

SEZNAM PŘÍLOH

Příloha č. 1: Jednotlivé sektory v demokratickém systému a jejich zóny protnutí před nástupem moderních komunikačních technologií dle Clifa (obrázek)

Příloha č. 2: Proměny demokratického systému po nástupu procesů e-democracy dle Clifa (obrázek)

Příloha č. 3: Remote Internet Voting (schéma)

Příloha č. 4: Poll site e-voting (schéma)

Příloha č. 5: Důvěra občanů v politické instituce v jednotlivých čtvrtletích mezi lety 1996 – 2006 (graf)

Příloha č. 6: Úroveň počítačových dovedností v ČR podle sociodemografických znaků sledované populace v roce 2006 (graf)

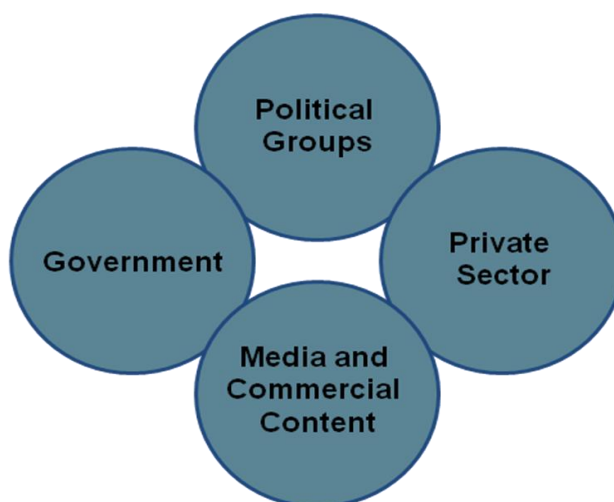
Příloha č. 7: Příklad alegorického příběhu městečka Demokratia Virtualis akcentujícího elektronizaci voleb od Jana H. Hanzka (text)

Příloha č. 8: Příklad technologického řešení elektronických voleb od Petra Šindeláře (text + schéma)

PŘÍLOHY

Příloha č. 1

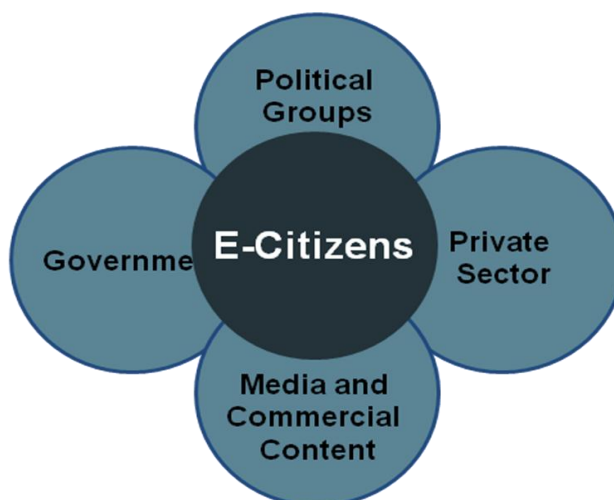
Jednotlivé sektory v demokratickém systému a jejich zóny protnutí před nástupem moderních komunikačních technologií dle Clifa



Zdroj: http://stevenclift.com/?page_id=5 (přístup: únor 2011).

Příloha č. 2

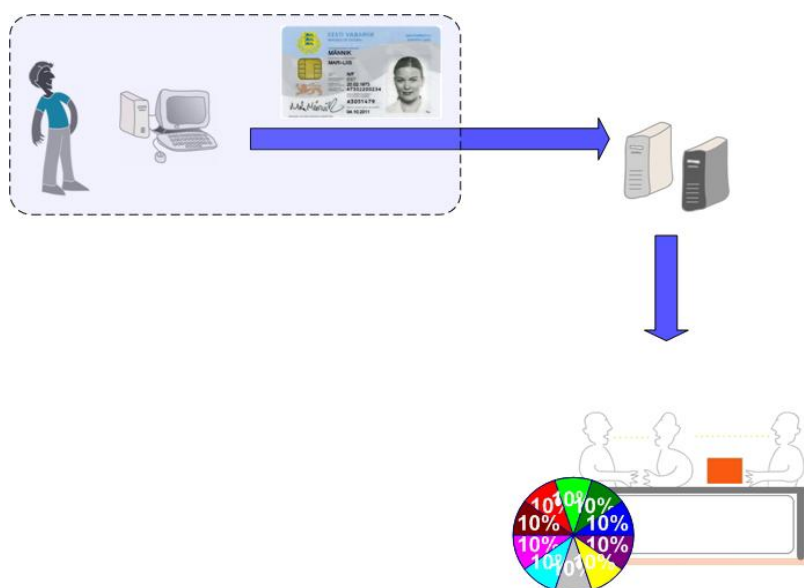
Proměny demokratického systému po nástupu procesů e-democracy dle Clifa



Zdroj: http://stevenclift.com/?page_id=5 (přístup: únor 2011).

Příloha č. 3

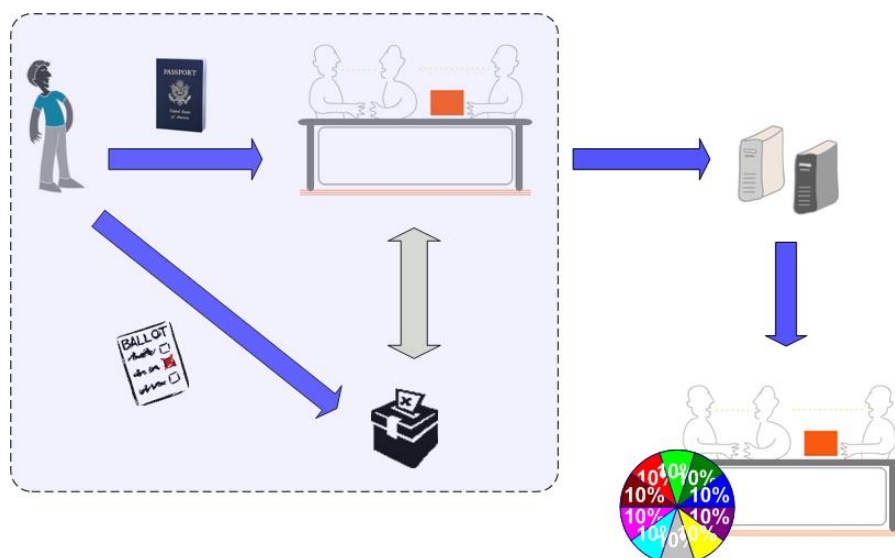
Remote Internet Voting



Zdroj: Šindelář, P. (2006): *Elektronické volby jako možný nástroj pro posílení demokracie*. Přístupné z WWW: <http://si.vse.cz/archive/proceedings/2006/elektronicke-volby-jako-mozny-nastroj-pro-posileni-demokracie.pdf> (přístup: březen 2011).

Příloha č. 4

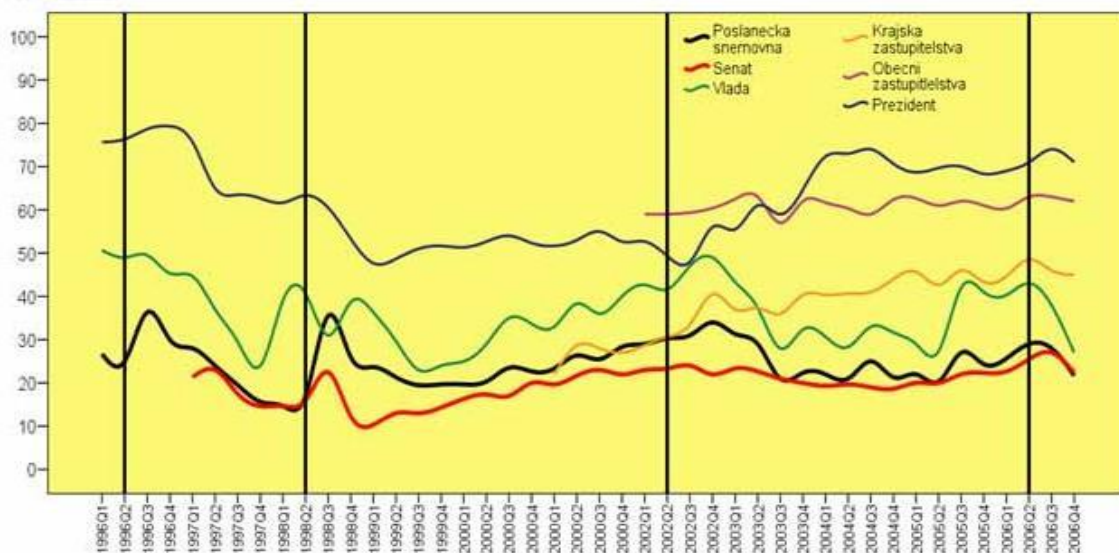
Poll site e-voting



Zdroj: Šindelář, P. (2006): *Elektronické volby jako možný nástroj pro posílení demokracie*. Dostupné z WWW: <http://si.vse.cz/archive/proceedings/2006/elektronicke-volby-jako-mozny-nastroj-pro-posileni-demokracie.pdf> (přístup: březen 2011).

Příloha č. 5

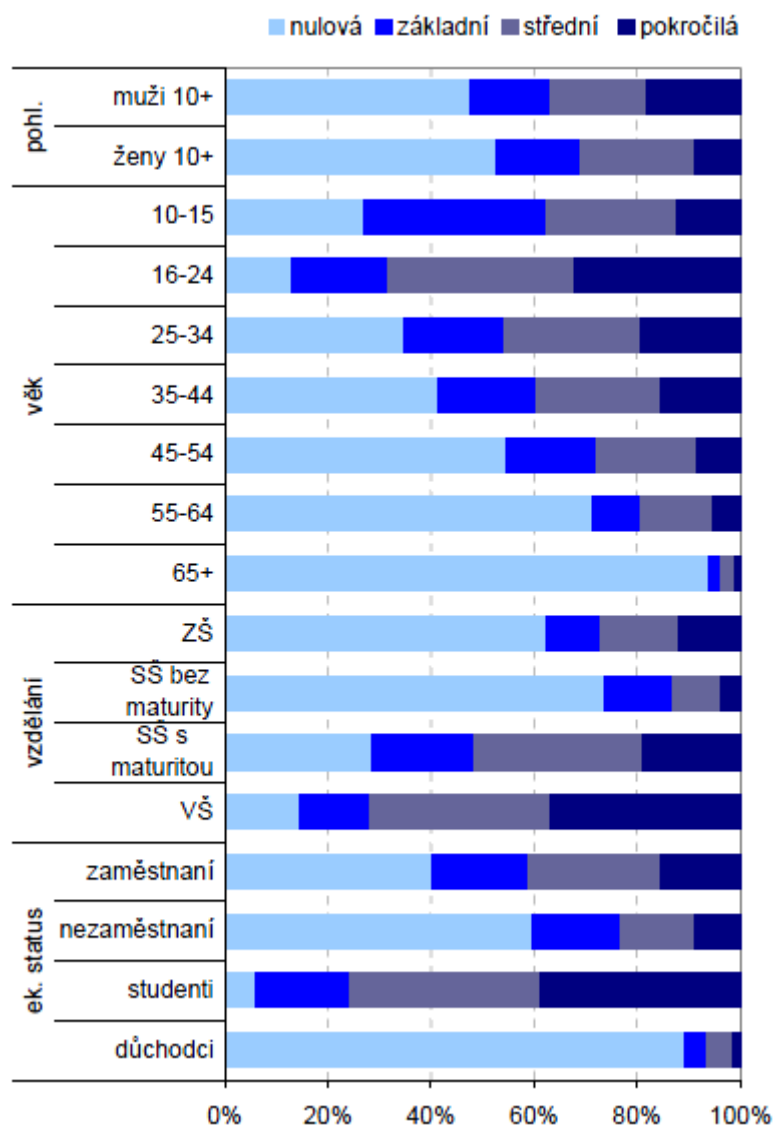
Důvěra občanů v politické instituce v jednotlivých čtvrtletích mezi lety 1996 – 2006



Zdroj: <http://www.socioweb.cz/index.php?disp=teorie&shw=359&lst=115> (přístup: duben 2011).

Příloha č. 6

Úroveň počítačových dovedností v ČR podle sociodemografických znaků sledované populace v roce 2006



Zdroj: http://www.czso.cz/csu/redakce.nsf/i/pocitacove_dovednosti_kapitola_7_jednotlivci (přístup: květen 2011).

Příloha č. 7

Příklad alegorického příběhu městečka Demokratia Virtualis akcentujícího elektronizaci voleb od Jana H. Hanzka¹⁵⁷

V tomto městečku od nepaměti vedla strmá ulička mezi domy od hřbitova na kopci k hlavnímu náměstí s kašnou. Touto uličkou každou neděli proudili místní obyvatelé nejdřív k hrobům svých předků a poté se šli všichni občerstvit ke kašně. Avšak s růstem města a zvýšením jeho populace došlo k tomu, že nedělních výletníků bylo více a více a stará ulička mezi domy již jejich náporu nestačila. Docházelo k mnoha strkanicím a zácpám, což lidi utvrdilo v přesvědčení, že situace je neúnosná a musí se nějakým způsobem řešit.

Rozšířit uličku a vybudovat širší schodiště by stálo neúměrně mnoho prostředků a proto bylo rozhodnuto o stavbě bulváru, který se na kopec přivede oklikou. Tento způsob byl v danou chvíli nejlepším a ideálním řešením. Cesta sice trvala déle a nutila lidi vstupovat do částí města, kam neměli původně vůbec namířeno, ale snadně zpřístupnila hřbitov a náměstí s kašnou velkému počtu obyvatel. Čas plynul dále a po nějaké době lidé zjistili, že jim cesta na hřbitov trvá déle, než si mohou dovolit a jejich políčka jsou pak zanedbaná. Proto si po čase každá rodina vybrala zástupce, který šel hroby na kopci upravit a přinesl čerstvé květiny. Tito zástupci každou neděli šplhali nahoru do kopce po bulváru a dostávali za to odměnu v podobě misky fazolí. Brzo se však v městečku rozkřiklo, že část rodinných zástupců na hřbitov vůbec nechodí, další si zkracují cestu skrz starou uličku, i když jsou odměňováni za delší cestu po bulváru. Lidé si proto vybírali jiné a jiné zástupce, kteří jim slibovali, že oni jsou ti nejlepší a oni opravdu každou neděli za misku fazolí na hřbitov dojdou a hroby dají do pořádku. I přes sliby však hřbitov na kopci chátral a chátral. Tu a tam se lidé rozzlobili, vzali vše potřebné a vyrazili směrem na kopec starou uličkou sami za sebe. Ale když takovýchto lidí bylo více, zase se všichni mačkali ve staré uličce jako před stavbou bulváru. Proto se dlouho nic neměnilo. Ze zástupců rodin se stala nová kasta, která se „vznešeně“ starala o odkaz předků (rozuměj hřbitov) za (jejich slovy) pár fazolí týdně a tato práce se stala vyhledávanou a prestižní. Co naplat, hřbitovy stejně chátraly, jen lidé již rezignovali na vzbouření a platili své zástupce s vědomím, že oni tam nejspíše nedojdou, ale to že

¹⁵⁷ <http://hippiecharlesmanson.blog.cz/1104/pohadka-demokratia-virtualis> (přístup: květen 2011).

by mohli jednou dojít je lepší, než kdyby nikomu nezaplatili a hřbitov chátral jejich vinou. Takto to plynulo mnoho a mnoho let a lidé už skoro zapomněli na doby, kdy na hřbitov chodili všichni starou příkrou uličkou.

Avšak jednoho dne přišel do městečka Inženýr, který tvrdil, že problém dokáže vyřešit jednou pro vždy pomocí parního stroje. Lidé se mu nejprve smáli. „Kdo to kdy slyšel, parní stroj obhospodařovat hřbitov?!“ Inženýra to stálo hodně úsilí, aby překřičel jednak chronické nevěřící Tomáše a jednak silnou fazolovo-zástupcovou lobby. Díky knihám, které přivez sebou, mohl lidem ukázat své smělé řešení – za peníze všech postaví vysokorychlostní lanovku poháněnou parním strojem v místech, kde se dnes nachází stará a strmá ulička, která dokáže rychle a bezpečně přepravit všechny lidi na kopec. Postupným zkoumáním lidé zjistili, že drahý projekt lanovky bude stát za začátku hodně peněz – protože budou muset platit jak stavbu lanovky, tak své zástupce, kteří chodí na kopec, ale po uvedení do chodu se jim každou neděli investice bude pomalu vracet, jelikož provoz lanovky bude mnohem levnější a efektivnější, než platit své zástupce, kteří stejně nic pořádného nedělají. A tak se stalo.

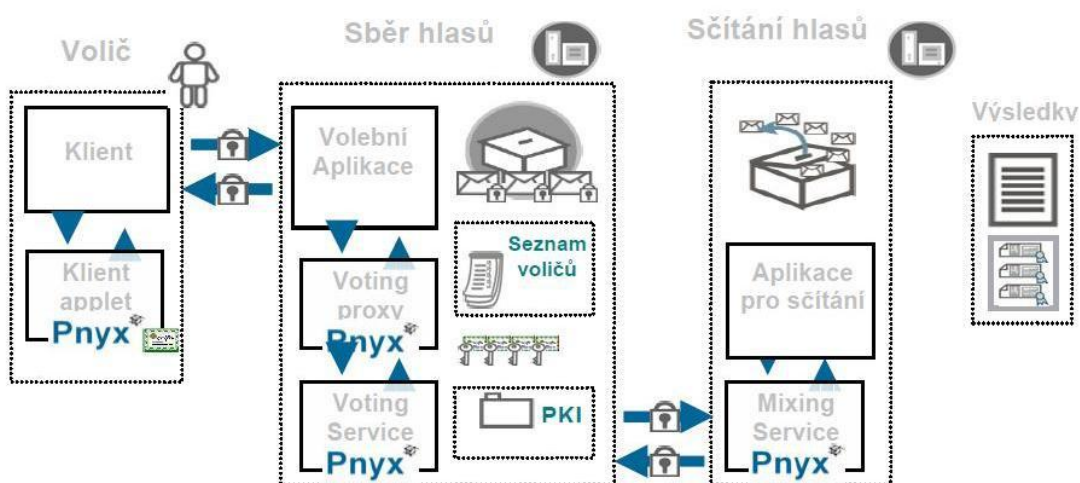
Lanovka byla postavena a lidé se mohli (díky vlastnostem vysokorychlostní a mnohasedačkové lanovky) zase vydávat na kopec zase v celých rodinách bez toho, že by jim schla jejich těžce obhospodařovaná políčka. Z Inženýra, kterému se všichni nejdříve smáli, se stal místní hrdina a zástupci přišli o práci. Naštěstí se nenaplnila jejich černá proroctví o velkých haváriích lanovky (ty byly později připsány jejich zhrzenému egu a obavám ze ztráty zaměstnání) a nakonec všichni našli práci novou – jako obsluha a technická podpora lanovky. Ve městě zase všichni mohli jezdit v neděli na kopec za svými předky a pak se jet osvěžit do kašny na náměstí i přes početnou populaci. Dnes jsou obyvatelé hrdí na svoji lanovku a smějí se svým předkům, kteří ve své rezignaci platili zástupcům za nic a ještě jim za to děkovali.

Příloha č. 8

Příklad technologického řešení elektronických voleb od Petra Šindeláře (cit.)¹⁵⁸

Společnost Hewlett-Packard strategicky spolupracuje v oblasti e-volebních řešení se společností Scytll. Obě společnosti společně realizovali řadu projektů/pilotních projektů jak v Evropě, Americe i Asii/Tichomoří. Pro popis konkrétního příkladu technického konceptu řešení jsem tedy zvolil produkt Scytll PNYX.Government. Stejný produkt byl použit pro volby v Madridu, které jsou popisovány v poslední části tohoto příspěvku.

Základní architektura i-volebního systému PNYX je zobrazena na následujícím obrázku.



Celý systém se skládá ze tří hlavních bloků:

1. Blok uživatelský
2. Blok sběru hlasů
3. Blok sčítání hlasů a publikace výsledků

¹⁵⁸ Šindelář, P. (2006): *Elektronické volby jako možný nástroj pro posílení demokracie*. Dostupné z WWW: <http://si.vse.cz/archive/proceedings/2006/elektronicke-volby-jako-mozny-nastroj-pro-posileni-demokracie.pdf> (přístup: květen 2011).

Jádro systému PNYX.Government (Pnyx.core) vytváří šifrováním na aplikační úrovni virtuální vztah mezi voličem a volební komisí. Tento přístup eliminuje nutnost důvěry ke komplexní technologické infrastruktuře celého řešení včetně technického personálu, který ji provozně obsluhuje. Kryptografická metoda je založena na infrastruktuře veřejných klíčů. Celková architektura je kombinací bezpečnostně auditovatelných hardwarových a softwarových komponent, zajištění fyzické a logické bezpečnosti a kryptografického volebního protokolu. Základní procesní postup podporovanou touto architekturou a patentovaným kryptografickým protokolem je následující:

1. Ustavení volební komise. Vytvoření páru PKI klíčů pro potřeby voleb. Každý člen komise obdrží dle tajného postupu část privátního PKI klíče, který slouží k otevření elektronické volební urny. Přítomnost minimálně určitého počtu členů komise je dohodnuta a vyžadována pro rekonstrukci celého klíče. Privátní klíč je zničen.
2. Zahájení voleb. Když se volič připojí k i-volebnímu systému, elektronicky podepsaný Java applet je dynamicky stažen na příslušné zařízení a je tak vytvořeno bezpečné prostředí pro vlastní volbu.
3. Volič je autentikován (dle registrace) a obdrží personalizovaný elektronický volební lístek s příslušnými možnostmi volby. Volič provede svoji volbu.
4. Volič obdrží elektronicky podepsané potvrzení o své volbě, které obsahuje náhodně generovaný unikátní identifikátor volby.
5. Ve volebním systému je hlasovací lístek společně s unikátním identifikátorem zapečetěn v elektronické obálce vytvoření zaručeným veřejným klíčem voleb. V tomto bodě je možno provádět dodatečné kontroly platnosti hlasu, v případě užití více kanálů neboť zde existuje vazba mezi identitou voliče a obálkou s jeho hlasem.

6. Důkaz autentičnosti hlasu je vytvořen na základě privátního klíče voliče a je připojen k elektronické obálce. Elektronická obálka je uložena v elektronické volební urně.
7. Na konci období voleb, kdy elektronická volení urna obsahuje všechny zapečetěné elektronické obálky, fyzicky přesunuta do systému pro sčítání hlasů.
8. Členové volební komise předloží své části privátního klíče.
9. Speciální kryptografické spojovací schéma je užito k rekonstrukci privátního klíče, jsou otevřeny zapečetěné digitální obálky a oddělena vlastní obálka (identifikátor voliče) a její obsah (vlastní hodnota hlasu). V tomto kroku je také možno provést kontrolu platnosti hlasů (odstranění možných duplicit mezi seznamem voličů mezi papírovou formou a i-formou).
10. Na separátních seznamech jsou publikovány výsledky a unikátní identifikátory hlasů.
11. Probíhá audit sečtení hlasů a výsledků voleb. Vedle toho mohou voliči ověřit na základě srovnání obdrženého identifikátoru hlasu a publikovaného seznamu, že jejich hlas byl ve finálním součtu zohledněn.