

# Volební systém Svobodných

## I. Organizační a technické zajištění voleb

### 1. Kdo zajišťuje volby u Svobodných?

Volby zajišťuje přímo volená volební komise. Její členy volí všichni členové strany, stejně jako funkcionáře dalších republikových orgánů (tj. předsedu, místopředsedy ad.). Volební komise má až sedm členů. V současné době je plně obsazená (má sedm členů). [Stanovy Svobodných](#)

### 2. Kdo provozuje volební systém a server, na kterém běží?

Provozuje ho volební komise na virtuálním serveru u poskytovatele Wedos (na straně zcela nezávislá soukromá firma).

Virtuální server objednala a platí strana (prostřednictvím svého vedení, které za ni dle Stanov jedná navenek). Vedení strany nemá žádný přístup na tento server, veškeré přístupy má k dispozici pouze volební komise.

### 3. Kdo zajišťuje program pro volební systém?

Volební systém si kompletně zajišťuje (programuje i provozuje) volební komise. Jeho zdrojové kódy jsou veřejně dostupné prostřednictvím služby GitHub na adrese [https://github.com/svobodni/ballot\\_box/](https://github.com/svobodni/ballot_box/)

GitHub je webová služba podporující vývoj softwaru při používání verzovacího nástroje Git. GitHub nabízí bezplatný hosting pro open-source projekty (tzv. otevřený software je

počítačový software s otevřeným zdrojovým kódem. Otevřenost zde znamená jak technickou dostupnost kódu, tak legální dostupnost). Po zaplacení měsíčního poplatku je možné ukládat soukromé repositáře. Projekt byl spuštěn v roce 2008.

#### **4. Kdo vidí identitu přihlášených?**

Identitu přihlášených uživatelů zná Registr i volební systém. Registr neví, kdy/kdo volí (tj. neví, zda se tam ten člověk šel jen podívat, nebo zda i volil a koho – jen sděluje volebnímu systému identitu přihlášeného uživatele).

Registr provozuje správce, kterého jmenuje vedení strany (správce není funkcionářem strany). Systém Registr je také otevřený a jeho zdrojové kódy jsou dostupné na adrese [https://github.com/svobodni/party\\_registry](https://github.com/svobodni/party_registry)

#### **5. Kdo může ve volbách hlasovat?**

Ve volbách do republikových orgánů mohou hlasovat všichni členové. Ve volbách do krajských orgánů všichni členové příslušní ke krajskému sdružení. Příslušnost ke krajskému sdružení vychází z aktivního volebního práva pro volby do Poslanecké sněmovny Parlamentu ČR (odpovídá adrese trvalého pobytu).

V primárních volbách (hlasování o pořadí pro sestavení kandidátních listin do veřejných funkcí či o nominaci) mohou hlasovat nejen členové, ale i příznivci. V primárkách pro komunální volby hlasují členové a příznivci z celého kraje, v ostatních primárkách (např. pro sestavení kandidátek pro volby do Poslanecké sněmovny) všichni členové a příznivci bez rozlišení kraje.

#### **6. Jak se počítají hlasy, kdo volby vyhraje?**

Při volbách, kdy je počet přihlášených menší nebo stejný, jako je počet obsazovaných míst (platí pro volby do orgánů i pro primárky), se u každého hlasuje PRO NÁVRH, nebo PROTI NÁVRHU. Zvoleni jsou ti, kteří obdrží větší počet PRO NÁVRH než PROTI NÁVRHU.

Je-li počet přihlášených větší než počet obsazovaných míst, volí se systémem „první na pásce“ – tzn., že vyhrají ti, kteří získají nejvíc hlasů. (ve volbě předsedy tedy uchazeč s nejvíce získanými hlasy, ve volbě čtyř místopředsedů čtyři s nejvyšším počtem získaných hlasů)

V případě rovnosti počtu hlasů se následně provádí další kolo, tzv. „rozstřel“ (rozstřelové volby se účastní už jen ti, kteří získali stejný počet hlasů).

## **II. Jak volební systém konkrétně funguje**

### **1. Jak systém pozná, kdo hlasuje?**

Každý oprávněný uživatel (člen, příznivec) má jedinečný identifikátor, který Registr předává volebnímu systému společně s dalšími údaji potřebnými pro posouzení, zda má uživatel v dané volbě hlasovací právo a pro odeslání potvrzujícího e-mailu volebním systémem. (člen/příznivec, příslušnost ke kraji, e-mailová adresa)

### **2. Jak se zaznamená konkrétní hlas?**

Při každém hlasování se vytvoří digitální otisk parametrů hlasu, a to ze všech údajů jedinečně identifikujících hlas (identifikátor volby, identifikátor hlasujícího, identifikátor možnosti/kandidáta), času hlasování (před potvrzením) a z kryptografické soli.

Kryptografická sůl je shluk znaků, který je pro každé hlasování náhodně předgenerován. Hlasující uživatel ji však sám může libovolně upravit. Řetězec se zobrazí před potvrzením volby (ve snadno zkopírovatelné podobě) společně s otiskem s výzvou, aby si správnost otisku ověřil hlasující sám, nebo u některé uvedené on-line služby pro generování SHA1 digitálních otisků.

### **3. Jak si může sám hlasující zkontrolovat svůj odevzdaný hlas?**

Po potvrzení hlasování je hlasujícím odeslán e-mail s informací, jak hlasoval (ten obsahuje: název volby, čas hlasování, kryptografická sůl a otisk). Současně se mu na obrazovce zobrazí obsah tohoto e-mailu s výzvou, aby si ho vytiskl či uložil (pro případ, že mu e-mail nepřijde).

#### **4. Když někdo nehlasuje, jak si zkontroluje, aby jeho hlas nebyl (ať už záměrně, nebo omylem) použit ve volbách (proti jeho vůli)?**

Při skončení hlasování volební systém automaticky vygeneruje stejným způsobem otisky pro všechny, kdo ve volbě nehlasovali. Ti budou mít identifikátor kandidáta 0. Každému nehlasujícím je tak automaticky odeslán e-mail s informací, že proběhla ta konkrétní volba, v níž on nehlasoval.

I u nehlasujících se do základu pro hash a do e-mailu uvádí přesný čas vygenerování. Za nehlasujícího se považuje ten, kdo nevyužil své volební právo a k momentu skončení volby měl právo hlasovat. Nejsou tedy zahrnuti ti, kteří nehlasovali a během voleb pozbyli volební právo (např. přestali být členy/příznivci strany).

#### **5. Jak se zobrazuje výsledek voleb?**

Výsledek volby je zobrazován automaticky ihned po skončení hlasování. Jsou uvedeni všichni kandidáti a zvláště (jako poslední položka) „nehlasovali“ a v každé části seznam digitálních otisků přiřazených k volbě, resp. k nehlasování.

### **III. Revizní zajištění - předpokládaný způsob řešení sporů a stížností**

Tato kapitola shrnuje předpokládané druhy stížností a činnosti rozhodčí komise. Není zde uvedena stížnost na anonymitu volby – ta je zajištěna politickou odpovědností přímo volených členů volební komise a jejich vzájemnou kontrolou.

Ve všech případech se předpokládá, že hlasující svoji stížnost doprovodí výtiskem, textovou kopií nebo e- mailem (včetně kompletních hlaviček) potvrzení o hlasování/nehlasování.

Druhy stížností: „Chybějící hlas“: Tvrzení, že otisk hlasujícího není uveden u žádného kandidáta, ani v nehlasujících. Rozhodčí komise provede ověření otisku. Pokud nesouhlasí, provede se brute-force pokus o vyhledání otisku mezi všemi otisky podle předložených údajů. Je-li nalezen, je důvod se domnívat, že

tvrzení o chybějícím hlasu je nepravdivé. Není-li nalezen, provede se kontrola úplnosti.

„Hlas u nesprávné volby“: Tvrzení, že otisk je přítomen, ale v nesprávné kolonce (u kandidáta, pro kterého člen nehlasoval). Rozhodčí komise provede ověření otisku. Provede se brute-force pokus o vyhledání otisku mezi všemi otisky podle předložených údajů, a to i pro jiná ID voličů. Je-li nalezen u jiného voliče, je důvod se domnívat, že stěžující prostě účelově převzal otisk ze zveřejněných otisků. Je-li nalezen u jiné volby stejného voliče, potom si volič nesprávně pamatuje, koho volil. Není-li nalezen, provede se kontrola úplnosti.

„Podezření z dosypání hlasů“: tvrzení, že některý z kandidátů dostal hlas od nehlasujícího. Rozhodčí komise provede automatizované oslovení všech hlasujících i nehlasujících s výzvou, aby zkontrolovali své otisky. V případě stížnosti na základě automatizovaného oslovení se provedou testy podle předchozích bodů.

## VYSVĚTLENÍ POJMŮ:

### Ověřovací úkony

Ověřovací úkony provádí rozhodčí komise na základě žádosti, tedy při napadení průběhu a výsledků voleb.

### Ověření otisku

Prvním úkolem při zpochybnění je ověření digitálního otisku z údajů, které uživateli poskytla volební komise po potvrzení hlasování e-mailem a zobrazením na obrazovce. Rozhodčí komise si od stěžovatele vyžádá informaci o tom, koho volil (či zda nevolil) a od volební komise si vyžádá identifikátor volby. Z těchto údajů a dalších údajů v e-mailu vytvoří základ

digitálního otisku, z něhož spočítá SHA1. Tím ověří, zda SHA1 otisk předložený stěžovatelem je správný.

## Brute-force vyhledávání

Tento ověřovací úkon vychází z toho, že pro konkrétní zpochybnění jsou k dispozici údaje pro tvorbu digitálního otisku (jsou v potvrzovacím e-mailu či e-mailu o neúčasti). Se znalostí těchto údajů je možné rychle tvořit otisky pro kombinace podkladových údajů pro otisky.

Při brute-force testu si rozhodčí komise od volební komise vyžádá identifikátor voleb, identifikátory kandidátů a získá od správce Registru seznam všech voličů s volebním oprávněním kdykoliv během průběhu hlasování (seznamy R1 a R2 níže). Pro efektivní vyhledání otisku je však nutné znát správnou časovou značku a kryptografickou sůl.

Pokud test nic nenajde, předložil stěžovatel nesprávnou časovou značku či kryptografickou sůl.

Brute-force metoda tedy systematicky vygeneruje otisky pro všechny varianty identifikátoru voliče (ze seznamů R1 a R2) a všechny varianty identifikátorů kandidátů a 0 (nehlasující). Pokud najde shodu, zároveň našla údaje o voliči a zvoleném kandidátovi (či nehlasování). Rozhodčí komise tak může zjistit, že podklady např. nepatří deklarovanému voliči, ale jinému.

## Kontrola úplnosti

Rozhodčí komise požádá správce Registru, aby sdělil seznam identifikátorů oprávněných voličů (dle druhu voleb) k okamžiku ukončení voleb („seznam R1“) a seznam identifikátorů dalších voličů („seznam R2“), kteří k okamžiku ukončení voleb již hlasovací právo neměli (seznamy musejí být oddělené). Rozhodčí komise požádá volební komisi o poskytnutí seznamu identifikátorů hlasujících („seznam VH“) a seznamu identifikátorů nehlasujících („seznam VN“). Celkový počet záznamů obou seznamů identifikátorů musí odpovídat počtu zveřejněných digitálních otisků, přičemž musí odpovídat i rozložení mezi hlasující a nehlasující. Rozhodčí komise použije tyto seznamy a zkontroluje, zda: všechny záznamy seznamu VN jsou obsažené v seznamu R1, (všichni nehlasující měli volební

právo k okamžiku skončení hlasování), v seznamu R1 zároveň označí identifikované záznamy (aby nemohly být identifikovány v dalších krocích) a zároveň: všechny zatím neidentifikované záznamy v seznamu R1 jsou obsaženy v seznamu VH , přičemž identifikované záznamy označí (tím se ověří, že všichni, kdo měli volební právo k okamžiku skončení voleb,

jsou zahrnuti v seznamu digitálních otisků) a zároveň: neoznačené záznamy VH vyhledá v seznamu R2 - každý záznam musí být nalezen (tím se ověří, že zbývající hlasy náleží voličům, kteří během voleb pozbyli volební oprávnění). Pokud výše popsaný test neprojde, je to důvod pro zpochybnění výsledku voleb - znamená to, že volební komise nezveřejnila všechny otisky, nebo jich zveřejnila více.

Předpokládaný způsob rozhodnutí o stížnosti Základním způsobem ověření je kontrola úplnosti. Ostatní testy jsou jen indikativní, přičemž brute-force vyhledávání může ukázat na zneužití cizího digitálního otisku (kontrolního hashe) či na to, že uživatel ve skutečnosti hlasoval pro jiného, než tvrdí (spletl se, zapomněl).

Stejně tak rozhodčí komise může ve spolupráci s provozovatelem registru zjistit, zda volič v deklarovaném času hlasování vůbec mohl hlasovat (= prošel přihlašovacím mechanismem).

Podobně může důvěryhodnost zvýšit nezávislé zjišťování vlastního otisku voličem. Na internetu je více stránek, které výpočet poskytují:

- <http://zmsoft.cz/clanky/sha1.php>
- <http://hash.online-convert.com/sha1-generator>
- <http://www.sha1-online.com/>
- <http://onlinemd5.com/>