IV064 Informační společnost

e-volby, e-hlasování

Jiří Zlatuška

8. října 2012

Politická účast

- Různé interpretace dopadu ITC na účast občanů

- Mobilizace – síť vytváří a podporuje nové formy aktivismu
- Posílení – síť zesílí, ale nikoli radikálně transformuje existující formy

Mobilizační teorie

- Zcela nové formy aktivit v digitálním prostředí (Negroponte, Dertouzos)
- Úloha virtuálních komunit (Schwartz)
- Elektronické diskuse jako demokratizující technologie stimulující výměnu idejí, mobilizaci veřejnosti a posílení sociálního kapitálu (Rheingold)
- Zmenšení vzdálenosti mezi vládnoucími a občany (Grossman)
- Přímá demokracie pomocí WWW
- Internetový aktivismus se silně liší od klasických forem politické podpory
- Nové formy vertikální i horizontální komunikace podporující a obohacující veřejné aktivity

Posilující teorie

- Internet zesílí a rozšíří mezeru mezi majetnými a nemajetnými
- Nové zdroje informací pro ty, kdo se zajímají, ale nestejná úroveň přístupu k ICT rozšíří rozdíly v zapojení (Owen, Davis)
- Sociálně-ekonomické rozdíly z běžného politického prostředí při užívání Internetu nezmizí, i když se budou možnosti připojení rozšiřovat (Murdock, Golding)
- Nové médium může rozšířit propast mezi informačně majetnými a informačně chudými
- Internetoví aktivisté vznikají z vlastního zájmu – Internet lidi nemění, jen jim dovoluje dělat stejné věci jiným způsobem (Hill, Hughes)
- „nové víno ve starých lahvích“

Politické kampaně a technologie

- 1924 – užití rozhlasu v prezidentské kampani, politická reklama a reklamy v kinech
- „nárazníkové řeči“ – kampaň ve vlaku a proslovy z vagonů (Eisenhower byl poslední, kdo tuto techniku použil)
- 1952 - televize
- 1960 – Nixon-Kennedy
- 1996 – Internet (Pat Buchanan, obě hlavní strany měly prezentace stranických sjezdů na Internetu, website dvojice Dole-Kemp)
- 1988 – Internet, televize, direct mail, telefoní kampaň, místní organizátoři kampaní
- 2000 – malí kandidáti získávali výraznou podporu přes Internet, nikoli však rozhodující pro výsledek

e-volby, e-hlasování

Z definice Rady Evropy:

- *e-volby* = politické volby nebo referendum, kde se elektronické prostředky užijí v jedné nebo více fázích
- *e-hlasování* = e-volby, ve kterých se elektronické prostředky užijí zejména pro vhození hlasu

Volby přes Internet - Arizona 2000

- Demokratické primárky formou e-voleb
- Účast o 600 procent vyšší

- Systém zkolaboval první hodinu voleb
- Někteří voliči ztratili svůj PIN
- Systém ne zcela kompatibilní s Macintoshi
- Necertifikovaný systém
- Obecný dojem: od hodnocení „chaos“ po pozitivní zprávy v médiích

Ministerstvo obrany 2000

- Úspěšně hodnocený pokus v celostátních volbách

SERVE – plán na obecné volby přes Internet v USA

- V roce 2000 problém s přepočtem hlasů oživil úvahy o elektronickém hlasování
- Invaze v Iráku před volbami v roce 2004 znamenala víc než 100 tisíc voličů momi území
- Americký Kongres uložil Ministerstvu obrany vyvinout internetové hlasování (Secure Electronic Registration and Voting Experiment)
- Očekávalo se přes 200 tisíc hlasujících prostřednictvím Internetu
- Projekt navzdory slibným pilotům zrušen

Michigan 2004 – Demokratické primárky

- Primárky konané 7. února s možností hlasovat předem poštou nebo přes Internet v době mezi 1. lednem a 16:00 7. ledna
- Největší experiment tohoto druhu v USA
- Chybí zhodnocení procesů a procedur ve vztahu k výsledku
- Volební účast stoupla z 19 tis. v roce 2000 na 163 tis. v 2004

Volba přes Internet	45 543	28,6 %
poštou	23 482	14,4 %
osobně	92 904	57,0 %
celkem	162 929	

Michigan 2004 – frekvence hlasování přes Internet

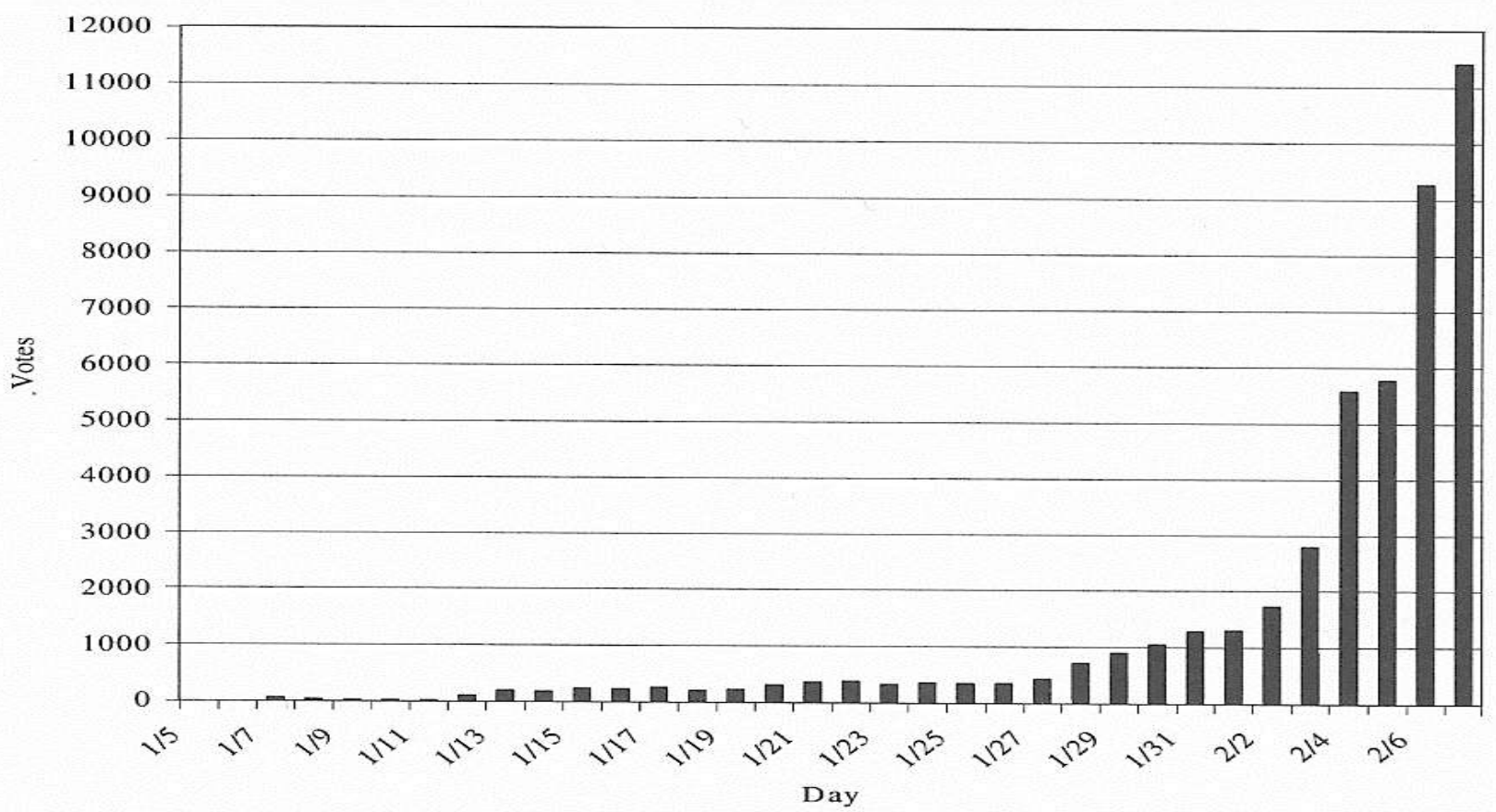


FIGURE 5.1 Michigan Caucus 2004 Internet Votes by Day

Zdroj: Alvarez-Hall: Electronic Elections, 1008

- Čtvrtina hlasů přišla poslední den,
- 70 procent během posledních čtyř dnů.

Časový průběh hlasování přes Internet odpovídá hlasování poštou

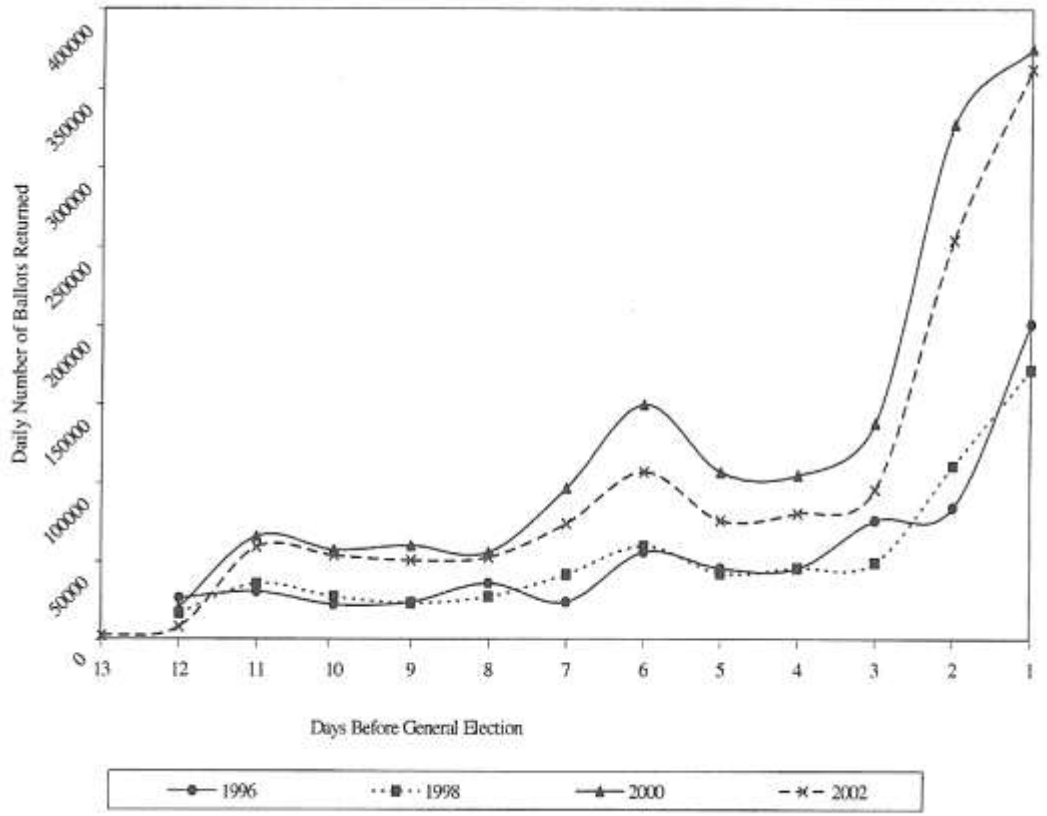


FIGURE 5.2 Daily Ballot Return Rates, Oregon General Elections, 1996–2002

- Srovnání detailních dat z poštovního hlasování v Oregonu odpovídá datům z Michiganského hlasování přes Internet (kde chybí data o příchodu hlasů poštou)

Zdroj: Alvarez-Hall: Electronic Elections, 1008

Kvalitativní zkušenost z Michiganských primárek

- Je známo, že z těch, kteří požádali o internetové hlasování, byl nevýznamně vyšší podíl mladších skutečně hlasujících (51,4 průměrný věk žadatelů, 48,5 těch, kteří skutečně volili)
- Výsledek voleb se nelišil podle způsobu hlasování
- Nedošlo k žádnému pokusu hacknout volby
- Voliči nevnímali Internet jako bezpečnostní riziko
- U vlastních voleb byla i mobilní hlasovací místa, která tvořila větší problém, než hlasování přes Internet

Bezpečnostní rizika elektronického hlasování

- Ztráta otevřenosti (chybí viditelnost získaných čísel)
- Ztráta možnosti lidí účastnit se procesu (a tedy si ověřit jeho přesnost v různých fázích)
- Ztráta rozložení odpovědnosti (vše závisí na činnosti jedné entity - stroje)
- Ztráta redundance a skutečné ověřitelnosti (pro ověření mohou chybět podklady)
- Ztráta veřejné kontroly (exkluzivní závislost na konkrétních článcích procesu)

Caltech/MIT Voting Technology Project, 2001

Teoretické argumenty proti

- Hlasovací stroj je „černá skříňka,“ do jejíž činnosti veřejnost nevidí a která sama exkluzivně dává zpětnou vazbu voliči. Funkce není nezávisle ověřitelná.
- Sebelepší prohlídka kódu nemusí odhalit vědomně nebo nevědomně chybný software. Neexistuje spolehlivé testování všech možných konfigurací.
- Softwarové systémy mohou úspěšně napadnout hackeři.
- U dodavatelů elektronických hlasovacích systémů mohou pracovat lidé s vlastními politickými zájmy a software může tyto preference zohledňovat.
- Případy chybné práce elektronických hlasovacích strojů se v praxi skutečně vyskytly

Systém Diebold – rok 2003

- Dotyková obrazovka pro elektronické hlasování z produkce firmy Diebold
- Zdrojový kód z roku 2002 získán přes Internet z nezabezpečeného zdroje FTP
- Analýza (Johns Hopkins & Rice University) ukázala jedenáct možných útoků proti systému
- Šest z jedenácti útoků mohlo proběhnout během přenosu dat přes Internet
- Chyběla kvalitní kryptografie i identifikace hlasujících
- Závěr: „Tento hlasovací systém je nevhodný pro použití ve volbách. Jakýkoli podobný systém bez použití papíru může trpět podobnými problémy bez ohledu na „certifikaci“, kterou může získat.
- Pozdější analýzy jiných pracovišť ukázala další problémy, včetně šíření virů mezi stroji.

Zrušení systému SERVE – únor 2004

- Plánem byl pilot pro cca 100 tisíc voličů mezi více než 100 miliony celkem
- Ze zprávy předcházející zrušení projektu: „*Skutečnou překážkou úspěchu není nedostatek vize, znalostí, prostředků nebo odhodlání; je jí fakt, že za současného stavu Internetu a zabezpečení PC je v podstatě nemožné zabezpečit jakýkoli zcela elektronický systém s dálkovým přístupem. Bez radikální změny v celkové architektuře Internetu a PC nebo nějakého dosud neznámého průlomu v zabezpečení není možné spolehlivý systém pro volby vytvořit*.“

(D. Jefferson, A. Rubin, B. Simons, and D. Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). Technical report, US Department of Defense, 2004. http://www.servesecurityreport.org/)

Bezpečnostní rizika systému SERVE

Threat	Skill needed	Consequences	Realistic?	Countermeasures
denial of service attack (various kinds)	low	disenfranchisement (possibly selective disenfranchisement)	common on the Internet	no simple tools; requires hours of work by network engineers; launchable from anywhere in the world
Trojan horse attack on PC to prevent voting	low	disenfranchisement	There are a million ways to make a complex transaction such as voting fail.	can mitigate risk with careful control of PC software; reason for failure may never be diagnosed
on-screen electioneering	low	voter annoyance, frustration, distraction, improper influence	trivial with today's web	nothing voter can do to prevent it; requires new law
spoofing of SERVE (various kinds)	low	vote theft, privacy compromise, disenfranchised voters	Web spoofing is common and relatively easy	none exist; likely to go undetected; launchable by anyone in the world
client tampering	low	disenfranchisement	one example: change permissions on cookie file. Many other trivial examples	none exist for all possible mechanisms. Too difficult to anticipate all attacks; likely never diagnosed.
insider attack on system servers	medium	complete compromise of election	Insider attacks are the most common, dangerous, and difficult to detect of all security violations	none within SERVE architecture; voter verified ballots needed, e.g. Appendix C; likely undetected
automated vote buying/selling	medium	disruption of democracy	very realistic, since voter willingly participates	none exist; buyers may be out of reach of U.S. law
coercion	medium	disruption of democracy	harder to deploy than vote buying/selling, but man in the middle attacks make it achievable with average skill	none exist; likely to go undetected.
SERVE-specific virus	medium or high	vote theft, privacy compromise, disenfranchised voters	Some attacks require only experimentation with SERVE; others require leak of SERVE specs or code and resourceful attacker	virus checking software can catch known viruses, but not new ones; likely to go undetected
Trojan horse attack on PC to change votes or spy on them	high	vote theft, privacy compromise	widely available spyware would be a good starting point	can mitigate risk with careful control of PC software; harder to control at cybercafe, or other institutionally managed networks; attack likely to go undetected

Problémy stávajících elektronických hlasování (Kalifornie a Ohio)

- *Špatná integrace ohrožuje bezpečnost*. Systém složený z částí od různých dodavatelů nemá ani společný návrh ani koherentní strukturu. Užívají se různé jazyku, vlastní datové struktury, celková analýza systému a toku dat se stává prakticky nemožnou.
- Použití části kódu z jiného systému musí být spojeno s analýzou celého systému.

Problémy elektronických hlasování 2

- *Kryptografie se těžko používá správně*. Užití kryptografie je často jen naivní, špatné nebo žádné. Existují systémy se správným užitím silné kryptografie, nicméně si ukládají klíč do vlastních datových struktur. Často chybí zakódování všech dat z průběhu volby.
- Promyšlené užití kryptografických technik je podmínkou, zabezpečeny musí být i klíče.

Problémy elektronických hlasování 3

- *Neopodstatněné předpoklady o důvěryhodnosti dat ohrožují bezpečnost*. Prakticky užívané systémy vesměs činí předpoklady o důvěryhodnosti některých zdrojů dat, například se užijí jen kontrolní součty, nikoli elektronický podpis. Data od různých komponent systému často nejsou testována na hraniční situace.
- Bezpečný hlasovací systém nesmí nikde činist předpoklady o důvěryhodnosti dat bez vyčerpávající kontroly všech vstupů.

Problémy elektronických hlasování 4

- *Současné certifikace a standardy nestačí*. Dnes užívané standardy nejsou dostatečně orientovány na bezpečnost, resp. nestačí jen výčtová kontrola splnění jejich požadavků.Konkrétní případy se týkají přetečení vyrovnávacích pamětí – standard sice předepíše kontrolu před každým zápisem, nezaručí však korektnost této kontroly.
- Hlasovací systémy vyžadují důkladnější bezpečnostní analýzu, než je v současné době standardně dělaná.

Problémy elektronických hlasování 5

- *Vestavěné testování dává klamný pocit bezpečnosti*. Testování správnosti se opírá o testovací mód systému, který však nelze použít během faktické činnosti. Tím že systém ví o tom, že jede v testovacím módu, se kód, který ho napadl, může účelově deaktivovat.
- Testování logiky činnosti i přesnosti musí vyloučit, že by software nebo firmware měl dostupnou informaci o tom, že systém funguje v testovacím módu.

Problémy elektronických hlasování 6

- *Hlasovací procedury podceňují vynalézavost protivníků*. Bezpečnost často závisí na konkrétní proceduře užití systému. Fyzické zabezpečení je však často možné překonat. Dodavatelé často nechápou, že zabudovaná vnitřní bezpečnost je spolehlivější, než předpoklady o způsobu použití.
- Procedury nebo konkrétní způsob užití nemohou být nikdy složkou bezpečnosti systému. Každá komponenta systému musí mít vlastní zabezpečení nezávislé na způsobu užití.

Zdroj: Analýza hlasovacích zařízení v Kalifornii a Ohiu,
Balzarotti et al.: Are Your Votes Really Counted? Testing the Security of Real-world Electronic Voting Systems, 2008

Evropa – pilotní studie i praktické užití

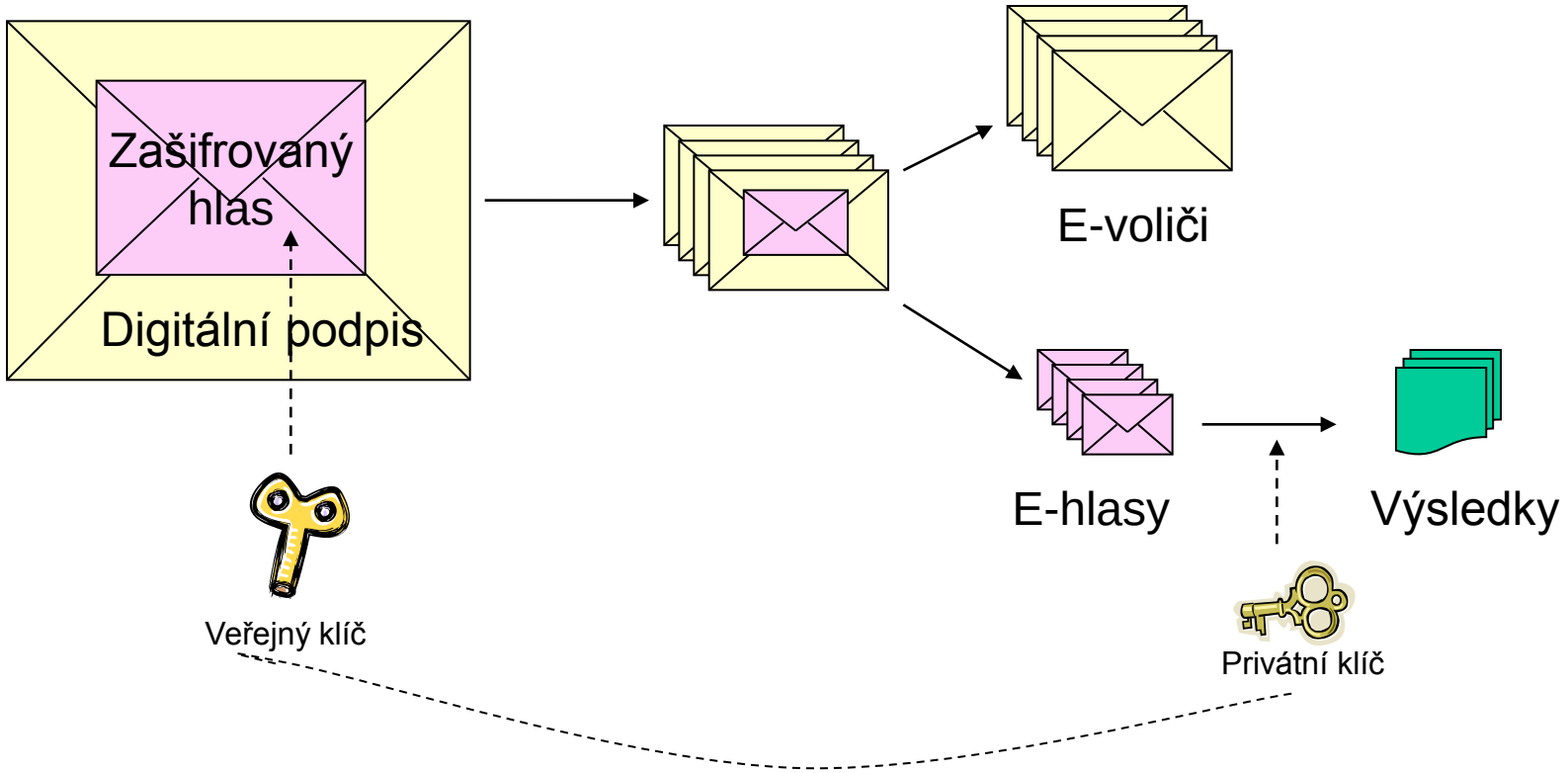
- V roce 2006 proběhlo skutečné hlasování pomocí internetu v osmi evropských státech
- Velká Británie – manipulace s papírovými lístky vedla k narušení důvěryhodnosti, odtud zájem o elektronické hlasování
- Francie, Švýcarsko, Holandsko – místní hlasování nebo hlasování pro voliče v zahraničí

Estonsko – první internetové volby na národní úrovni v březnu 2007

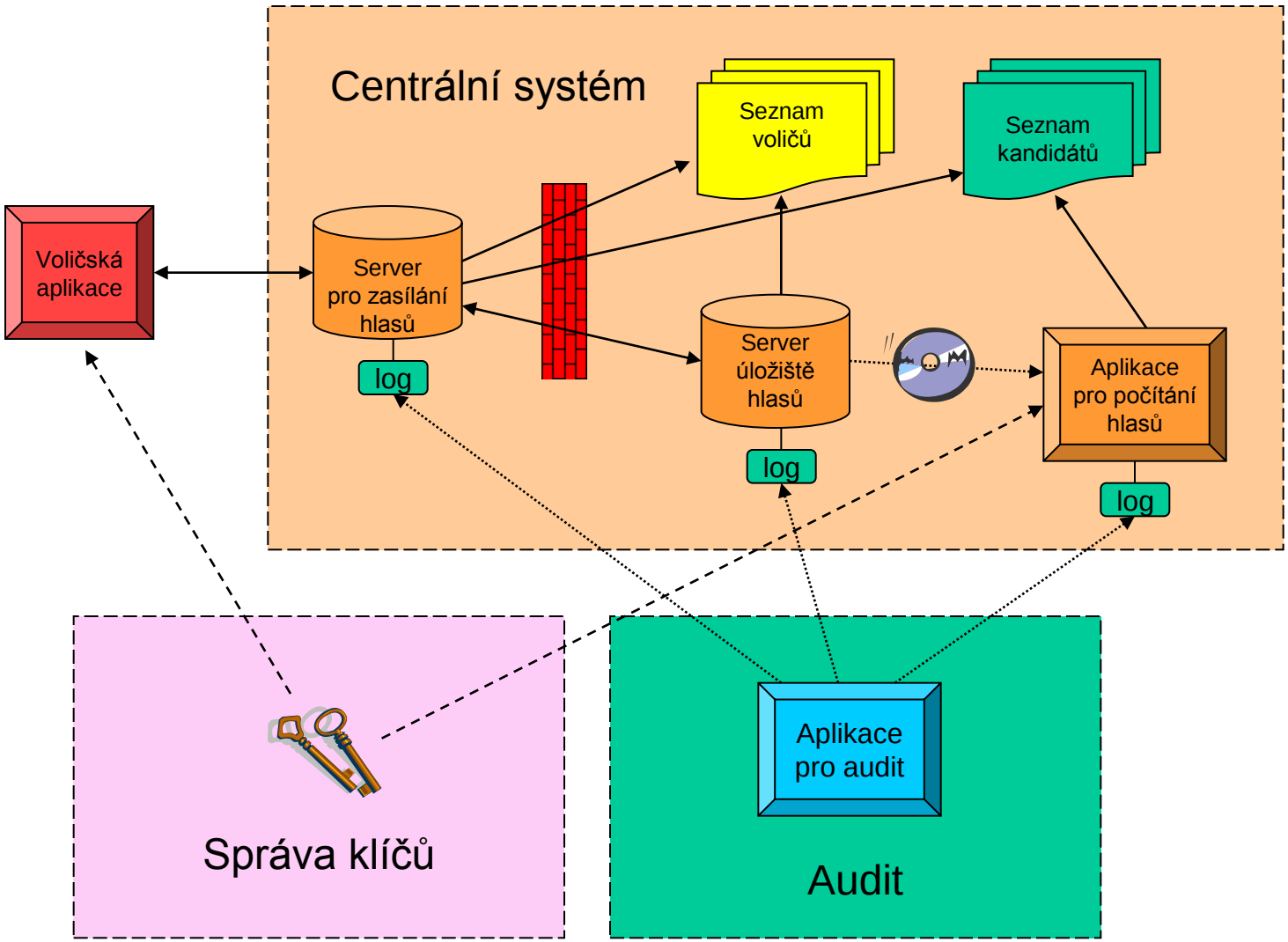
- Občané mají povinnou obecně užívanou elektronickou identifikaci nahrazující různé průkazy a sloužící i pro elektronický podpis

- Volbu přes Internet je možné měnit, platí poslední verze (v roce 2007 bylo takto zneplatněno 32 hlasů)
- Papírový hlas osobně odevzdaný má přednost před hlasem daným přes Internet
- 940 tisíc oprávněných voličů, 30 tisíc z nich hlasovalo elektronicky, 170 tisíc hlasovalo tradičním způsobem vhozením lístku do urny (5,4 % hlasovalo přes Internet)

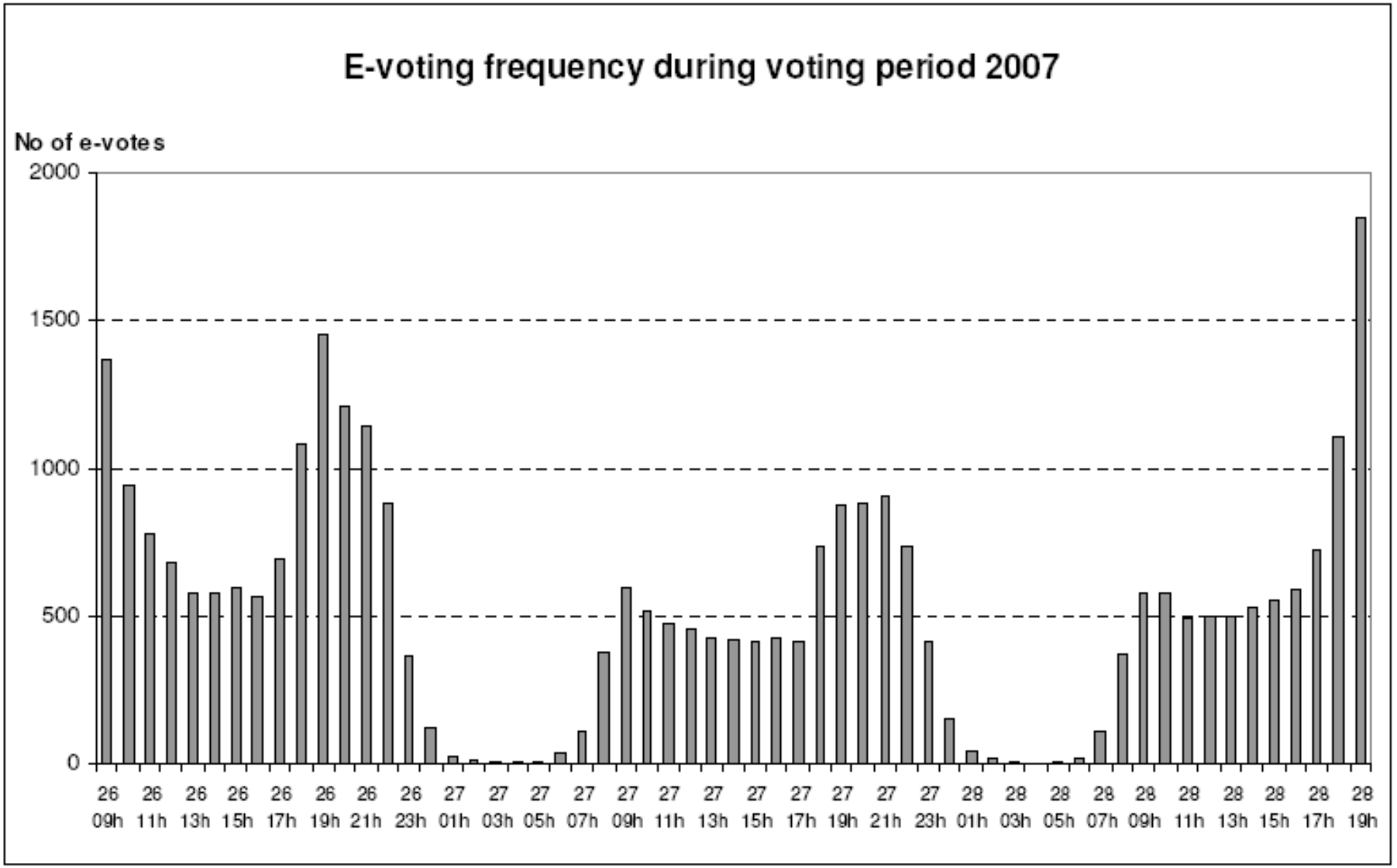
Estonsko – princip hlasovacích obálek



Estonsko – architektura I-voleb

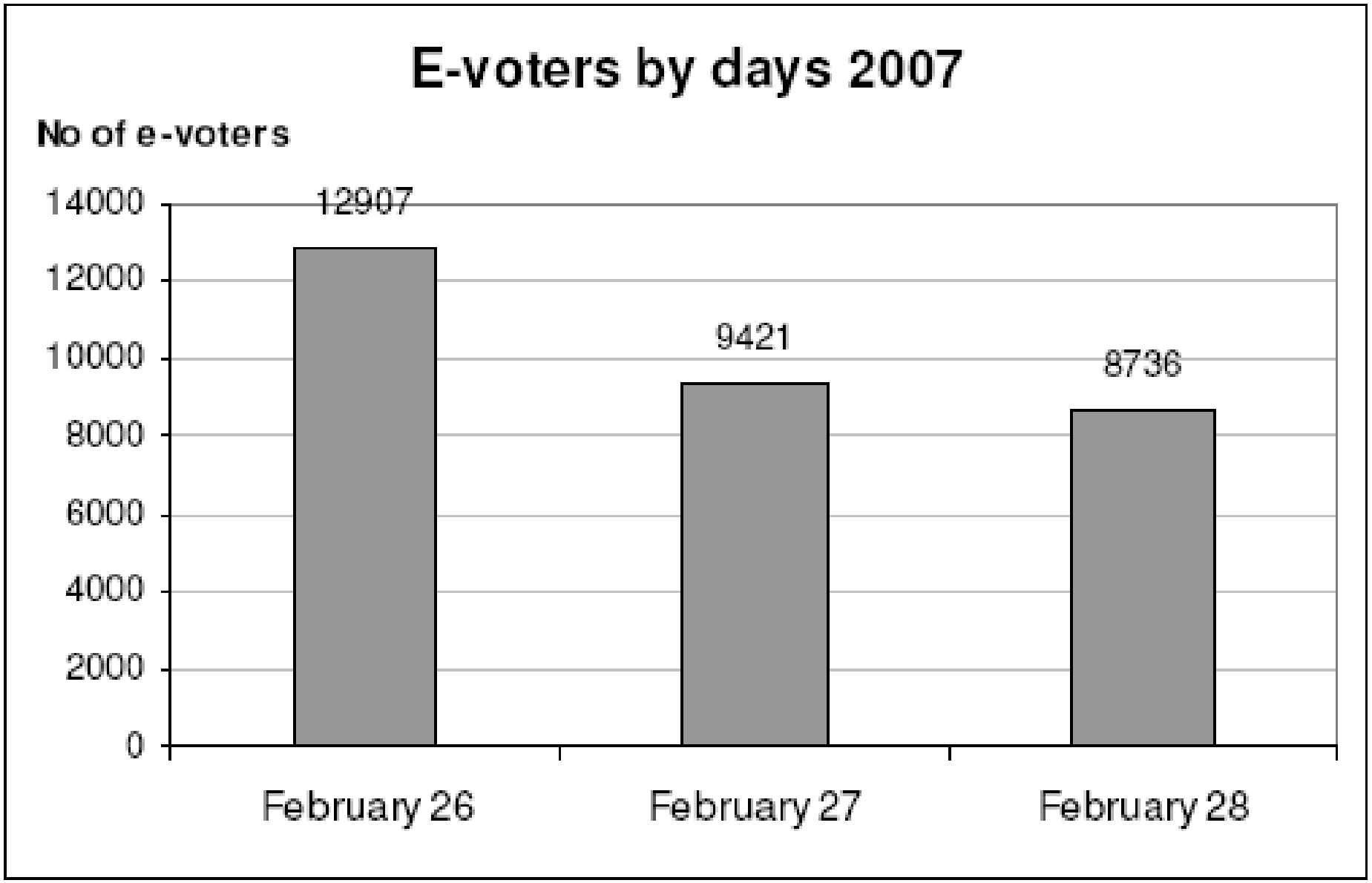


Estonsko – průběh elektronického hlasování



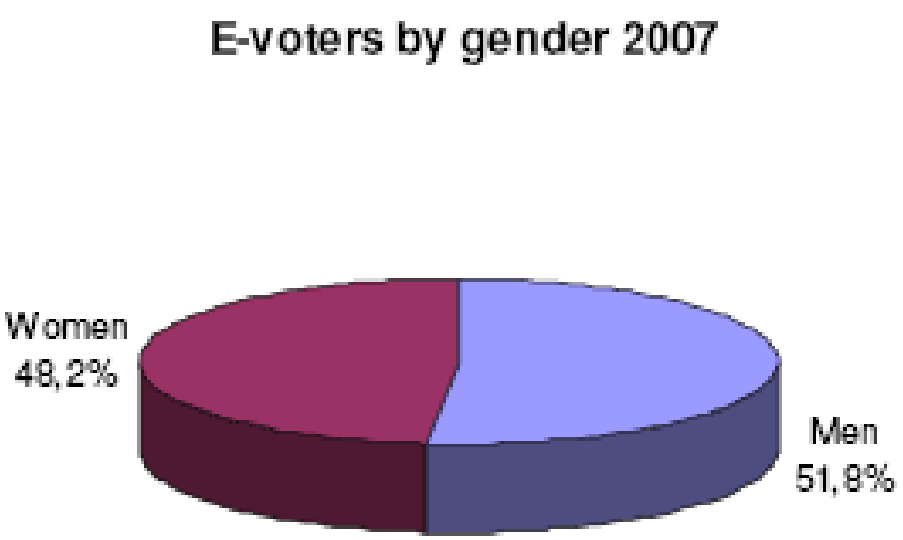
Zdroj: http://www.vvk.ee/english/Ivoting%20comparison%202005_2007.pdf

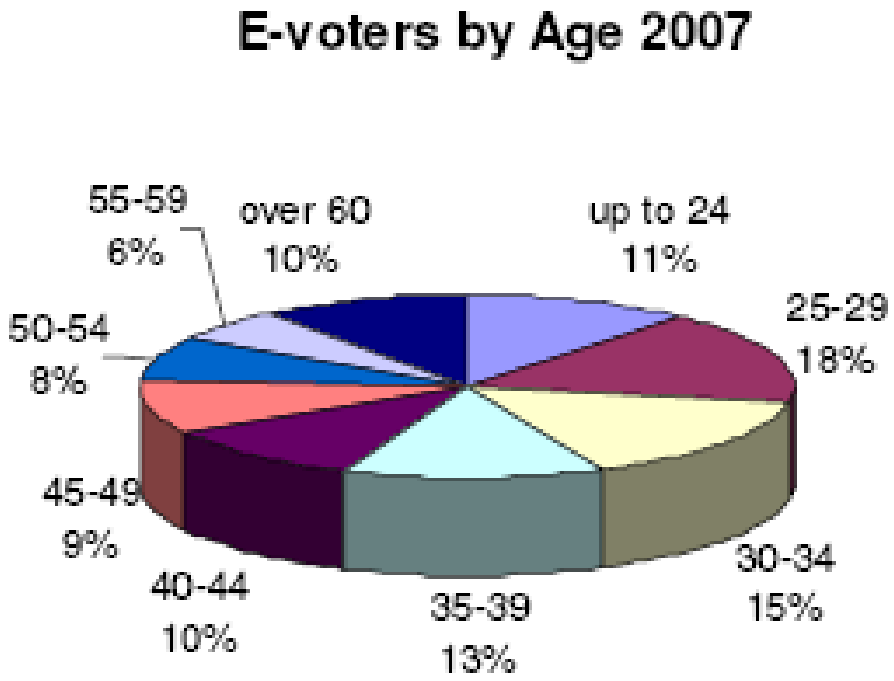
Estonsko – průběh elektronického hlasování



Zdroj: http://www.vvk.ee/english/Ivoting%20comparison%202005_2007.pdf

Estonsko – pohlaví a věk elektronicky hlasujících





Zdroj: http://www.vvk.ee/english/Ivoting%20comparison%202005_2007.pdf