

Na základě analýzy dokumentu „Volební manuál mnichovské advokátní komory“ (Příloha č.1), resp. části jeho návrhu přeložené do češtiny (Příloha č.2) jsem dospěl k těmto závěrům.

1) V oblasti anonymního hlasování, pokud se v tomto případě bere za anonymní to, že členové České Advokátní Komory (dále jen ČAK), nemají přístup k informacím o průběhu hlasování. Tedy zejména o tom, kdo a jak hlasoval. Tento návrh řešení tuto podmínku splňuje.

2) V případě implementace v Českém prostředí se přístup k hlasování může provádět rozličnými způsoby např:

A) Ověření pomocí datové schránky vedené na advokáta či advokátní kancelář.

B) Ověření pomocí kvalifikovaného certifikátu pro elektronický podpis.

C) Pomocí systému MojID

3) Popsaný proces:

A) Advokát se nejdříve jedním ze způsobů uvedeným v bodě 2) registruje do registračního systému.

B) Po registraci je mu v registračním systému vygenerován token.

C) Tímto tokenem se poté přihlásí přímo do systému hlasování.

D) Provedete hlasování v systému pro hlasování.

E) Po úspěšném hlasování je daný token zneplatněn a do registračního systému je přenesena informace o tom, že na daného uživatele nesmí být vygenerován další token.

Za předpokladu, že registrační a hlasovací systém budou rozdílné systémy a zároveň bude zajištěna jejich bezpečnost. Je tento způsob vhodný pro nasazení anonymního hlasování tak, jak je definováno v bodu 1)

4) Bezpečnost celého systému je samozřejmě odvislá od způsobu implementace či vývoje systému, použitých technologiích pro elektronické hlasování, použitých šifrách a hashovacích funkcích pro přenos elektronické komunikace toto hlasování umožňující. V průběhu procesu vývoje / implementace by měly být ze strany dodavatele / vývojáře toho systému konzultovány kroky mající přímý dopad na bezpečnost s auditorem / specialistou věnujícím se IT bezpečnosti.

5) Před vlastním vývojem / implementací bude vhodné dojednat také konzultaci, na které se jednotlivé kroky vyjasní.