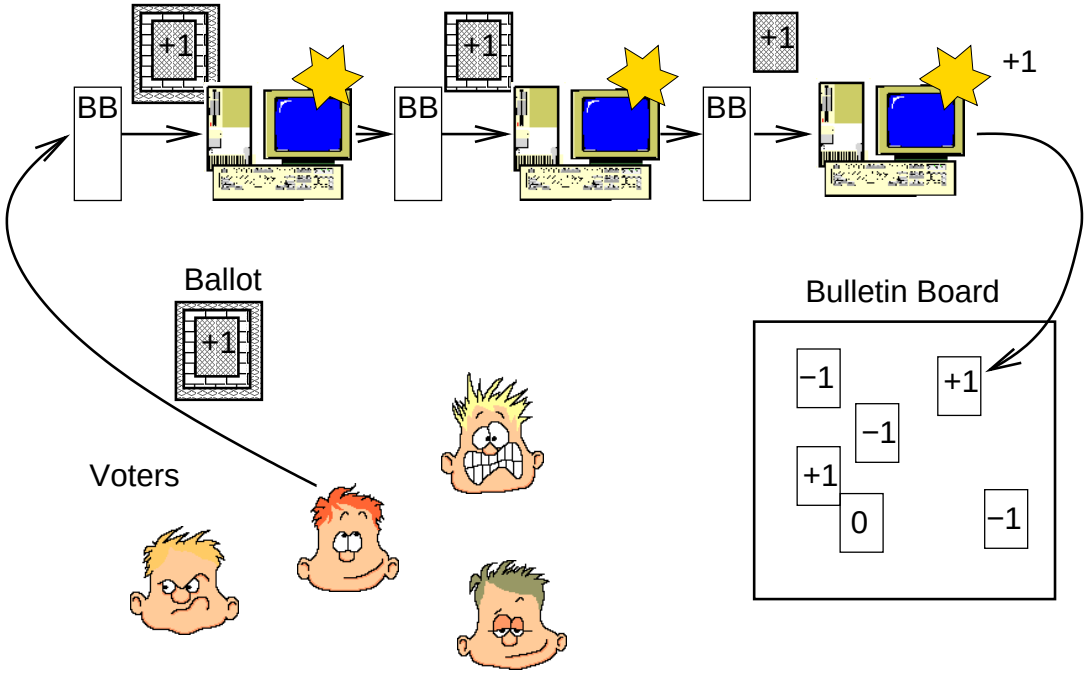


- okamžité výsledky (postupné sčítavanie)
- len 1 fáza
- ľahká overiteľnosť (otvoria sa hlasy namietajúcich)

- nepodporuje zložité hlasovania

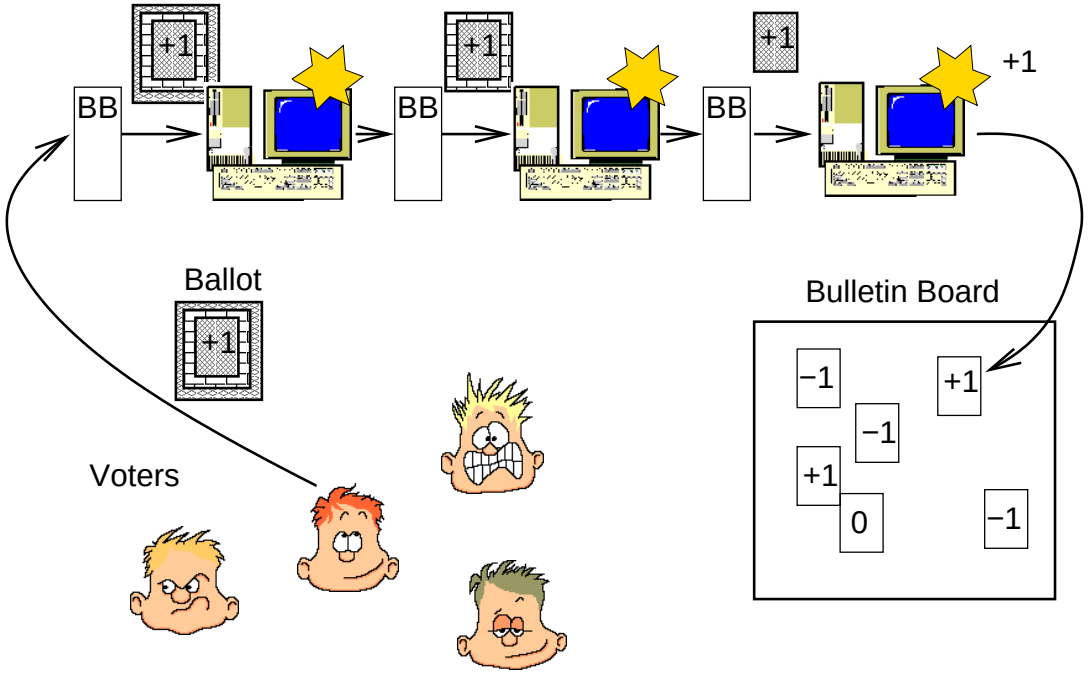
Zdroj: M. Hirt

Teoretické modely: voľby s použitím mixnets



Zdroj: M. Hirt

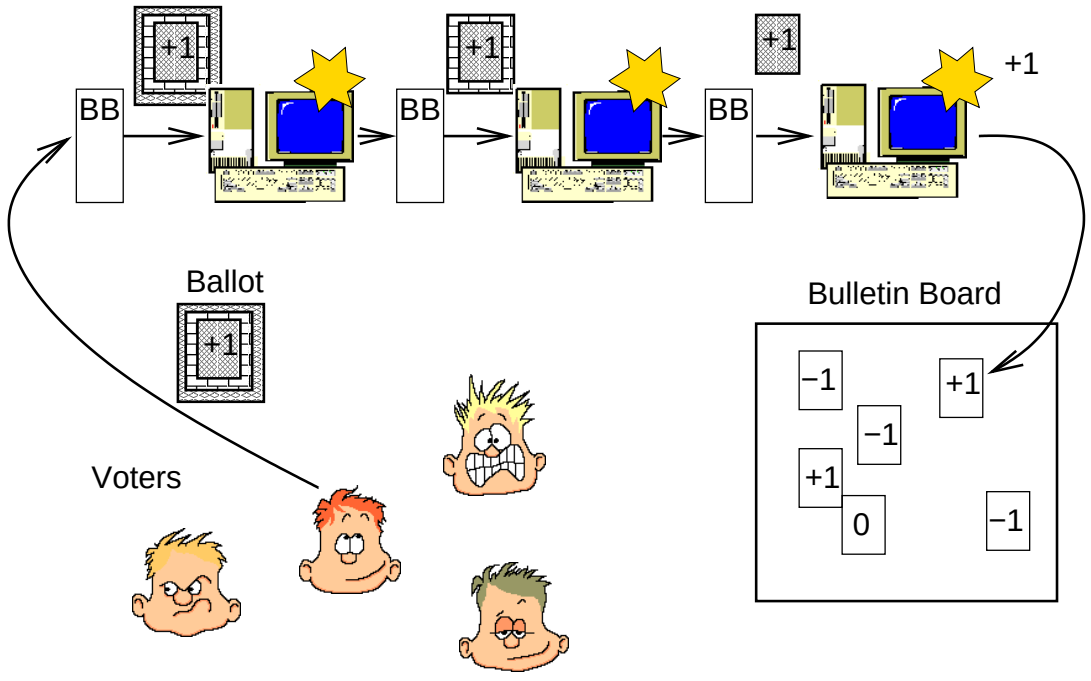
Teoretické modely: voľby s použitím mixnets



- autority musia dokazovať korektnosť mixovania
  - veľké a neefektívne dôkazy

Zdroj: M. Hirt

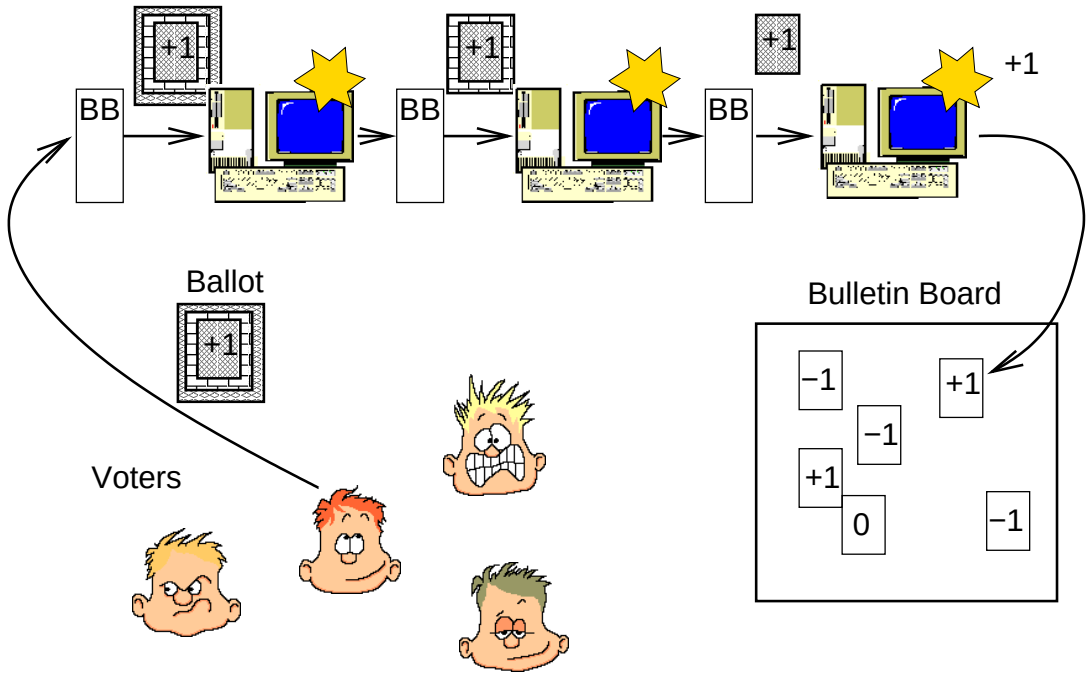
Teoretické modely: voľby s použitím mixnets



- len 1 fáza
- aj zložité hlasovania

Zdroj: M. Hirt

Teoretické modely: voľby s použitím mixnets



- len 1 fáza
- aj zložité hlasovania

- overenie je drahé
- neumožňuje priebežné vyhodnocovanie

Zdroj: M. Hirt

Praktický pohľad: priebeh volieb

1. Registrácia voliča
2. Identifikácia a autentifikácia
3. Autorizácia
4. Vykonanie voľby
5. Ukladanie a správa hlasov
6. Spočítavanie hlasov
7. Zverejnenie výsledkov
8. Riešenie protestov
9. Archivácia
10. Audit systému

Praktický pohľad: voľby na Slovensku

- 1 z 2 možností
  - referendum
- 1 z L možností
  - voľba starostu, primátora
- 1 z L možností, 2 kolá
  - voľba prezidenta
  - voľba župana
- K z L možností
  - voľby do VÚC
  - voľby do obecných zastupiteľstiev
  - voľby do Európskeho parlamentu
- 1 z L možností + preferenčné hlasy
  - parlamentné voľby

Praktický pohľad: voľby na Slovensku

- 1 z 2 možností
  - referendum
- 1 z L možností
  - voľba starostu, primátora
- 1 z L možností, 2 kolá
  - voľba prezidenta
  - voľba župana
- K z L možností
  - voľby do VÚC
  - voľby do obecných zastupiteľstiev
  - voľby do Európskeho parlamentu
- 1 z L možností + preferenčné hlasy
  - parlamentné voľby

Potrebujeme jednotné riešenie.

Autentizácia voliča

- Estónsko
  - elektronický občiansky preukaz (ID-Card)
  - autentifikácia, digitálne podpisy
  - momentálne vydaných 1 156 211 ID-kariet (na 1 340 022 obyvateľov)
  - potrebná čítačka (20 EUR)

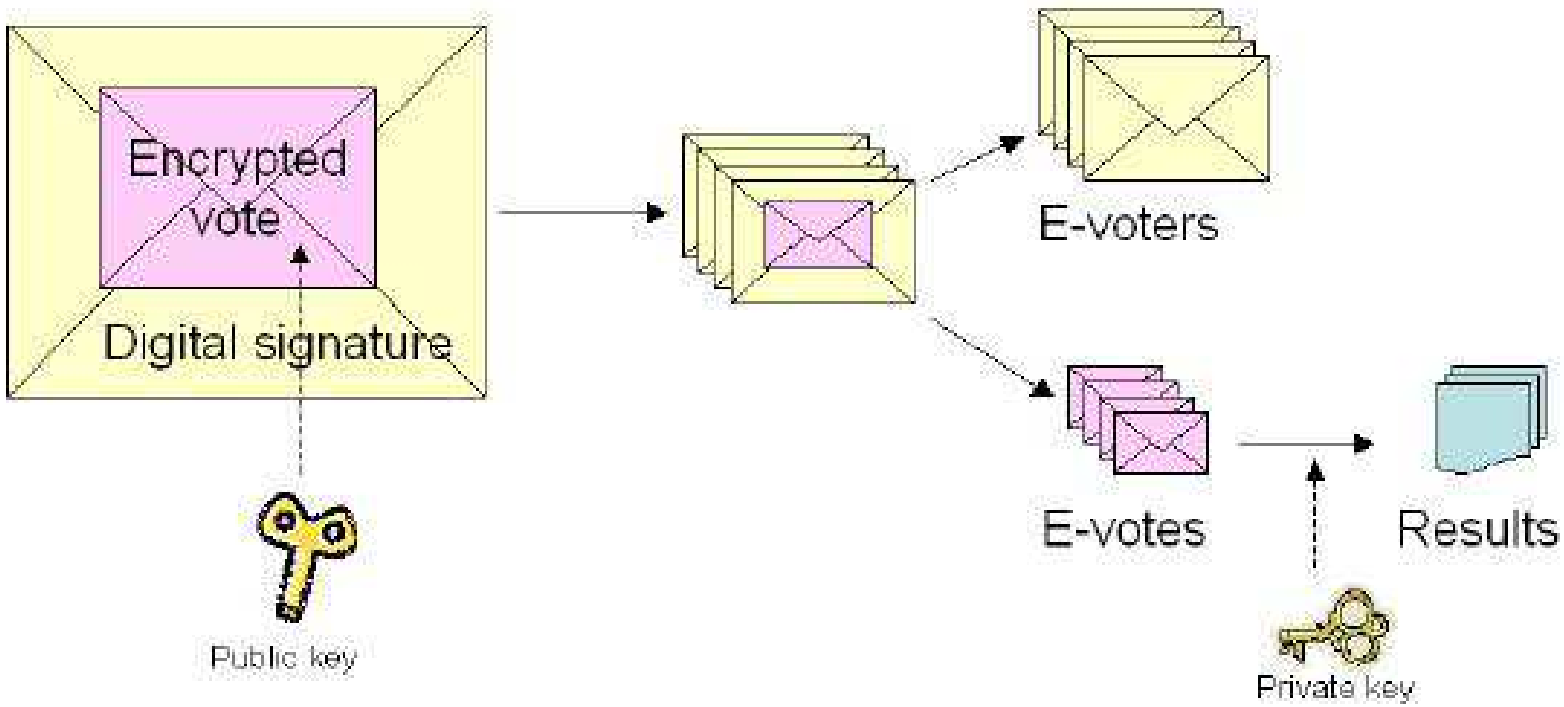
Autentizácia voliča

- Estónsko
  - elektronický občiansky preukaz (ID-Card)
  - autentifikácia, digitálne podpisy
  - momentálne vydaných 1 156 211 ID-kariet (na 1 340 022 obyvateľov)
  - potrebná čítačka (20 EUR)

- Slovensko?
  - existuje plán Elektronickej identifikačnej karty (eID)
  - pridanie čipu do OP
  - ukončenie realizácie: august 2012
  - zaručený el. podpis, šifrovanie

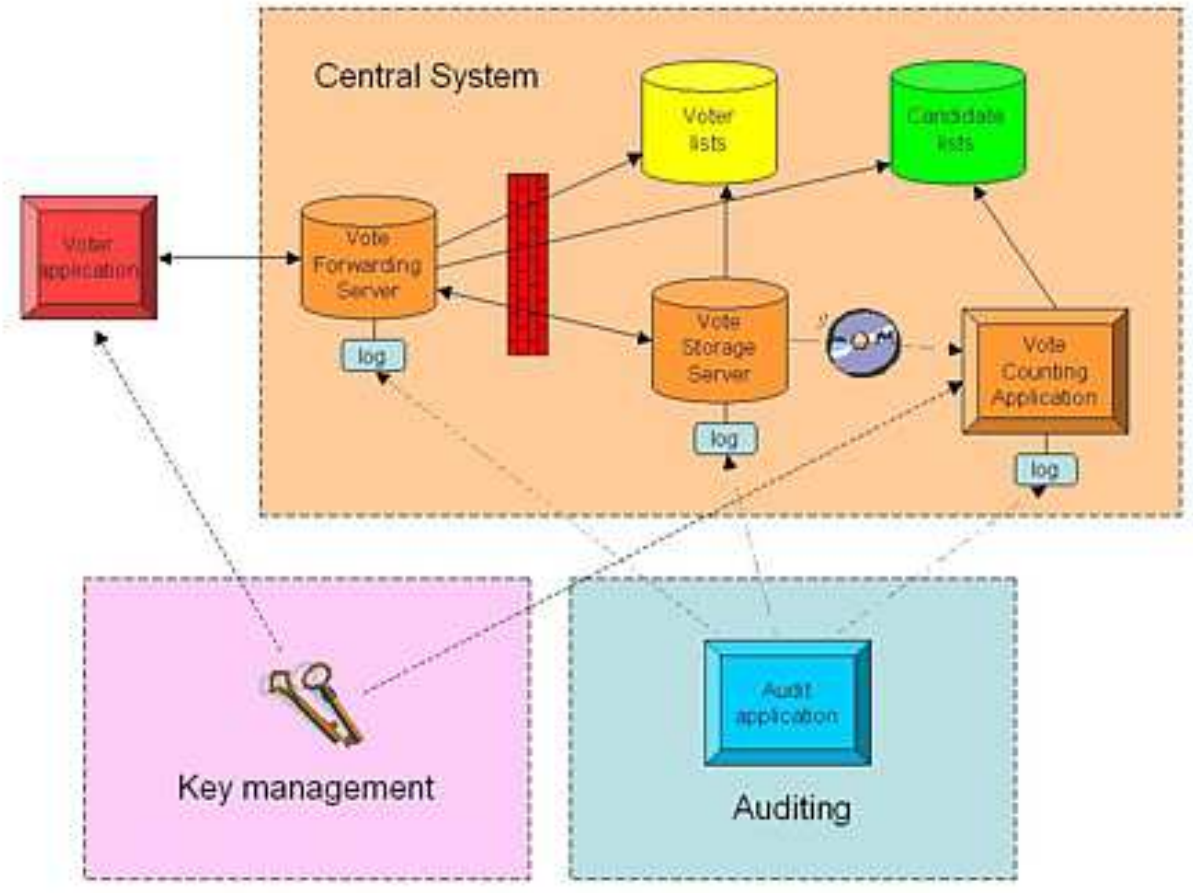
Zdroj: Estonian National Electoral Committee, Ministerstvo vnútra Slovenskej republiky

Estónsky model



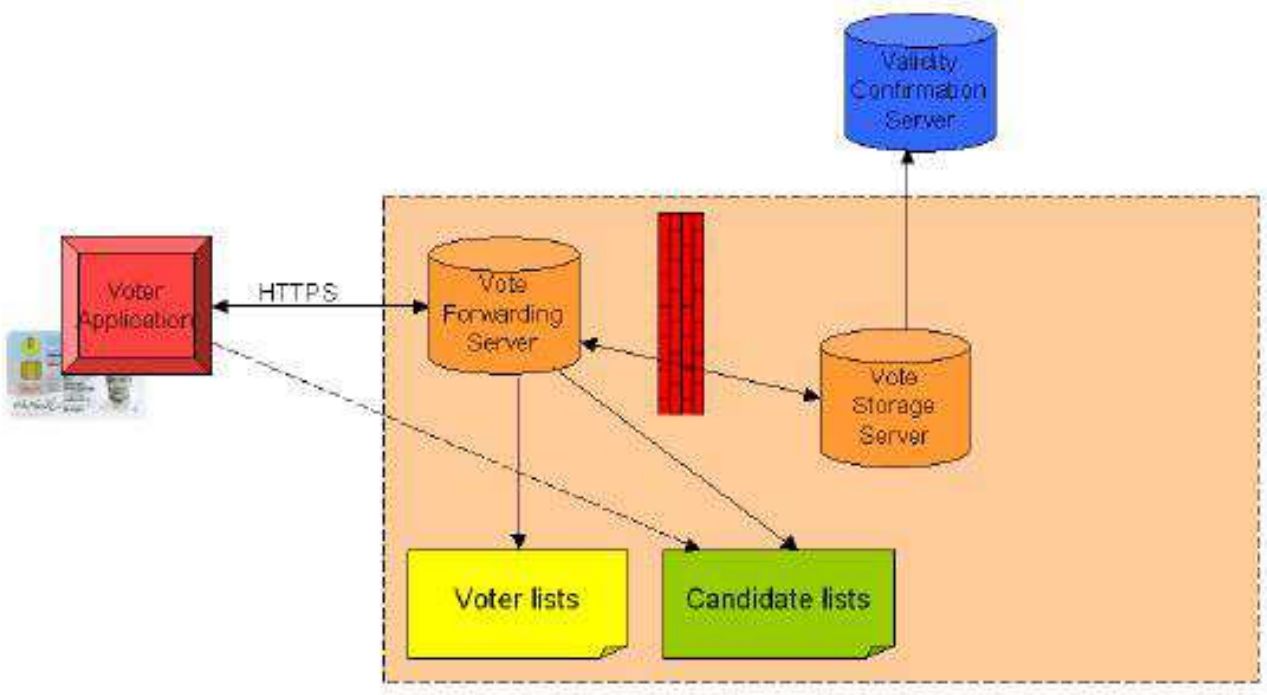
Zdroj: Estonian National Electoral Committee

Estónsky model



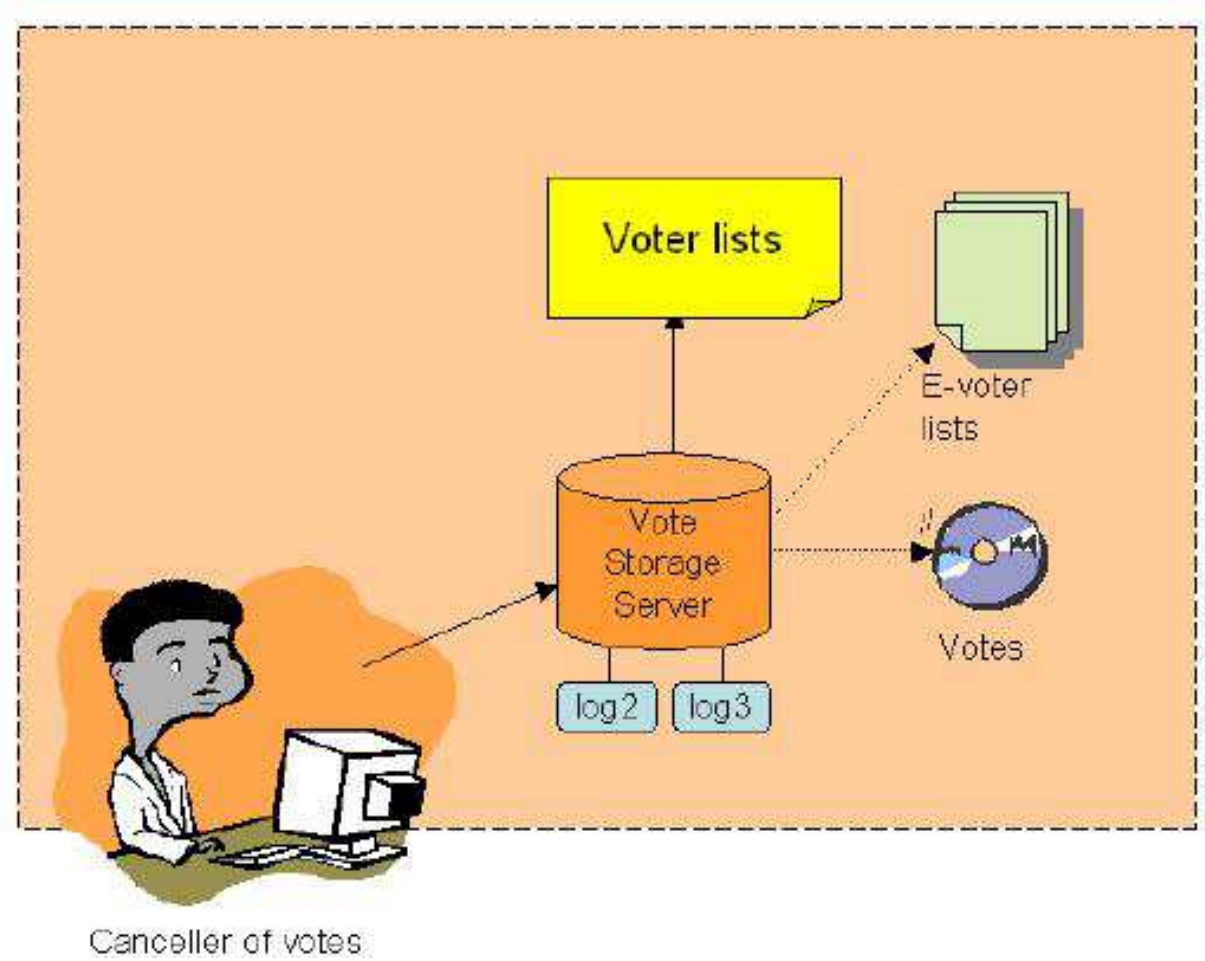
Zdroj: Estonian National Electoral Committee

Estónsky model: Hlasovanie a ukladanie hlasov



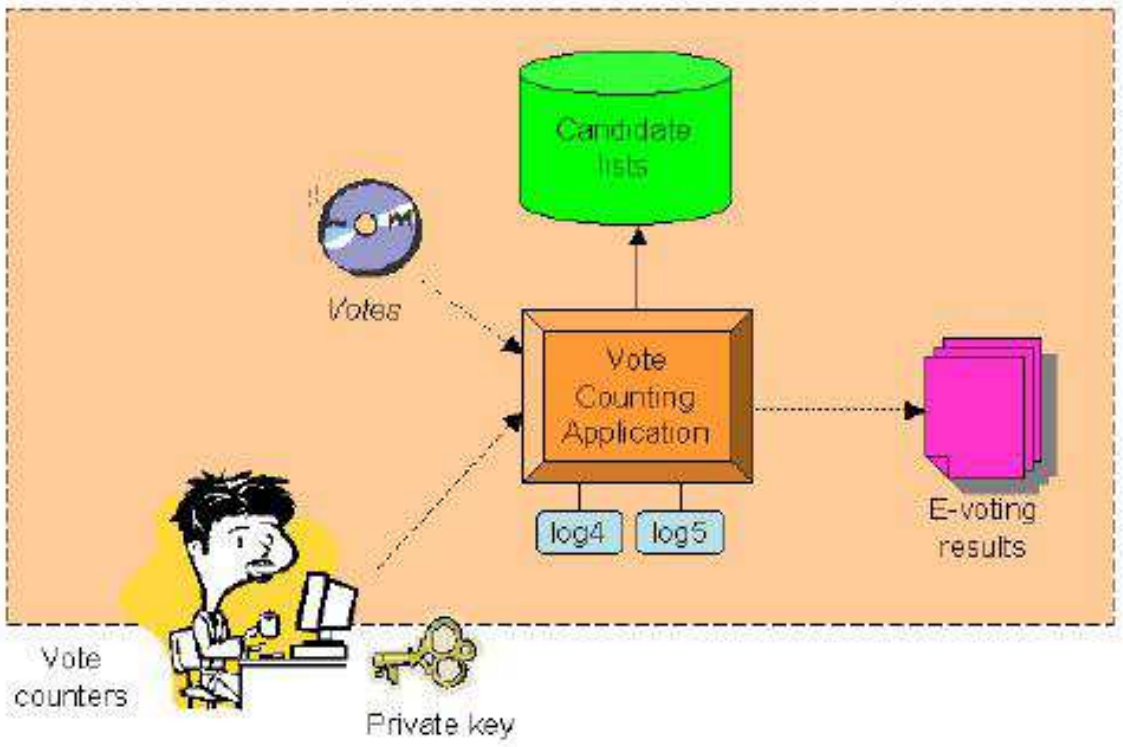
Zdroj: Estonian National Electoral Committee

Estónsky model: Triedenie hlasov



Zdroj: Estonian National Electoral Committee

Estónsky model: Sčítavanie hlasov



Zdroj: Estonian National Electoral Committee

Estónsky incident

- parlamentné voľby 2011
- študent vyvinul malware, ktorý zneužíval slabinu hlasovacej aplikácie a skryte blokoval "nepohodlné" hlasy

- Najvyšší súd voľby neanuloval
  - malware bol testovaný len s vedomím hlasujúcich
- praktická realizácie by bola obtiažna
  - vždy nová volebná aplikácia
  - príliš krátky čas na vytvorenie exploitu a rozšíenie vírusu

Zdroj: Estonian Public Broadcasting

Zhrnutie optimistu

- estónsky príklad ukazuje, že sa to dá
- dostupnosť technológii sa zvyšuje
- naše porozumenie celému procesu sa zlepšuje
- máme dostatok solídnych a overených stavebných kameňov (krypto), stačí ich správne poskladať a nezabudnúť pri tom na detaily

Zhrnutie pesimistu

Computer Technologists' Statement on Internet Voting

- verejné vyhlásenie 31 amerických odborníkov v oblasti, september 2008
- varujú pred pilotnými štúdiami, ktorých neúspech by mohol otriasť dôverou verejnosti
- poukazujú na nedoriešené technické aspekty

"Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting."

Zdroj: Verified Voting Foundation

Zhrnutie realistu... ?