VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH SYSTÉMU PRO ELEKTRONICKÉ HLASOVÁNÍ A JEHO PRÁVNÍ SPECIFIKA

DESIGN OF THE E-VOTING SYSTEM AND ITS LEGAL SPECIFICS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Vojtěch Váňa

AUTHOR

VEDOUCÍ PRÁCE — JUDr. Pavel Loutocký, BA (Hons), Ph.D.

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Vojtěch Váňa ***ID:*** 221580

Ročník: 2 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Návrh systému pro elektronické hlasování a jeho právní specifika

POKYNY PRO VYPRACOVÁNÍ:

Diplomová práce se bude zabývat základním návrhem systému, který by obsáhl klíčové prvky související s problematikou a možností elektronické hlasování, a který by umožnil bezpečné a transparentní hlasování v digitálním prostředí. Cílem této práce je navrhnout systém, který by zajistil důvěryhodnost a integritu hlasovacího procesu a současně umožnil vhodný a jednoduchý přístup. Teoretická část se bude věnovat analýze souvisejících právních požadavků kladených na elektronické hlasování, praktická část práce se pak zaměří na návrh konkrétního systému a jednotlivých požadovaných kroků pro elektronické hlasování. Cílem práce je tak identifikovat limity a důsledky právní úpravy elektronické hlasování a v té souvislosti představit technologické řešení, ve formě webové stránky, umožňující vzdálené hlasování. V rámci technického výstupu této práce bude webová stránka pro elektronické hlasování – Konkrétní implementace webové stránky, která umožňuje voličům hlasovat elektronicky a zaznamenává jejich hlasy. Databáze hlasovacích údajů – Záznamy o hlasování uložené v databázi. Rozhraní pro administrátora – Speciální rozhraní pro administrátora systému, umožňující správu hlasování, monitorování procesu a kontrolu systému.

DOPORUČENÁ LITERATURA:

podle pokynů vedoucího práce

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 21.5.2024

Vedoucí práce: JUDr. Pavel Loutocký, BA (Hons), Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Diplomová práce se zaměřuje na návrh systému pro elektronické hlasování a jeho právní specifika. Práce se věnovala právním aspektům elektronického hlasování, jako je autentizace voličů, zabezpečení dat a záruka anonymity hlasů. V teoretické části práce byl proveden průzkum historického vývoje elektronického hlasování a analýza zkušeností zemí, které tento systém již implementovaly. Dále práce ukazuje, jaká je současná situace v České republice s elektronickým hlasováním a rozebírá relevantní legislativu související s touto problematikou. Praktická část práce obsahuje konkrétní návrh systému pro elektronické hlasování, který kombinuje technologické inovace s právními požadavky.

KLÍČOVÁ SLOVA

elektronické hlasování, právní specifika, autentizace, zabezpečení dat, návrh systému

ABSTRACT

The thesis focuses on the design of the electronic voting system and its legal specifics. The work focused on the legal aspects of electronic voting, such as voter authentication, data security and guarantee of anonymity of votes. In the theoretical part of the thesis, a survey of the historical development of e-voting and an analysis of the experience of countries that have already implemented this system was conducted. Furthermore, the thesis shows the current situation in the Czech Republic with electronic voting and analyses the relevant legislation related to this issue. The practical part of the thesis contains a concrete proposal for an electronic voting system that combines technological innovations with legal requirements.

KEYWORDS

electronic voting, legal specifics, authentication, data security, system proposal

VÁŇA, Vojtěch. *Návrh systému pro elektronické hlasování a jeho právní specifika*. Diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Vedoucí práce: JUDr. Pavel Loutocký, BA (Hons), Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Bc. Vojtěch Váňa
VUT ID autora:	221580
Typ práce:	Diplomová práce
Akademický rok:	2023/24
Téma závěrečné práce:	Návrh systému pro elektronické hlasování a jeho právní specifika

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu JUDr. Pavlu Loutockému, Ph.D., BA (Hons), za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Hlavní cíl diplomové práce se zaměřuje na zkoumání problematiky elektronického hlasování, jehož vývoj, přijetí a různé přístupy v různých zemích jsou hlavním fokusem teoretické části práce. Na základě této analýzy a teoretických zjištění posléze vytvořit webovou stránku, která by objevená zjištění reflektovala.

Práce se v úvodních kapitolách zabývá obecným vymezením elektronického hlasování a podává přehled jeho historického vývoje, přičemž se postupně zaměřuje na zkušenosti Spojených států, kde bylo elektronické hlasování poprvé implementováno. V této části práce se ukazuje, že i přesto, že byla tato inovace vnímána jako průlomová, byla provázena negativními a kontroverzními reakcemi občanů, a nikdy nebyla zavedena celonárodně.

Následně se práce soustředí na Estonsko, tedy zemi, která se stala průkopníkem v elektronickém hlasování a celkově digitalizaci státu v 21. století a kde se tato forma hlasování stává stále populárnější. Estonský přístup k elektronickému hlasování je široce vnímán veřejností pozitivně a slouží jako inspirace pro další země, které o elektronickém hlasování, případně o větší digitalizaci uvažují.

Další část práce je věnována situaci v České republice, která zatím elektronické hlasování nezavedla, ale tato otázka se opakovaně objevila v rámci vládních programů. Současná vláda se snaží o implementaci tzv. korespondenčního hlasování. Zvláštní pozornost je věnována i postupnému rozvoji online služeb pro komunikaci s úřady od roku 2018, kdy byl založen Portál občana. Tento krok naznačuje směřování ČR k moderním formám interakce s veřejnou správou, přičemž se inspiruje zejména estonským modelem. Díky členství obou zemí v EU je zde prostor pro vzájemnou inspiraci a spolupráci v oblasti digitální demokracie.

Závěrečná část této práce se věnuje zabezpečení hlasovacích údajů a vytvoření praktické webové aplikace ze získaných znalostí a informací o elektronickém hlasování prostřednictvím vytvoření podkladů webové stránky, která umožňuje uživatelům hlasovat elektronicky. Tato část bude detailněji rozebírat proces vytváření a fungování takové platformy a použité technologie k bezpečnému provozu.

1 Teoretická část studentské práce

1.1 Úvodní definice

S rozvojem technologií v různých oblastech našeho života se prudce zvýšilo i využití mechaniky a elektroniky. První papírové volební lístky vznikly před zhruba dvěma sty lety v rámci otevřeného hlasování, kdy voliči napsali jméno svého preferovaného kandidáta, své vlastní údaje, a následně je předložili ke hlasování. Tato raná forma volebních lístků byla v podstatě jednoduchými lístky, které si voliči přinesli sami. Postupem času však začali kandidáti a politické strany distribuovat předtištěné volební lístky, což ne vždy naráželo na vřelé přijetí. Například v Massachusetts bylo třeba rozhodnutí nejvyššího soudu státu (Henshaw v. Foster, 1829), aby takové předtištěné volební lístky byly formálně uznány za legální. Vzhledem k tomu, že otevřené hlasování ohrožovalo soukromí jednotlivců, začal se rychle prosazovat požadavek na tajné hlasování. Tento požadavek byl poprvé zdůrazněn v dokumentu nazvaném Lidová charta, který byl vytvořen Londýnským Sdružením pracujících v roce 1838. Tajné hlasování zahrnovalo situaci, kdy volič vstoupil do volební místnosti s vlastním lístkem a soukromě na něm označil svého preferovaného kandidáta. A až v roce 1856 přišli Australané s novým způsobem hlasování, který měl za cíl potlačit podvody a nátlak ve volbách. K tomu došlo tím, že kandidátům a jejich týmům bylo znemožněno zjistit, jakým způsobem voliči hlasovali. Australská vláda zaručila tajnost voleb tím, že sama poskytla hlasovací lístky a seznam kandidátů. Voliči přišli na volební místo bez vlastních materiálů, obdrželi hlasovací lístek a tužku, na němž označili svého preferovaného kandidáta. Poté složili lístek a vhodili ho do volební urny. Tento systém byl tak efektivní v eliminaci podvodů a chaotických voleb, že se brzy tento systém začal rozšiřovat po celém světě. [1]

Integrace mechaniky do oblasti hlasování se datuje již od 90. let 19. století, kdy Herman Hollerith zavedl děrné štítky pro sčítání lidu v USA.[2] Následně se z toho vyvinul koncept elektronického hlasování. Elektronické hlasování neboli e-voting zahrnuje celou řadu metod hlasování, které zahrnují jak elektronické prostředky pro odevzdání hlasů, tak elektronické prostředky pro sčítání hlasů.

Stejně jako se oblast hlasování vyvinula z tradičního veřejného hlasování a papírových hlasovacích lístků s vyznačenými možnostmi volby, tak i elektronické hlasování prošlo svou vlastní transformací. Přešlo se od systémů děrných štítků k používání optických skenovacích systémů a specializovaných elektronických hlasovacích kiosků, jako jsou elektronické hlasovací systémy s přímým záznamem. Elektronické hlasování může zahrnovat také dálkový přenos hlasovacích lístků prostřednictvím telefonů nebo počítačových sítí, přičemž nejnovějším vývojem prošlo hlasování přes internet.

S rostoucím rozšířením počítačů je prostřednictvím internetu k dispozici stále

více soukromých i vládních služeb. Internet se nyní používá pro ekonomické transakce, daňové přihlášky, přijímací služby na univerzity a další. V důsledku toho roste zájem o možnost umožnit hlasování přes internet.

Technologie elektronického hlasování nasazená ve volebních místnostech může urychlit proces sčítání hlasů a zlepšit přístupnost pro voliče se zdravotním postižením. Zavedení hlasovacího systému, který umožňuje hlasování na dálku prostřednictvím internetu, by mohlo dále zlepšit dostupnost a nabídnout pohodlnější proces hlasování. Tato inovace má potenciál zvýšit účast voličů ve volbách a postupně odstranit stávající, těžkopádné a nejisté postupy hlasování v nepřítomnosti, které se v USA stále ještě provádí převážně poštou.[3]

Snaha o přesnost, bezpečnost a preciznost je hnací silou vývoje elektronických hlasovacích systémů. Nicméně obavy z poškozeného nebo upraveného softwaru brání širokému rozšíření některých systémů. Zejména internetové hlasovací systémy se staly předmětem zkoumání a kritiky. Existuje mnoho hrozeb a problémů souvisejících s možnými útoky a podvodným chováním, včetně síťových útoků, napadených počítačů a poškozených součástí systému.

Oblast kryptografických technologií se také vyvíjela a systémy pro hlasování na dálku přes internet jsou nyní řazeny do kategorie kryptografických hlasovacích systémů. Cílem této kategorizace je nejen zajistit dostatečné utajení, ale také nabídnout možnosti ověření. Jak kdysi řekl Josef Stalin: „Není ani tak důležité, jak kdo hlasuje, ale kdo počítá hlasy!“ [4] Účelem kryptograficky ověřitelných hlasovacích systémů je zabránit nesprávnému zaznamenávání a sčítání hlasů tím, že tyto procesy budou ověřitelné pro každého.

Zatímco papírová hlasovací řešení umožňují v případě chyb opakované sčítání hlasů, kryptografické systémy nahrazují papírovou kontrolní stopu elektronickými potvrzeními a důkazy generovanými pomocí kryptografických mechanismů. Prohlášení typu „Důvěřujte mi“ či „Hardware a software byly důkladně otestovány“ v dnešní době nejsou považována za přijatelná pro hlasovací systém nebo zdůvodnění výsledku voleb. Již nestačí kontrolovat zařízení a nechat ho obsluhovat „důvěryhodnými“ úředníky, je třeba ověřit každý výsledek a proces voleb.

1.2 Elektronické hlasování v USA

Zvolení USA jako příkladu pro elektronického hlasování je relevantní a prospěšné, například i z toho důvodu, že v USA má s tímto hlasováním jedno z nejdelších zkušeností. Celkově vzato, volba USA jako studijního příkladu má potenciál poskytnout široký a cenný pohled na různé aspekty elektronického hlasování, včetně technologických inovací, zabezpečení, inkluzivity a výzev spojených s modernizací volebního procesu. Tato srovnání mohou být klíčovou oporou pro Českou republiku

při přemýšlení o možném zavedení elektronického hlasování v budoucnosti. Existuje několik klíčových důvodů, proč je USA vhodným referenčním bodem:

- Technologický pokrok: USA jsou v čele technologického vývoje a inovací, což znamená, že mají přístup k pokročilým technickým řešením pro elektronické hlasování. Tento faktor poskytuje důležité poznatky o tom, jak nové technologie mohou zlepšit a modernizovat volební procesy.
- Historie volebních reforem: USA mají dlouhou historii volebních reforem a inovací, což zahrnuje také vývoj elektronického hlasování. Studium této historie může nabídnout cenné lekce a inspiraci pro Českou republiku.
- Výzvy a kontroverze: Elektronické hlasování v USA čelí různým výzvám a kontroverzím, včetně otázek týkajících se zabezpečení, integrity a soukromí. Tyto problémy jsou klíčovými tématy, která mohou být relevantní pro českou diskuzi o elektronickém hlasování.
- Rozsah a rozmanitost: USA mají rozsáhlý a rozmanitý systém volby, který zahrnuje volby na federální, státní a místní úrovni. Tato široká škála voleb nabízí bohatý materiál pro studium různých přístupů k elektronickému hlasování na různých úrovních vlády.
- Výsledky a efektivita: Zavedení elektronického hlasování v USA může poskytnout data a výsledky, které lze analyzovat a hodnotit, abychom zjistili, zda tato technologie skutečně zvyšuje efektivitu volebního procesu a zvyšuje účast voličů.
- Potenciální výhody: Zahrnutí konkrétních úspěšných případů elektronického hlasování v USA může poskytnout důkazy o tom, jak tato technologie může zvýšit efektivitu, rychlost a přesnost volebního procesu, což by mohlo přesvědčit oponenty a podpořit zavedení elektronického hlasování v České republice.

1.2.1 Historie elektronického hlasování v USA

V roce 1996 bylo poprvé využito internetového hlasování v USA během prezidentských primárek reformní strany. Toto online hlasování bylo dostupné pouze členům strany, kteří se nemohli zúčastnit sjezdu osobně. V roce 2000 Republikánská strana na Aljašce umožnila voličům hlasovat online na dálku, avšak pouze 35 hlasů bylo tímto způsobem odesláno. Některé parametry z těchto voleb jsou zachyceny na obrázku 1.1.

Stejného roku Demokratická strana v Arizoně nabídla svým členům možnost online hlasování během primárek, což využilo téměř 40 000 voličů, což činilo přibližně 46 procent celkového počtu účastníků. Některé parametry z těchto voleb jsou zachyceny na obrázku 1.2.

Sponsor:	Alaska Republican Party
Election Type:	Party Primary
Date or Voting Period:	January 24, 2000
Target Population:	Alaskan Republican Party members
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	VoteHere Inc.
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	35[8]
Authentication:	One-factor: eight-digit PIN

Obr. 1.1: Parametry voleb na Aljašce.

Obrázek byl převzat z [5]

V roce 2000 FVAP (Federal Voting Assistance Program) spolupracoval s několika dobrovolnickými státy na zcela průkopnickém projektu nazvaném „Hlasování přes internet“ (Voting Over the Internet - VOI), což mělo umožnit příslušníkům zahraničních armád volit online během listopadových voleb. Tato metoda se odlišovala od hlasování faxem či elektronickou poštou tím, že byla založena na webových stránkách. To znamenalo, že voliči mohli použít svá vlastní zařízení k připojení k zabezpečené webové stránce, kde se přihlásili s uživatelským jménem a heslem. Poté mohli vyplnit hlasovací lístek své místní jurisdikce, hlasovat pro kandidáty a další otázky a svůj hlas odeslat zpět kliknutím. Během tohoto procesu bylo zapojeno pět států s 50 okrsky, které předkládaly hlasovací lístky. Voliči ze zahraničí přistupovali k serveru FVAP pro hlasování a místní volební úředníci poté stahovali zašifrované digitální informace. Tímto způsobem bylo poprvé v historii USA umožněno občanům volit online ve skutečných volbách. Ačkoliv bezpečnostní experti ministerstva obrany Spojených států byli obeznámeni s hrozbami internetového hlasování a způsoby, jak jim čelit, FVAP pozvalo externí etické hackery, známé jako „White Hat“, aby prozkoumali systém VOI a identifikovali jeho slabiny. Kromě toho stát Florida na systém VOI trval na nezávislém testování podle svých vlastních standardů, což bylo splněno, a systém VOI získal oficiální certifikaci. Těchto voleb se zúčastnilo pouze 84 lidí. [5] Některé parametry z těchto voleb jsou zachyceny na obrázku 1.3.

V roce 2003 FVAP (Federal Voting Assistance Program), jedná se o agenturu pod ministersvem obrany, rozšířil možnost volit prostřednictvím faxu a poskytl vojákům v Iráku a Afghánistánu možnost volit pomocí elektronické pošty. [6]

Hodnotící studie srovnávala využití internetového hlasování s tradičním systé-

Sponsor:	Arizona Democratic Party
Election Type:	Party Primary
Date or Voting Period:	March 7, 2000
Target Population:	Registered Democratic Party members
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	election.com
Channel Protection:	HTTPS, shared administrative passwords
Participating Voters:	39,942[15]
Authentication:	One-factor: PIN

Obr. 1.2: Parametry voleb demokratických primárek v USA.

Obrázek byl převzat z [5]

mem hlasování poštou (Digital Vote by Mail - VBM), který byl v minulosti často používán vojenskými osobami. Výzkum přinesl několik klíčových zjištění, včetně toho, že uživatelé měli větší důvěru v systém VOI oproti tradičnímu procesu VBM. Dále bylo zaznamenáno, že systém VOI přijímal pouze jeden hlas od každého voliče a poskytoval vyšší úroveň tajnosti, soukromí a ochrany proti manipulacím s hlasovacími lístky ve srovnání s procesem VBM. Systém VOI také usnadňoval spolehlivé auditování a přepočty, což bylo důležité pro zachování integrity voleb. Důležitým aspektem bylo také to, že právo na hlasování bylo posíleno, protože mnoho potíží spojených s procesem VBM, které často odradily voliče od účasti, bylo díky VOI odstraněno. Mezi tyto problémy patřily zpoždění při doručování pošty a odmítnutí registračních formulářů. [5] [6]

Na ministerstvu obrany začalo narůstat povědomí, že internetové hlasování bude budoucností hlasování pro své vojenské osoby v zahraničí. Navíc ještě odborníci na počítačové vědy v projektu „Caltech/MIT pro technologii voleb“ označili registrační aplikaci VOI za osvědčenou praxi ve volbách. [7]

Experiment se zabezpečenou elektronickou registrací a hlasováním (SERVE)

Začátek SERVE zákona o národní obraně pro fiskální rok 2002 nařídil ministru obrany provést rozšířený demonstrační projekt, který by umožnil příslušníkům ozbrojených složek odevzdávat hlasy prostřednictvím elektronického volebního systému do voleb v roce 2004. Využívaje znalostí získaných z proof of concept projektu VOI, FVAP začalo pracovat na experimentu Secure Electronic Registration and Voting Experiment (SERVE). Padesát pět okresů ze sedmi států dobrovolně souhlasilo

Sponsor:	FVAP; South Carolina (Statewide); Okaloosa County, FL; Orange County, FL; Dallas County, TX; Weber County, UT
Election Type:	General Election
Date or Voting Period:	September - November 2000
Target Population:	UOCAVA voters
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	U.S. Department of Defense (DoD) FVAP
Channel Protection:	VPN between central server and servers at state/county offices; SSL between voters and central server; session and object encryption
Participating Voters:	84
Authentication:	Two factor: User name and password with hard token DoD PKI medium assurance (X.509) digital certificate

Obr. 1.3: Parametry listopadových voleb v USA.

Obrázek byl převzat z [5]

s účastí. Podle zprávy EAC (Election Assistance Commission) o projektu SERVE „služby pro voliče zahrnovaly: online registraci voličů a aktualizaci informací o voličích online; doručování volebních lístků a výběr hlasů; a kontrolu svého registračního a volebního stavu.“ [5]

Skupina, která měla na starost SERVE, zaměstnala několik členů předchozího týmu VOI. Dále se do projektu zapojily soukromé společnosti, včetně Accenture a VeriSign, které měly zkušenosti s vývojem internetových volebních systémů podobných tomu, který byl úspěšně nasazen v Arizoně. V Arizoně byl tento systém přizpůsoben pro vojenské osoby v zahraničí a stal se nejdelší stávající programem internetového hlasování pro vojenské osoby v zahraničí v USA. [5]

Hlasovací proces SERVE byl komplexně zabezpečen od začátku do konce. Každý volič musel podat žádost o hlasování v systému. Po schválení registrace byl každému voliči přidělen digitální certifikát X.509, který sloužil k ověření totožnosti voliče při přihlášení. [5]

Podobně jako u systému VOI, tyto bezpečnostní kontroly byly navrženy tak, aby zabránily volebnímu podvodu tím, že zajistily, že hlasují pouze registrovaní voliči a že každý volič hlasuje pouze jednou. Centrální server byl umístěn v bezpečném zařízení na pozemcích společnosti Accenture v Restonu ve Virginii. Správci systému museli používat bezpečnostní průkazy k vstupu na pozemky, a přístup k serveru byl omezen na certifikovaný personál, přičemž každý z nich měl svůj vlastní bezpečnostní kód.

Pro každou účastnickou místní volební správu byly na centrálním serveru vytvořeny samostatné moduly. Pouze jejich autorizovaný personál mohl přistupovat k centrálnímu serveru ze své místní kanceláře. Pro další zvýšení zabezpečení poskytlo FVAP každé místní správě přenosný počítač určený výhradně pro projekt SERVE. Pomocí těchto počítačů mohly místní správy stahovat zašifrovaná volební data z centrálního systému. Počítače vydávané FVAP byly nastaveny tak, aby dešifrovaly pouze data pro danou místní správu. Alespoň dvě autorizované osoby v místní správě musely provést přihlášení k přístupu k datům voličů. [5]

Šifrování rovněž znemožňuje neoprávněným osobám zjistit, kdo hlasoval, nebo jak kdo hlasoval. Mít všechna zašifrovaná volební data pro každou místní správu na jednom přenosném počítači, který vyžaduje alespoň dvě osoby pro použití dešifrovacích klíčů, vytváří mnohem bezpečnější situaci než mít hromady a hromady tisíců přijatých hlasů odeslaných poštou roztroušených po kanceláři volebního úředníka. Během vývoje byly operace SERVE a bezpečnostní opatření drženy ve standardních, které již používaly vojenské oddělení DoD, včetně Národní bezpečnostní agentury. Široké spektrum nezávislých expertů na příslušné téma prošlo systém SERVE ve snaze najít bezpečnostní zranitelnosti a stejně jako u VOI byl systém SERVE nezávisle certifikován státem Florida. David Chu, ředitel FVAP, využil tabulku 1.4, aby přehledně ukázal bezpečnostní rizika, která byla předpokládána týmem SERVE, a strategie, které byly vypracovány k ochraně proti těmto hrozbám, a to ve své zprávě pro Kongres.

Systém SERVE byl navržen tak, aby zvládl mnohem více hlasů než pouhých 84 odevzdaných v experimentu VOI. Pracovníci SERVE si dále stanovili za cíl vytvořit vzorový systém, který by byl schopen v budoucnu rozšířit, tak aby obsáhl přibližně šest milionů občanů USA. Aby se zajistilo, že technologický pokrok nezůstane utajený a že se jedná o otevřený proces místo tajné operace prováděné vládními elitami, FVAP zřídil Skupinu pro přezkum bezpečnosti SERVE (SPRG). Tato skupina sestávala z 10 členů, kteří pocházeli z akademického prostředí a průmyslu. Někteří z těchto odborníků byli vybráni z důvodu své známé kritiky internetových voleb. Nic nebylo před nimi utajeno a vše bylo otevřeno pro jejich inspekci. Členové SPRG, kteří byli skeptičtí k projektu, nesdíleli nadšení týmu SERVE ohledně vize, že všichni občané UOCAVA (The Uniformed and Overseas Citizens Absentee Voting Act) by mohli jednoho dne volit přes internet. [6]

Projekt SERVE byl tedy zrušen ještě před jeho zavedením z důvodu obav o bezpečnost. Ministerstvo obrany s odkazem na nedostatek důvěry veřejnosti v systém kvůli této zprávě rozhodlo, že projekt za těchto okolností nemůže pokračovat. 1.5

Kancelář státního tajemníka státu Arizona zaváděla internetový volební systém pro obecné volby v letech 2008 a 2010. Tento volební systém byl vyvinut kanceláří státního tajemníka státu Arizona s využitím několika standardních průmyslových

Threat	Mitigation
Network Security	- Encryption - Intrusion Detection Systems - Redundant Firewalls - Penetration Tests
Privacy	- Digital Signatures - Secure Socket Layers - Encryption - Voter Identity—Ballot Data Separation - Voter Ballot Data Verification
Virus, Worm, Trojan Horse	- Anti Virus Scanning - Digital Signatures - Voted Ballot Data Verification
Spoofing	- Secure Socket Layer - Digital Signatures - Voted Ballot Data Verification
Denial of Service	- Large Quantity of Bandwidth, Multiple Carriers - Multiple Internet Service Provider Entry Points - Utilization Monitoring
Voter Fraud	- Digital Signatures

Obr. 1.4: Obrázek ukazující hrozby a jejich mitigaci.

Obrázek byl převzat z [7]

technologií, včetně Microsoft .Net 3.5, Microsoft SQL Server a 128bitového protokolu SSL. [5]

Proces voleb fungoval následovně: [5]

- Volič nejprve kontaktoval úřad státního tajemníka státu Arizona a požádal o účast v programu.
- Okres, kde byl volič zaregistrován, obdržel e-mailové oznámení o žádosti voliče od úřadu státního tajemníka.
- Okres povolil účast voliči a vytvořil pro něj účet.
- Úřad volby zaslal voliči e-mail obsahující přihlašovací údaje a instrukce k systému.
- Hlasovací lístek byl voliči doručen poštou, e-mailem nebo faxem.
- V případě potřeby si volič vytiskl hlasovací lístek.
- Volič provedl výběr na hlasovacím lístku a naskenoval jej na svůj osobní počítač.
- Volič přešel na webovou adresu uvedenou v e-mailu a provedl přihlášení.
- Volič nahraje naskenovaný hlasovací lístek a podepsané čestné prohlášení na webové stránky státního tajemníka státu Arizona.
- Volič a příslušný okresní úředník obdrží potvrzovací e-mail týkající se ode-

Election Type:	General Election
Date or Voting Period:	Scheduled for 2004 General Election
Target Population:	Military and Overseas voters
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	FVAP, Hart InterCivic
Channel Protection:	SSL 3.0 with session keys, and encrypted and digitally signed data (SHA1 with DSA)
Participating Voters:	0
Authentication:	Two factor: User name and password, X .509 digital certificate

Obr. 1.5: Parametry neuskutečněných SERVE voleb do parlamentu v USA.

Obrázek byl převzat z [5]

vzdání hlasovacího lístku.

- Úředník okrsku stáhne hlasovací lístek z webu státního tajemníka státu Arizona a provádí jeho přepis, sčítání a sčítání hlasů.

Některé parametry z těchto voleb jsou zachyceny na obrázku 1.6.

UOCAVA

The Uniformed and Overseas Citizens Absentee Voting Act of 1986 (UOCAVA) slouží k ochraně volebních práv vojáků v aktivní službě, jejichž umístění je mimo jejich domovské volební obvody, stejně jako práv manželů a dalších oprávněných rodinných příslušníků těchto vojáků. Zákon také zajišťuje ochranu volebních práv občanů USA, kteří žijí mimo území Spojených států a dalších příslušníků uniformovaných složek. UOCAVA stanovuje, že všechny státy, teritoria a District of Columbia musí umožnit těmto občanům registrovat se a hlasovat v nepřítomnosti ve všech federálních volbách.

Tato opatření jsou zaměřena na přibližně 1,33 milionu příslušníků aktivní služby a zhruba 573 000 manželů a manželek vojáků, stejně jako na závislé osoby, kteří jsou mimo své domovské volební obvody. Pro dalších přibližně 2,6 milionu občanů USA, kteří mají právo volit a žijí, studují nebo pracují v zahraničí, přináší proces hlasování v nepřítomnosti odlišné výzvy a může být složitější než pro nevojenské voliče s trvalým bydlištěm ve Spojených státech. Zákon se jmenuje Public Law 99-410 a byl podepsán prezidentem Ronaldem Reaganem 28. srpna 1986. [8]

Sponsor:	Arizona Secretary of State's Office
Election Type:	General Election
Date or Voting Period:	November 4, 2008, November 2, 2010
Target Population:	UOCAVA Voters
Channel:	Controlled>Electronic Ballot Return>Web Application/Email/Fax
Technology Provider:	Arizona Secretary of State's Office
Channel Protection:	128-bit SSL
Participating Voters:	The EAC was unable to obtain this information
Authentication:	Two-factor: Username/Password and electronic representation of voter's signature

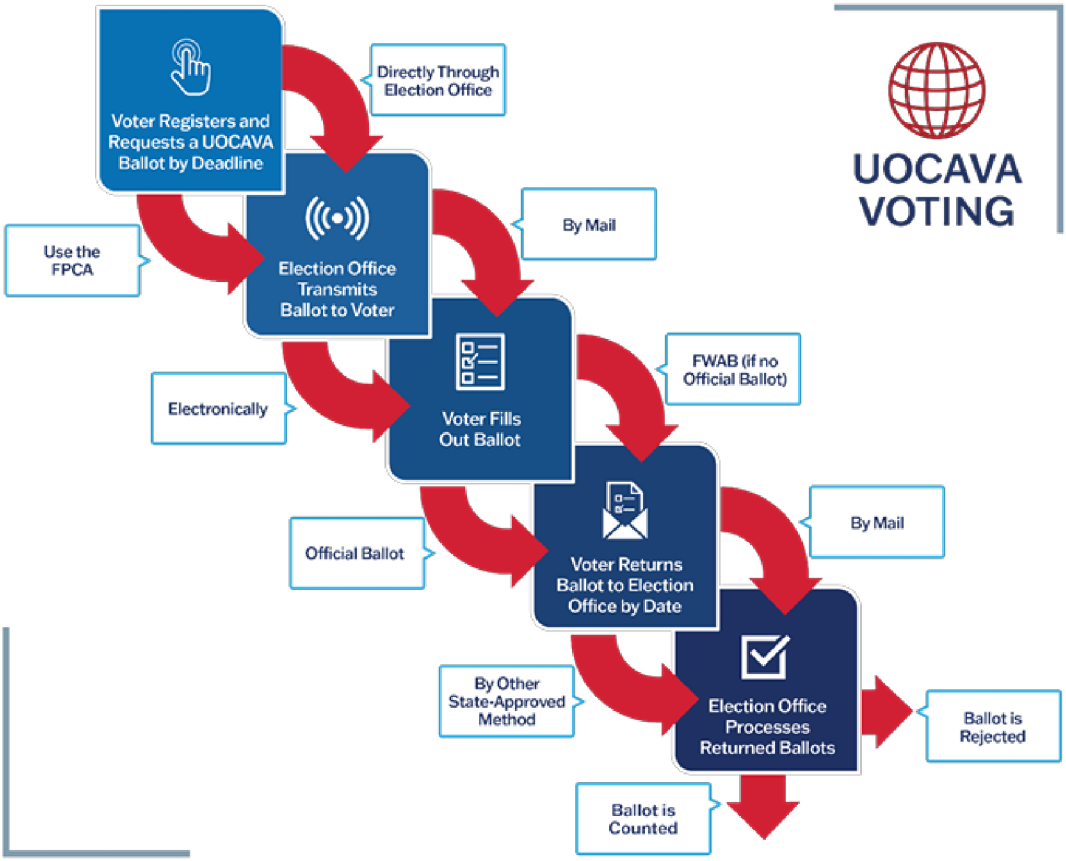
Obr. 1.6: Parametry voleb do parlamentu v USA v letech 2008 a 2010.

Obrázek byl převzat z [5]

USA státy povolující elektronické hlasování

Podle aktuálních údajů již 34 států umožňuje či bude umožňovat nějakou formu elektronického hlasování (viz mapa 1.8). Nicméně tento počet se v mnoha zdrojích liší. Dále tato forma hlasování není určena pro všechny, ale pouze pro občany UOCAVA, tedy zpravidla vojenský personál. Případně také některým lidem se zdravotním postižením. Oproti parlamentním volbám v roce 2018 došlo v parlamentních volbách v roce 2022 k poklesu jak počtu odevzdaných a sečtených hlasovacích lístků od voličů v zahraničí (UOCAVA), tak i procenta voličů, kteří využili tohoto způsobu hlasování. Z dat EAVS 2018 vyplývá, že bylo odevzdáno 358 137 hlasovacích lístků UOCAVA, což představovalo 0,3 procent všech voličů. V parlamentních volbách v roce 2022 bylo odevzdáno a sečteno 254 721 hlasovacích lístků UOCAVA, což představuje 0,2 procent všech voličů. Počet odevzdaných hlasovacích lístků UOCAVA a procento voličů, kteří tuto možnost využili, se v parlamentních volbách v roce 2020 rapidně zvýšily na 938 297 a 0,6 procent, ale pro volby v roce 2022 klesly pod úroveň před pandemií. Nejčastěji používaným způsobem, jak předat hlasovací lístky voličům UOCAVA pro všeobecné volby v roce 2022, byl elektronický přenos pomocí e-mailu (48,5 procent). Tento způsob byl následován předáním poštou (38,4 procent) a dalšími metodami, jako jsou fax nebo online systémy (12,6 procent). Podíl hlasovacích lístků odeslaných elektronickou poštou se ve srovnání s rokem 2018 snížil o přibližně 8 procentních bodů (na 56,6 procent). Předávání hlasovacích lístků pomocí jiných metod zaznamenalo v období 2018 až 2022 významný nárůst. [8] Jak funguje

proces volby pro UOCAVA je zobrazen zde 1.7



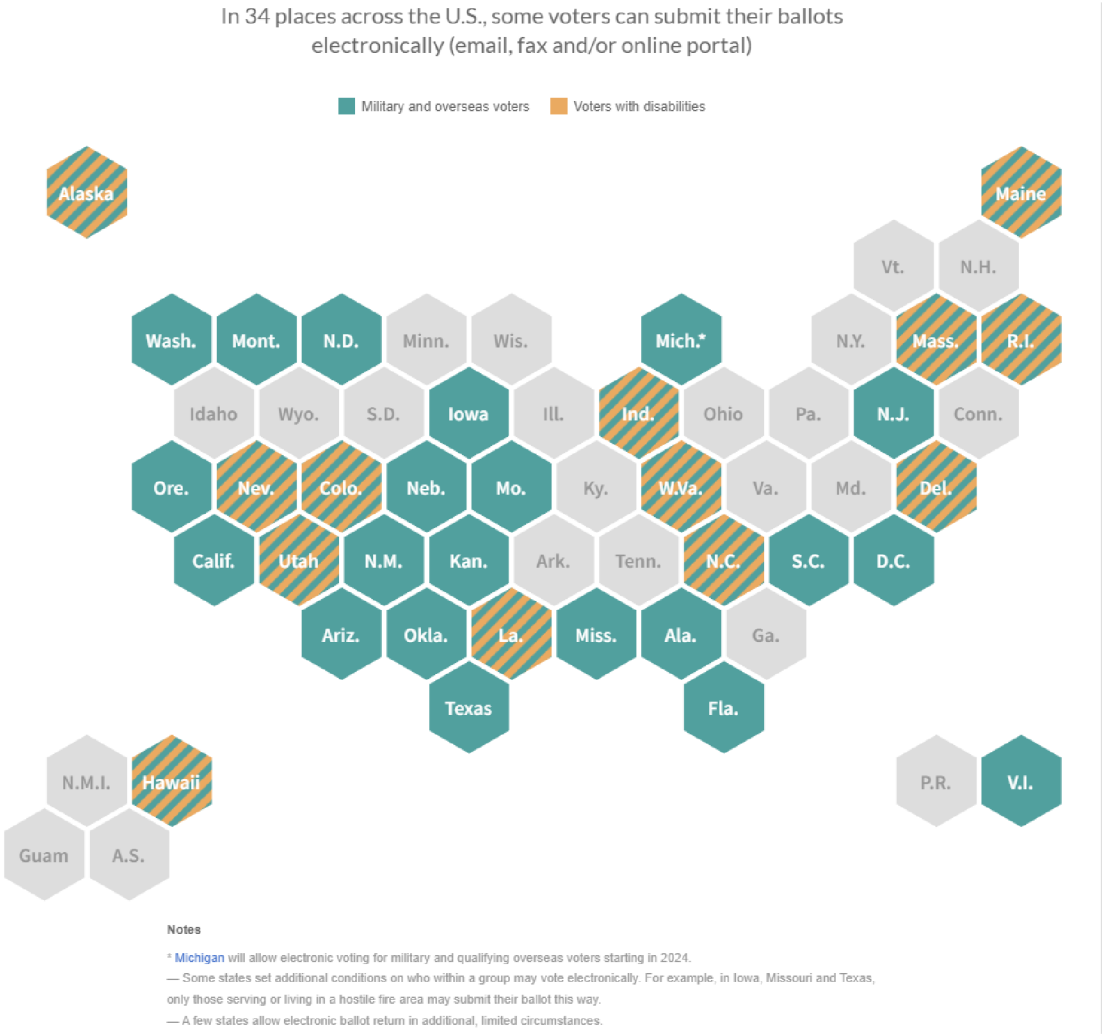
Obr. 1.7: Proces UOCAVA volby.

Obrázek byl převzat z [8]

Američané jsou zvyklí využívat také korespondenční hlasování i přesto, že volební účast prostřednictvím korespondenčního hlasování v roce 2022 klesla ve srovnání s parlamentními volbami v roce 2020, stále zůstala vyšší než před vypuknutím pandemie. Tato míra dosáhla 31,9 procent voličů, kteří se zúčastnili voleb v roce 2022 a odevzdali své hlasovací lístky prostřednictvím pošty. Skoro polovina všech voličů dala svůj hlas osobně v den voleb. Více než dvě třetiny voličů odevzdaly své hlasovací lístky osobně buď v den voleb nebo před ním při všeobecných volbách v roce 2022.

Obecně jsou Američané z odborných kruhů z této možnosti poměrně skeptičtí viz citát William Adlera (z Centra pro demokracii a technologie). „V podstatě všichni odborníci na bezpečnost voleb se shodují na tom, že bychom neměli nechat hlasovat velké množství lidí přes internet. V tomto bodě panuje skutečně větší shoda než

téměř v čemkoli jiném v oblasti bezpečnosti voleb.“[9] Také zpravidla starším občanům se tato možnost nezamlouvá. Zhruba 39 procent obyvatel Spojených států vyjadřuje zájem o možnost hlasovat přes svůj počítač nebo mobilní zařízení, pokud by to bylo k dispozici. Většina těch, kteří by byli nakloněni online hlasování, patří do věkové skupiny mladších 30 let. [10]



Obr. 1.8: Státy USA umožňující elektronické hlasování.

Obrázek byl převzat z [9]

Shrnutí

Elektronické hlasování ve Spojených státech amerických poskytuje důležité poznatky a zkušenosti, které mohou být cenné i pro Českou republiku při úvahách o možném zavedení této technologie do volebního procesu. V historii elektronického hlasování v USA jsou patrné technologické inovace, ale také výzvy a kontroverze spojené s

bezpečností, integritou a soukromím. Přestože byly provedeny různé experimenty s internetovým hlasováním pro vojenské osoby a občany žijící mimo USA, jako projekt SERVE, následovala opatrnost a následné zrušení projektu kvůli obavám o bezpečnost. Navzdory této zkušenosti některé státy v USA již umožňují určité formy elektronického hlasování, především pro vojenské osoby a lidi se zdravotním postižením. Nicméně, způsoby odevzdávání hlasů se mění a přizpůsobují vývoji, jak ukazuje trend voličů, kteří využívají elektronickou poštu ke komunikaci a odevzdání svých hlasů. Tyto zkušenosti a změny v preferencích voličů v USA mohou poskytnout užitečné informace pro budoucnost elektronického hlasování v České republice. Je důležité brát v úvahu jak potenciální výhody, tak i rizika spojená s touto technologií při hledání optimálních způsobů jejího využití v rámci volebního procesu a zajištění demokratického a spolehlivého hlasování.

Přestože USA patří mezi státy, které povolují nějakou formu elektronického hlasování, tato možnost není využívána široce. Většinou je určena pro občany UOCAVA (The Uniformed and Overseas Citizens Absentee Voting Act) a vojenský personál nebo pro lidi se zdravotním postižením. Navzdory existenci elektronického hlasování stále převažuje korespondenční hlasování a osobní účast voličů v den voleb.

Většina států USA umožňuje určitou formu elektronického hlasování, ale jeho využití je stále omezené. Pokles účasti voličů při elektronickém hlasování v porovnání s jinými formami hlasování naznačuje, že existují obavy ohledně bezpečnosti a důvěryhodnosti tohoto systému.

Tato historie a experimenty s elektronickým hlasováním v USA poskytují cenné poznatky ohledně technických inovací, bezpečnosti, a výzev spojených s modernizací volebních systémů. Tyto informace mohou být užitečné pro Českou republiku při posuzování možnosti zavedení elektronického hlasování v budoucnosti. Při zvažování této technologie je nezbytné zohlednit a adresovat obavy týkající se zabezpečení, integrity voleb a ochrany osobních údajů, aby bylo zajištěno důvěryhodné a demokratické hlasování.

Tab. 1.1: Tabulka výhod elektronického hlasování v USA.

Výhody
Umožňuje lepší dostupnost volby pro mladé lidi a technologicky zdatné občany, kteří jsou zvyklí na online interakce.
Umožňuje hlasování z domova nebo ze zahraničí, což je obzvláště užitečné pro voliče žijící mimo USA nebo pro osoby s omezenou mobilitou.
Rychlejší sčítání hlasů
Zrychlené zveřejnění výsledků.
Může vést k úsporám nákladů spojených s tiskem a distribucí

papírových hlasovacích lístků.
Potencionální zvýšení účasti voličů
Pohodlí elektronického hlasování může motivovat více lidí k účasti ve volbách.
Umožňuje voličům hlasovat v jakoukoliv dobu během volebního období, což zvyšuje flexibilitu.
Ekologický přínos snížením spotřeby papíru a dopravních emisí souvisejících s distribucí a sčítáním papírových hlasovacích lístků.
Elektronické záznamy umožňují efektivnější procesy auditování a ověřování hlasovacích výsledků.

Tab. 1.2: Tabulka nevýhod elektronického hlasování v USA.

Nevýhody
Bezpečnostní obavy například z hackerských útoků a manipulace s hlasovacími daty.
Potenciální technické problémy, jako jsou chyby v softwaru nebo selhání hardwaru, mohou ovlivnit hlasovací proces.
Výzvy spojené s ověřením identity voličů a zajištěním, že každý hlas je jedinečný a autentický.
Aktuální limitace pouze na úzkou skupinu lidí jako UOCAVA
Důvěra veřejnosti, výzvy spojené s budováním a udržováním důvěry veřejnosti v elektronické hlasovací systémy.
Sociálně-ekonomický problém, mohou vzniknout rozdíly v účasti na hlasování založené na přístupu k technologiím a internetu mezi různými sociálně-ekonomickými skupinami.
Závislost na internetové infrastruktuře, efektivita a dostupnost elektronického hlasování může být omezena v oblastech s nízkou úrovní internetového pokrytí.
Výzvy spojené s přijetím a adaptací nových technologií mezi staršími voliči a těmi, kteří nejsou technologicky zdatní.

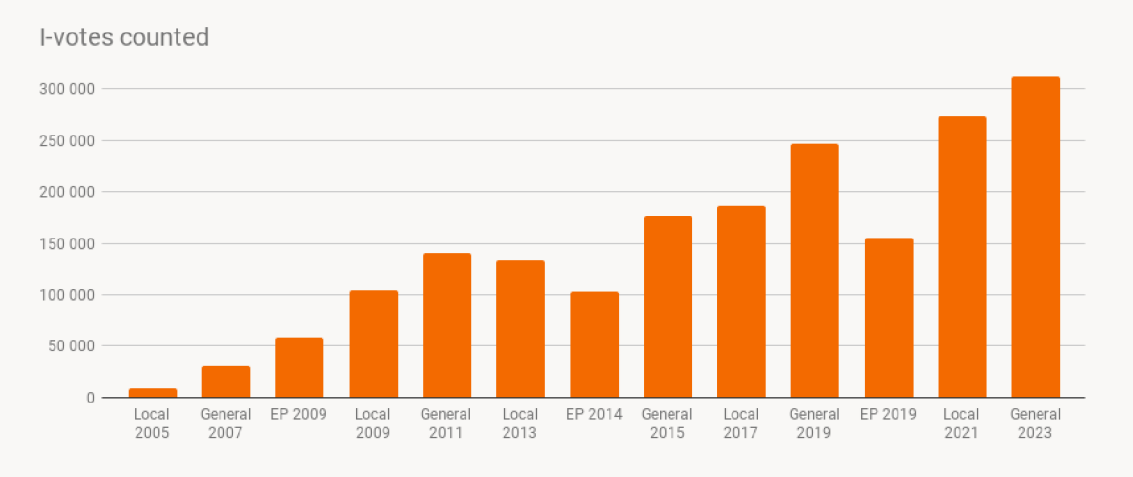
1.3 Elektronické hlasování v Estonsku

Estonský internetový volební systém představuje jedinečný nebo neobvyklý případ, neboť žádná jiná země na světě nesahá k úrovni, kde by umožňovala všem voličům hlasovat plošně online. Proto si myslím, že použití Estonka jako příkladu pro elektronické hlasování je velmi relevantní a přínosné. Obecně vzato, volba Estonska jako modelu pro zkoumání elektronického hlasování v České republice poskytuje možnost získání hlubšího porozumění fungování efektivního a bezpečného volebního systému založeného na moderních technologiích. V zemi, která má pouze 1,3 milionu obyvatel a HDP na obyvatele o polovinu menší než Česká republika, nabízí zajímavá srovnání, která mohou být klíčovým prvkem při zvažování možného zavedení elektronického hlasování v budoucnosti. Existují některé klíčové důvody, proč je Estonsko vhodným bodem pro referenci:

- Digitální přístupnost a inovace: Estonsko je považováno za jednu z nejvíce digitálně pokročilých zemí na světě. Má bohaté zkušenosti s využíváním moderních informačních technologií ve veřejné správě, což zahrnuje i elektronické hlasování. Studium estonského modelu může poskytnout příklady úspěšné integrace digitálních technologií do volebního procesu.
- Bezpečnostní opatření: Estonsko přikládá velký důraz zabezpečení elektronického hlasování. Jejich systém využívá moderní šifrovací a autentizační technologie k zajištění bezpečnosti a důvěryhodnosti voleb. Tato bezpečnostní opatření mohou poskytnout užitečné poučení o tom, jak efektivně ochránit elektronický volební systém.
- Zkušenosti s elektronickým občanstvím: Estonsko bylo jednou z prvních zemí, které zavedly elektronické občanství. Tato zkušenost může být relevantní při studiu elektronického hlasování, protože ukazuje, jak se technologie může úspěšně integrovat do občanské participace a demokratického procesu.
- Vysoká účast voličů: Estonsko se může pyšnit vysokou účastí voličů, což naznačuje, že elektronické hlasování může být efektivním nástrojem k podpoře angažovanosti občanů v politickém procesu. Tato zkušenost může posloužit jako inspirace pro země, které hledají způsoby, jak zvýšit účast občanů.
- Transparentnost a otevřenost: Estonsko klade důraz na transparentnost a otevřenost ve svém volebním procesu. Toto zaměření může poskytnout model pro zajištění důvěryhodného volebního systému a zapojení občanů do sledování volebního procesu.
- Podpora inovací: Estonsko je známé pro svou podporu inovací a modernizaci ve veřejné správě. Studium estonského přístupu k elektronickému hlasování může poskytnout náhled na to, jak podnítit inovace v oblasti volebních systémů.

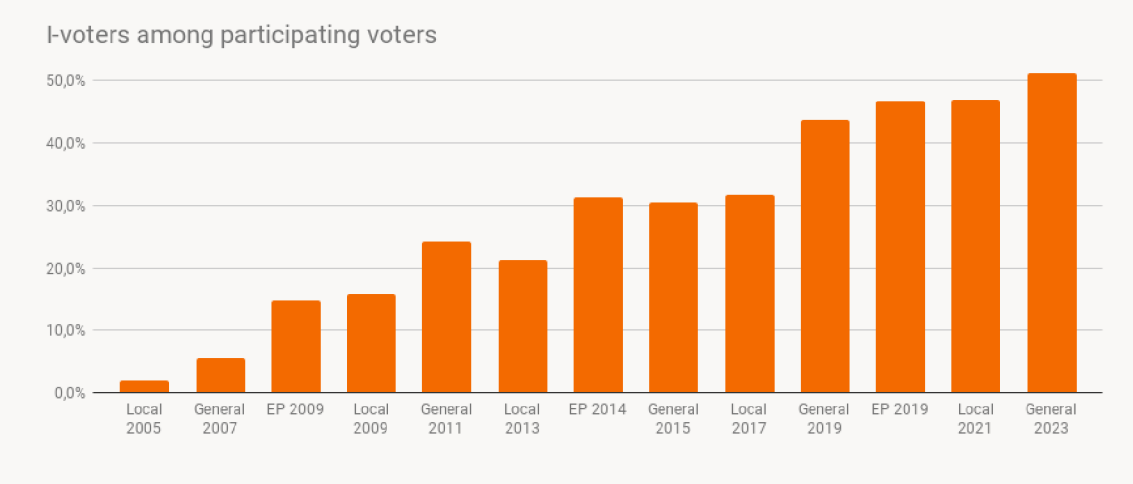
Estonsko (vstup do EU v roce 2004) se vynořuje jako výrazná výjimka v kontextu

celosvětově omezených a zastavených pokusů s elektronickým hlasováním. Estonsko se stalo první zemí na světě, která implementovala internetové hlasování do svých celostátních voleb, a to od roku 2005, umožňujíc voličům hlasovat z libovolného počítače připojeného k internetu kdekoliv na světě. Rovněž je to také země, ve které se každým rokem zvětšuje počet lidí, kteří využijí možnost volby přes internet (viz obrázky 1.9 1.10). Pro vysvětlení jak elektronické volby fungují, nahlédnutí na výsledky a statistiky, mají web `www.valimised.ee` (v překladu volby), který je přehledný a lokalizovaný do třech jazyků, a to Estonština, Angličtina a Ruština. Výtku bych měl pouze k tomu, že některé hlavně technické soubory nacházející se na webu jsou pouze v Estonštině. Díky této inovaci může Estonsko snížit náklady na volby a zároveň podporovat zvýšenou účast voličů, zejména mezi mladšími lidmi.[11]



Obr. 1.9: Počet hlasů v absolutním čísle, které byly odevzdaný online v Estonsku. Obrázek byl převzat z [14]

Zvyšující se zájem o elektronické hlasování spolu s rostoucím povědomím o souvisejících rizicích přivedl k mezinárodnímu úsilí o formulaci standardů pro elektronické volby. Doporučení Rady Evropy rec(2004)11 [12] a aktualizované doporučení rec(2017)5 ([13]) stanoví právní normy pro elektronické hlasování, včetně obecného, svobodného a tajného hlasování a poskytují procesní záruky jako je transparentnost, ověřitelnost, odpovědnost, spolehlivost a bezpečnost. Tato doporučení také stanoví normy pro provoz a techniku, které se týkají dostupnosti, interoperability, systémového provozu, bezpečnosti, auditu a certifikace. S cílem usnadnit uplatňování těchto doporučení. Rada vytvořila směrnice pro certifikaci elektronických volebních systémů a transparentnost elektronických voleb. Zároveň doporučení upozorňují na fakt, že elektronické hlasování lze zavést pouze tehdy „pokud voliči mají důvěru ve svůj stávající volební systém“ a vyzývá státy, aby „učinily vše pro to, aby byla



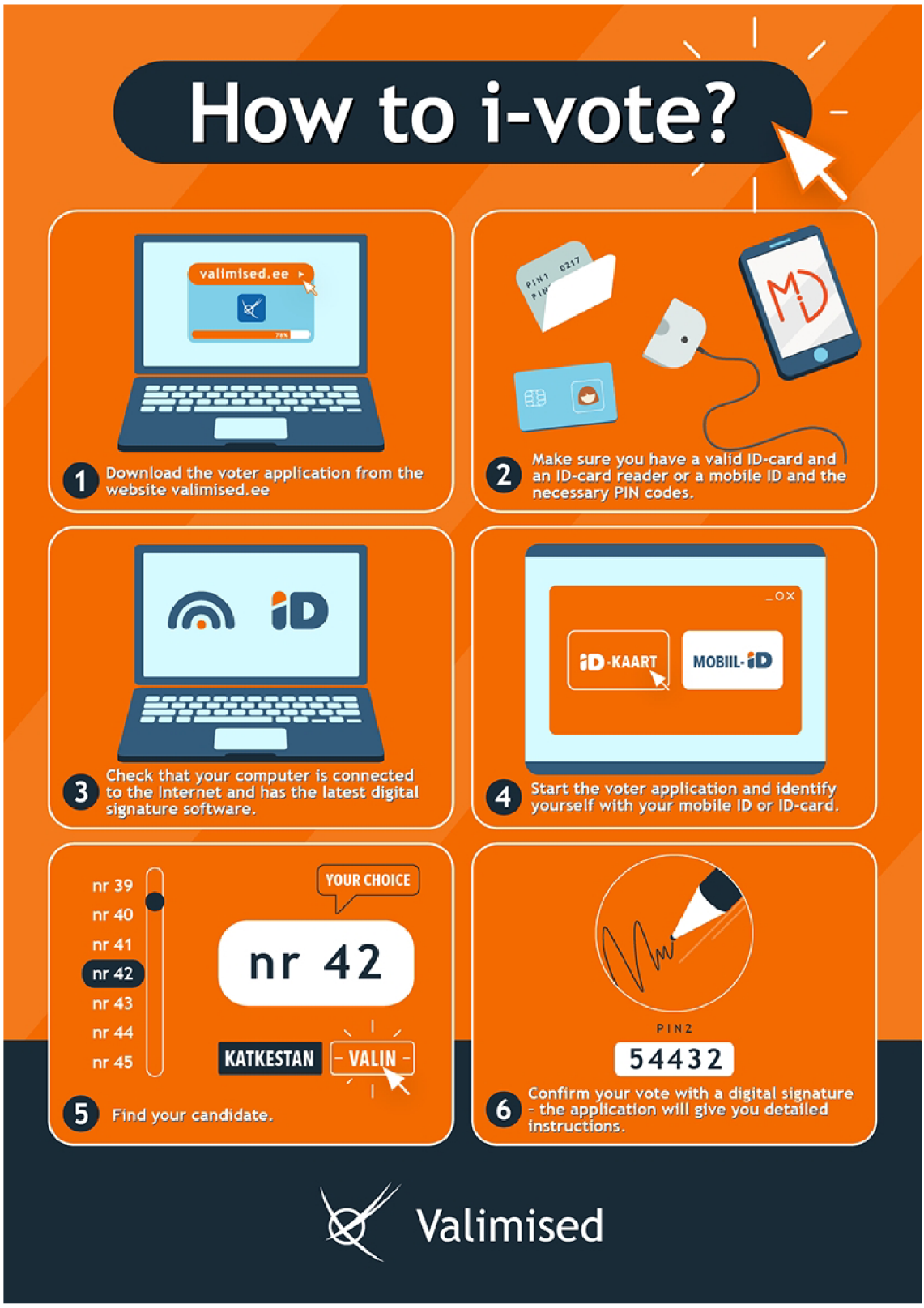
Obr. 1.10: Počet hlasů v procentech, které byly odevzdaný online v Estonsku. Obrázek byl převzat z [14]

důvěra zachována“ [11]

1.3.1 Proces elektronického hlasování v Estonsku

Je důležité zdůraznit, že elektronické hlasování je volitelnou alternativou k tradičnímu papírovému hlasování a je k dispozici v předem stanoveném období před samotným dnem voleb, konkrétně od desátého do čtvrtého dne před volbami. Tyto volby mohou probíhat tak, že voliči mají možnost hlasovat z libovolného počítače připojeného k internetu, a to z jakéhokoli místa na světě. Volební proces se dá popsat následovně: Viz obrázek 1.11 [15]

- Volič si stáhne oficiální aplikaci z vládního webu.
- Volič si vezme svůj občanský průkaz. (V roce 2002 byl přijat zákon, který nařizoval občanům, aby si pořídili identifikační kartu s kódem a mikročipem obsahujícím osobní údaje.) A k počítači má připravenou ID čtečku nebo mobileID.
- Volič si zkontroluje, zda má přístup k internetu a a má nejnovější digitální software pro digitální podpis.
- Zapne aplikaci, identifikuje se pomoci čtečky s ID kartou nebo pomoci mobileID.
- Vyhledá svého kandidáta či stranu.
- Potvrdí svůj hlas digitálním podpisem.



Obr. 1.11: Proces elektronického hlasování v Estonku.

Obrázek byl převzat z [15]

MobileID

Kromě občanského průkazu, který je opatřen čipem, a poskytuje pokročilé elektronické funkce, jako je bezpečné ověřování a digitální podpisy. Další metodou elektronické identifikace, která se objevila v roce 2007, je mobile-ID, využívající chytré telefony s SIM kartou. Tato mobilní identifikace a digitální funkce ID karty jsou denně intenzivně využívány k přístupu k internetu, poskytují přístup k tisícům veřejných elektronických služeb a umožňují právně závazné digitální podpisy. K začátku roku 2021 se očekává, že celkový počet elektronických identifikací prostřednictvím estonského občanského průkazu a celkový počet digitálních podpisů poskytnutých obyvateli Estonska překročí hranici jedné miliardy. To poskytne komplexní přehled o estonském občanském průkazu a jeho digitálním systému. [16]

Zajímavým aspektem je, že během předčasného hlasování mají voliči možnost libovolně měnit svůj elektronický hlas, a každý nový hlas automaticky zruší předchozí. Odevzdání hlasu v tradiční volební místnosti v průběhu předčasného hlasování způsobí neplatnost elektronicky odevzdaného hlasovacího lístku. Tato opatření byla zavedena s cílem zajistit utajení hlasování: volič, který byl nějakým způsobem nucen nebo zastrašen, může odevzdat nový hlas a nahradit tak svůj předchozí výběr. Až do roku 2021 nebylo možné, aby elektroničtí voliči hlasovali v den voleb, protože jejich jména byla odstraněna ze seznamů voličů. Od roku 2021 mají tito voliči možnost odevzdat papírový hlasovací lístek v den voleb, což automaticky zneplatní jejich elektronický hlas. [11]

Estonská vláda vyjádřila plány na zavedení internetového hlasování v roce 2001. Zájem o tuto formu hlasování byl motivován nadějí na zvýšení účasti voličů, přilákání mladší generace k účasti ve volbách a zpříjemnění celého procesu hlasování. První legislativa umožňující hlasování přes internet byla přijata v roce 2002. Implementace internetového hlasování byla poté poprvé použita v komunálních volbách, které se konaly v říjnu 2005, kde tento nový způsob hlasování využilo 1,9 procent účastnících se voličů. Od té doby se podíl těchto voličů zvýšil na 50 procent. Mimo jiné možnost spojit digitální a fyzickou identitu pomocí identifikačních průkazů umožnila estonské vládě úplně přepracovat veřejné služby. Procesy, jako je žádost o dávky, vyplňování daňových přiznání nebo obnova řidičských průkazů, se staly dostupné pro lidi přímo z jejich domova, což nahradilo nutnost chodit na úřad.[11]

Velikým rozdílem oproti ČR či USA je také v tom, že elektronické správní postupy v Estonsku nejenže mají vysoké využití, ale také získaly vysokou důvěru veřejnosti. Průzkum z roku 2020 ukázal, že 82 procent obyvatel má důvěru v estonskou e-government a digitální služby. [17] A to i přes to, že proběhl bezpečnostní incident s občanskými průkazy v roce 2017. Tehdy bylo zjištěno, že čip v občanských průkazech, vyráběný společností Infineon, má bezpečnostní zranitelnost, která se

dotýkala přibližně 800 000 estonských občanských průkazů. Estonské úřady vyřešily tuto krizi vytvořením aktualizace softwaru, která umožnila obcházet tuto bezpečnostní zranitelnost. [11]

Estonsko si tedy na elektronickém hlasováním trvá a lidé mu věří. Rovněž má i poměrně dynamický vývoj. Zákony se připravovali již od roku 2002. Poprvé byl e-voting využit v roce 2005, během následujících skoro dvou dekád došlo k mnoha změnám v legislativě a technických aspektech internetového hlasování, které se vyvíjely prostřednictvím různých úprav a novelizací předpisů. Estonské soudy provedly zkoumání a potvrdily, že postupy týkající se internetového hlasování jsou v souladu s ústavou. Rozhodly, že právní předpisy o hlasování přes internet splňují ústavní požadavky na svobodné, všeobecné a tajné hlasování, které je součástí voleb. Nejvyšší soud Estonska v roce 2005 zjistil, že možnost změnit elektronický hlas během předčasných voleb je v souladu se zákony platné pro volby do Evropského parlamentu a neporušuje zásadu jednotnosti voleb. Soud dále zdůraznil, že tato možnost představuje další záruku pro svobodný výběr voličů. [11]

1.3.2 Technické zpracování internetového hlasování v Estonsku

Základní systém estonského internetového hlasování, známý pod označením protokol IVXV, je využíván od roku 2017 (viz obr. 1.12). Tento protokol je rovněž zveřejněn Estonskou vládou na GitHubu (`https://github.com/valimised/ivxv`), aby i veřejnost mohla sama vyhodnotit, zda-li je zdrojový kód v pořádku. [11]

- Volič zahajuje proces autentizace z hlasovací aplikace na svém počítači, která se připojuje k serveru Vote Collector (VC) prostřednictvím hlasovacího zařízení, které využívá elektronickou identitu (ID karta, MobileID).
- Server reaguje na požadavek s výpisem kandidátů L, který odpovídá volebnímu lístku volebního okrsku voliče.
- Volič vybere kandidáta své volby (cv), zašifruje svůj hlas pomocí veřejného klíče dešifrovacího serveru, podepíše ho a následně odesílá výsledek zpět na VC. Je důležité si všimnout, že veškerá šifrování jsou prováděna náhodně, což znamená, že hlasy udělené stejnému kandidátovi mají různé šifrování. Právě v tomto kroku se používá šifrovací náhodnost r za účelem zajištění toho, že VC nevyřadí náhodně nebo úmyslně žádné hlasy.
- Poté protokol přikazuje, aby hlas byl předán do samostatné registrační služby (RS).
- RS vrátí časové razítko (ts) s potvrzením, že hlas byl skutečně odevzdán mimo platformu VC. Následně má volič možnost provést individuální ověření svého hlasu. Tímto způsobem se zjistí dvě důležité věci. Za prve volič se může ujistit, že šifrovaný hlas odpovídá tomu, co zamýšlel a že nebyl náhodou změněn, na-

příklad škodlivým softwarem na jeho zařízení. Za druhé volič může kontrolovat časové razítko ts, aby potvrdil, že jeho hlas byl správně odeslán mimo VC, a tudíž nemůže být odstraněn VC bez jeho vědomí.

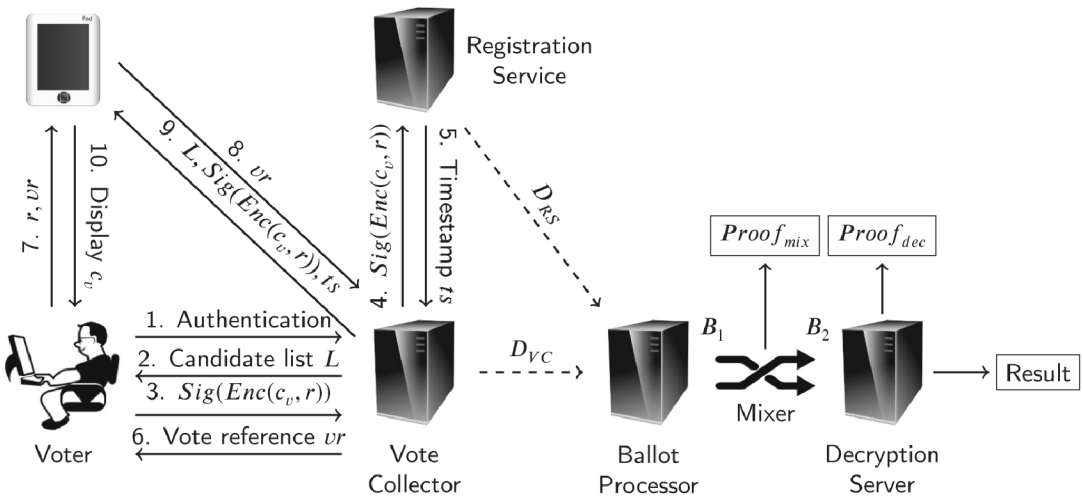
- Pro usnadnění ověřování VC poskytuje odkaz na hlasovací aplikaci vr. Cílem je zajistit, že ověřování probíhá nezávisle na počítači voliče, i když by byl napaden.
- Voličům je umožněno využít svá mobilní zařízení pro toto ověření. Mobilní zařízení komunikuje s VC pomocí optického kanálu blízkého dosahu, kterým je například QR-kód.
- Mobilní zařízení pošle dotaz na VC
- Následně obdrží šifrovaný a podepsaný hlas, seznam kandidátů L a časové razítko ts
- Nyní může mobilní zařízení prověřit časové razítko a podpis na hlasu, následně dešifrovat a zobrazit na obrazovce informace o kandidátovi. Volič provádí porovnání se svým původním záměrem a pokud jsou výsledky rozdílné, je vyvolán poplach nebo hlasování je opakováno.
- Po skončení doby hlasování jsou hlasovací lístky připraveny ke sčítání. Informace o hlasovacích sadách DVC a DRS, uložené v VC a registrační službě, jsou přeneseny bezdrátově do offline hlasovacího zařízení. Procesorová jednotka ověřuje časová razítka všech hlasů v DVS, odstraňuje všechny hlasy kromě posledních v DRS a vytváří seznam B1. Tento seznam je odeslán směšovači, vzniká tak seznam B2 spolu s kryptografickým důkazem správného míchání. Kryptografické údaje hlasů v seznamu B2 jsou nakonec dešifrovány pomocí soukromého klíče dešifrovacího serveru, čímž vznikne konečný výsledek a kryptografický důkaz správného zpracování.

Shrnutí

Elektronické hlasování v Estonsku představuje významný model pro zkoumání a implementaci moderních technologií do volebních procesů. Estonsko se stalo průkopníkem v oblasti internetového hlasování, nabízí inspiraci a příklady úspěšné integrace digitálních prostředků do volebního systému.

S jasným důrazem na digitální přístupnost, bezpečnost, transparentnost a vysokou účast voličů představuje estonský model několik klíčových prvků pro zvážení při zavádění elektronického hlasování i v jiných zemích. Je však důležité brát v úvahu i rizika a bezpečnostní opatření, jak ukázal bezpečnostní incident s občanskými průkazy v roce 2017.

Technické zpracování internetového hlasování v Estonsku, založené na protokolu IVXV poskytuje systematický a zabezpečený proces, který využívá šifrování, digi-



Obr. 1.12: Technické schéma elektronického hlasování v Estonku.

Obrázek byl převzat z [11]

tální podpisy a ověřitelné kroky pro zajištění důvěryhodnosti a správnosti hlasů.

Estonský přístup k elektronickému hlasování je významným studijním materiálem, který nabízí důležité ponaučení pro zavedení moderních technologií do volebních procesů po celém světě.

Hlavním zjištěním je, že během téměř dvaceti let se proces hlasování přes internet v Estonsku stal běžným a pevně zakotveným. Voličské orgány již nepovažují tuto praxi za experimentální: internetové hlasování je běžnou a nezbytnou součástí běžného rámce pro konání voleb. Vysoká míra využívání a silná důvěra voličů naznačují, že většina občanů sdílí toto hodnocení a stále více považuje hlasování přes internet za standardní postup. Tento postoj byl podpořen soudy a získal akceptaci mezinárodními organizacemi, které sledují volby a stav demokracie. Důvodů proč zrovna Estonsko dokázalo elektronické hlasování masově rozšířit je více. Například časování hrálo důležitou roli - Estonsko bylo průkopníkem v oblasti e-hlasování před tím, než kybernetické útoky a hackerské interference ve volbách se staly běžnými jevy. To znamená, že v době, kdy bylo elektronické hlasování přijímáno a vyvíjeno, nebyly tyto obavy a odpor výraznější. Dále v Estonsku zavedení a rozvoj internetového hlasování bylo součástí širšího úsilí o vytvoření digitálního státu - Estonsko si na tomto zakládá. Následně až na malé kauzy systém funguje a má velkou oblíbenost (až 50 procenty se již využívá u voleb). Dále se vláda a úřady zavázaly k neustálému zlepšování, rozvoji a aktualizaci technologických, právních a organizačních aspektů systému e-hlasování.

Celkově stojí za zmínku také fakt, že celková volební účast (tedy hlasování kla-

sické papírové + elektronické) se příliš nezměnila, v podstatě zůstává stejná, u některých voleb je větší (celonárodní atp.) a u některých nižší (EU volby) podobně jako u nás v ČR.

Tab. 1.3: Tabulka výhod elektronického hlasování v Estonsku.

Výhody
Přístupnost a pohodlí, Estonsko umožňuje všem voličům hlasovat online, což zvyšuje pohodlí a snižuje potřebu fyzické přítomnosti.
Umožňuje vzdálené hlasování z domova, což je obzvláště užitečné pro voliče žijící mimo Estonsko, což se týká zhruba až 20 procent Estonců.
Zrychlené sčítání hlasů a zveřejnění výsledků
Potencionální zvýšení účasti voličů.
Estonsko používá pokročilé technologie, včetně šifrování a bezpečných digitálních podpisů.
Transparentnost a auditovatelnost, estonský systém umožňuje voličům ověřit, že jejich hlas byl správně zaznamenán.
Estonci mají velikou důvěru v tento systém.

Tab. 1.4: Tabulka nevýhod elektronického hlasování v Estonsku.

Nevýhody
Bezpečnostní rizika, obavy z možných kybernetických útoků a manipulace s hlasovacími daty.
Výzvy spojené s důvěrou veřejnosti, nutnost budování a udržení důvěry veřejnosti v elektronický hlasovací systém.
Výzvy spojené s ověřením identity voličů a zajištěním, že každý hlas je jedinečný a autentický.
Závislost na technologické infrastruktuře, efektivní elektronické hlasování vyžaduje stabilní a bezpečnou internetovou infrastrukturu.
Důvěra veřejnosti, výzvy spojené s budováním a udržováním důvěry veřejnosti v elektronické hlasovací systémy.
Technické a operační výzvy, nutnost řešení technických výzev a zajištění bezproblémového provozu systému.
Výzvy spojené s přijetím a adaptací nových technologií mezi staršími voliči a těmi, kteří nejsou technologicky zdatní.

Klíčové rozdíly mezi estonským a americkým přístupem

- Přístupnost: Estonsko umožňuje všem voličům hlasovat online, zatímco v USA je elektronické hlasování často omezeno na specifické skupiny voličů, jako jsou vojáci sloužící v zahraničí a osoby s určitými zdravotními postiženími.
- Technologie a bezpečnost: Estonsko je známé využíváním pokročilých technologií, jako jsou bezpečné digitální podpisy a šifrování, což zajišťuje vysokou míru bezpečnosti a důvěry v elektronické hlasování. V USA jsou bezpečnostní opatření různorodá a závisí na konkrétním státu nebo jurisdikci.
- Centralizace vs. decentralizace: Estonský model je více centralizovaný, což umožňuje jednotný systém pro celou zemi. Americký systém je více decentralizovaný, s pravidly a systémy, které se liší stát od státu.
- Důvěra a veřejné vnímání: V Estonsku je vysoká míra důvěry ve veřejné digitální služby, včetně elektronického hlasování. V USA jsou obavy z bezpečnosti a důvěry v elektronické hlasování častější, což je důsledkem rozdílných historických zkušeností.
- Rozvoj digitální společnosti: Estonsko je považováno za jednu z nejpokročilejších digitálních společností na světě, kde je většina vládních služeb dostupná online. Tento rozvoj digitální společnosti podporuje širší přijetí a integraci elektronického hlasování. V USA, ačkoliv je digitální technologie rovněž rozšířená, neexistuje stejně integrovaný a všeobecně přijímaný systém pro elektronické hlasování na federální nebo státní úrovni.
- Zkušenosti s implementací: Estonsko má dlouholeté zkušenosti s provozováním elektronického hlasování (od roku 2005) a systém neustále zdokonaluje na základě zpětné vazby a technologického vývoje. V USA je situace proměnlivá, kde některé státy mohou mít zkušenosti s omezenými formami elektronického hlasování, zatímco jiné nemají žádnou praxi nebo systém na podporu široce dostupného elektronického hlasování. Estonsko tedy na rozdíl od USA své občany postupně na tuto volbu připravovalo a zároveň se snažilo o udržení důvěry v tento systém.

1.4 Elektronické hlasování v České republice

V dnešní době rychlého technologického vývoje a digitalizace ve všech sférách života se stává elektronické hlasování (e-voting) a rozvoj elektronické vlády (eGovernment) klíčovými tématy pro mnohé země, včetně České republiky. Tyto inovace mají potenciál významně zvýšit efektivitu a dostupnost veřejných služeb, zlepšit transparentnost a integritu volebních procesů a posílit participaci občanů na veřejném životě. Tento text se zaměřuje na analýzu současného stavu a výzev spojených s implementací elektronického hlasování v České republice, přičemž čerpá inspiraci z mezinárodních zkušeností a osvědčených postupů, zejména z USA a Estonska, dvou zemí, které se staly průkopníky v oblasti e-votingu.

Elektronické hlasování (koncepčně) v České republice prochází složitým vývojovým procesem, který je zatížen technickými, legislativními a bezpečnostními výzvami. Tyto výzvy vyplývají z nutnosti zajistit bezpečnost a integritu volebního procesu, ochranu soukromí voličů a odolnost vůči vnějším útokům. Zkušenosti z USA naznačují, že technologický pokrok a inovace jsou klíčem k úspěšné implementaci, zatímco estonský přístup ukazuje význam vysoké úrovně digitální důvěry a transparentnosti procesů. Česká republika, inspirována těmito modely, stojí před úkolem vytvořit robustní, ale flexibilní systém, který by umožnil elektronické hlasování z jakéhokoli místa s internetovým připojením.

V rámci širšího rámce elektronické vlády se Česká republika zaměřuje na rozvoj e-Government služeb, které usnadňují interakci mezi občany a veřejnou správou. Iniciativy jako Portál občana a eObčanka jsou příkladem snah o modernizaci a zjednodušení přístupu k veřejným službám, čímž se otevírá cesta k efektivnějšímu a transparentnějšímu veřejnému sektoru.

V textu se budu zabývat podrobnou analýzou konceptu elektronického hlasování v České republice, zkoumat jeho potenciál, omezení a možnosti pro budoucí rozvoj. Dále roli e-Governmentu ve zvyšování efektivity veřejné správy a posilování demokratického zapojení občanů. Cílem je poskytnout ucelený přehled o stávajícím stavu, výzvách a perspektivách elektronického hlasování a elektronické vlády v České republice, s důrazem na význam technologie, bezpečnosti, legislativy a veřejné důvěry v úspěšnou implementaci těchto moderních přístupů.

Na základě informací ze zemích co již elektronické hlasování přijalo, se zaměříme hlavně na USA a Estonsko. Od těchto zemí se můžeme inspirovat případně vyvarovat se z některých chyb.

Inspirace z USA

Technologický pokrok a inovace – ČR by měla investovat do vývoje a testování pokročilých technologických řešení pro elektronické hlasování, aby zabezpečila volební

proces. Zkušenosti USA ukazují, že technologická vyspělost je klíčem k efektivnímu a modernímu hlasovacímu systému. Zároveň politický systém musí udržovat důvěru v tento systém mezi svými občany. Tuto důvěru je nutné získat a pozitivně rozvíjet. Opatření pro zabezpečení a integritu – Podle amerického modelu je nutné prioritizovat bezpečnostní opatření a integritu volebního systému. To zahrnuje investice do šifrování, autentizace voličů a ochrany proti vnějším útokům. Omezení elektronického hlasování – USA aplikují elektronické hlasování primárně pro specifické skupiny voličů, jako jsou členové ozbrojených sil v zahraničí nebo osoby se zdravotním postižením. ČR by mohla zvážit podobný přístup jako pilotní projekt před plošným zavedením. Například otestovat ho na části populace, nikoliv celoplošně a vyhodnotit následně procesy. ČR by se měla vyvarovat rizik spojených s elektronickým hlasováním, které byly identifikovány v USA, včetně potenciálních hackerů, manipulace s hlasovacími daty a technických problémů. To znamená zavedení robustního a průběžně aktualizovaného bezpečnostního rámce. Zkušenosti s korespondenčním hlasováním – ČR by měla využít amerických zkušeností s korespondenčním hlasováním jako možný přechodný krok k plně elektronickému hlasování, zejména ve fázích, kdy se buduje důvěra veřejnosti v nový systém. Korespondenční hlasování se ukazuje jako takový předstupeň před elektronickým hlasováním.

Inspirace z Estonska

Celostátní přístup k elektronickému hlasování – Estonsko je příkladem země, která úspěšně implementovala elektronické hlasování na celostátní úrovni. ČR by se měla snažit o vytvoření podobně robustního, ale zároveň flexibilního systému, který by umožňoval hlasování z jakéhokoliv místa s internetovým připojením. Vysoká úroveň digitální důvěry – Estonský model ukazuje, jak je důležité vybudovat a udržet vysokou úroveň důvěry veřejnosti v elektronické hlasování a další digitální služby. Tento proces je pomalý a postupný a ČR by měla věnovat značné úsilí osvětě a transparentnosti procesů, aby zajistila veřejnou důvěru. Ověřitelnost a transparentnost je proto nezbytně nutná obdobně v Estonsku, kde jsou výsledky hlasování a systém transparentní a veřejně dostupné pro kontrolu, by i ČR měla zajistit, aby její systém elektronického hlasování byl plně ověřitelný a transparentní pro širikou veřejnost.

Příklady z USA a Estonska poukazují na potřebu pečlivé přípravy jak z technického, tak z legislativního hlediska.

1.5 Koncept elektronické hlasování v České republice

Koncept, který ukončil první fázi vývoje mechanismu online hlasování v České republice. Následující druhá fáze zahrnovala vývoj technické infrastruktury a konečná

třetí fáze se zaměřovala na vytvoření legislativy. Informace jsou veřejně dostupné jako výsledek druhé fáze. Na druhou stranu tento koncept (hlavní výsledek první fáze) není veřejně dostupný. [18]

Informace obsahovaly plán nasazení online hlasování v České republice. Pilotní projekt byl plánován na rok 2015 s prvním použitím online hlasování plánovaným na rok 2016 ve volbách do Senátu ve dvou obvodech.

Česká vláda uznala existenci těchto informací. Nicméně informace byly explicitně požadovány vládou a nebyly připraveny pouze k uznání. Informace také požadovaly rozhodnutí, zda pokračovat jednou ze tří možností. Vláda měla rozhodnout, zda nepokračovat dále v online hlasování nebo připravit pilotní projekt v roce 2015 a přiřadit úkol organizace pilotního projektu ministerstvu vnitra nebo nepokračovat dále v online hlasování, ale vyvíjet volební infrastrukturu pro budoucí nasazení online hlasování. [18]

Nicméně úplně k prvotním pokusům o elektronickém hlasování se již pokoušelo více předchozích vlád. V roce 2008 došlo k uzavření dohody o spolupráci mezi Ministerstvem vnitra a Českým statistickým úřadem, která zahrnovala plán na implementaci elektronických voleb. Jan Fischer, který byl tehdy předsedou Českého statistického úřadu, vyjádřil názor, že první elektronické volby by mohly být uskutečněny v roce 2014 (k tomuto nedošlo). Další vláda v roce 2012, avšak k této otázce nepřistoupila jako k prioritě. Výsledkem bylo, že nebylo učiněno žádné rozhodnutí ohledně dalšího postupu. Tento postoj byl překvapující. Vláda, která pouze uznala tyto informace, dříve dala online hlasování prioritu ve své Koaliční dohodě z roku 2010 (koalice ODS + TOP 09 + Věci veřejné). Koaliční dohoda stanovila cíl „Zahájíme přípravu projektu elektronických voleb tak, aby mohl být pilotně realizován ve volebním roce 2012 a plnohodnotně zaveden od voleb do Poslanecké sněmovny PČR v roce 2014.“ [19] Plán uvedený v těchto informacích již byl v porovnání s časovým plánem Koaliční dohody zpožděný. Nicméně to nevedlo vládu k aktivnějšímu postoji. Rovněž bylo přijato usnesení ze dne 14. března 2012 zadávající úkol ministrovi vnitra o podání podrobných informací o elektronickém hlasování a předložit návrh volebního zákoníku. [20] Informace nastínila základní principy zamýšleného mechanismu online hlasování. Online hlasování by mělo: [21]

- Být alternativou k tradičnímu hlasování
- Být ve formě vzdáleného online hlasování
- Být realizováno jako hlasování přes internet
- Umožňovat voličům hlasovat opakovaně, sčítat pouze poslední odevzdaný hlas
- Zajistit tajnost hlasu a zabránit možnosti odevzdat dva hlasy
- Zajistit, že třetí osoba a žádný orgán volby nemohou zjistit, jak volič hlasoval
- Zajistit, že hlas nemůže být nezjištěně změněn
- Umožňovat vysokou úroveň bezpečnosti pro identifikaci a ověření voliče

- Umožňovat určení, zda byly všechny platné hlasy správně sečteny
- Sdílet informace o tom, jak systém pracuje veřejně

Hlasy v online hlasování měly být odeslány prostřednictvím Informačního systému Datových schránek. Měla být vytvořena zvláštní datová schránka s názvem Volební datová schránka, která by byla přidělena jednotlivým voličům za účelem zajištění tajnosti hlasu. Nicméně po změně vlády v roce 2014 nebyl pokus o implementaci online hlasování dále realizován. Od této doby myšlenka online hlasování v České republice byla upozaděna. V roce 2019 byl předložen návrh zákona o správě voleb, ze kterého plyne, že s elektronickým hlasování se nepočítá. I když návrh nebyl schválen, byl znovu předložen vládou v roce 2022. Jeho odůvodňující memorandum dochází k podobnému závěru. [22] [23] V letech 2020 a 2021 byly volby ovlivněny covid-19 onemocněním. Byla zavedena možnost odevzdat hlas v drive-in režimu, aby se umožnila účast voličů v karanténě způsobené infekcí covid-19. Tímto způsobem teoreticky může dojít k oslabení výrazně konzervativního přístupu k volbám v České republice. Nicméně online hlasování je pravděpodobně stále velmi vzdálenou možností.[18]

V současné době se v České republice hovoří o zavedení korespondenčního hlasování, tedy hlasování dopisem. Což by mohlo být jakýmsi předvojem elektronického hlasování přes internet. První pokusy probíhali již v roce 2015, kdy Marek Ženíšek, místopředseda TOP 09, navrhl v zavedení korespondenční volby [24]. Nicméně korespondenční hlasování je součástí také v programovém prohlášení současné vlády. Protože zákon, který by měl změnit organizaci voleb, má ústavní povahu, vyžaduje jeho schválení podporu alespoň 120 poslanců, což zahrnuje i ty z opoziční strany. A opozici se tento zákon příliš nezamlouvá. [25] [26] [27]

1.5.1 Relevantní legislativa v České republice

Volební zákon je právní norma, která řídí proces volby. Stanovuje pravidla pro aktivní a pasivní volební právo, jejich podmínky, organizaci voleb, počítání hlasů, oznámení výsledků a možnost soudního přezkumu. V České republice je pro přijetí volebního zákona vyžadován souhlas obou komor Parlamentu - Poslanecké sněmovny i Senátu, přičemž Senát nemůže být přehlasován, ale také sám nemůže schválit zákon. V minulosti se předpokládalo, že volební zákony se týkají jen parlamentních voleb, ale Ústavní soud rozhodl, že se týkají i dalších typů voleb, jako jsou komunální volby, krajské volby či volby do Evropského parlamentu. Seznam českých volebních zákonů:

- Č. 247/1995 Sb. – Zákon o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů

- Č. 130/2000 Sb. – Zákon o volbách do zastupitelstev krajů a o změně některých zákonů
- Č. 491/2001 Sb. – Zákon o volbách do zastupitelstev obcí a o změně některých zákonů
- Č. 62/2003 Sb. – Zákon o volbách do Evropského parlamentu a o změně některých zákonů
- Č. 275/2012 Sb. – Zákon o volbě prezidenta a o změně některých zákonů

Ve všech těchto zákonech není zmínka ani o elektronickém hlasování ani o korespondenční volbě. Volič si pouze může vyřídit tzv. voličský průkaz (a to ve všech typů voleb, kromě voleb do zastupitelstev obcí), volební průkaz umožňuje voličům hlasovat v jiném volebním okrsku, než je jejich trvalé bydliště. To je praktické zejména pro ty, kteří se v době voleb nacházejí mimo místo svého bydliště, například kvůli práci, studiu nebo dovolené. Volební průkaz tedy zajišťuje, že voliči nemusí zmeškat svoji možnost účastnit se voleb, pokud nejsou fyzicky přítomni ve svém obvyklém volebním okrsku – nicméně bod, že stále musí jít fyzicky k volbám zůstává.

Dalším pro nás relevantním zákonem je zákon o elektronické identifikaci (č. 250/2017 Sb.) konkretně upravuje následující klíčové body:

- Využití elektronické identifikace: Zákon stanovuje pravidla pro používání elektronické identifikace pro prokazování totožnosti podle právních předpisů nebo výkonu působnosti, což je možné jen prostřednictvím kvalifikovaného systému elektronické identifikace.
- Působnost Agentury: Zákon specifikuje roli Digitální a informační agentury (Agentura), která má působnost v oblasti elektronické identifikace, včetně udělování akreditací správcům systémů a dohled nad jejich činností.
- Akreditace: Stanovuje podmínky pro získání akreditace pro správu kvalifikovaného systému elektronické identifikace, včetně technických specifikací, bezúhonnosti, pojištění odpovědnosti a schopnosti poskytnout služby národního bodu pro identifikaci a autentizaci.
- Národní bod: Ustanovuje „národní bod“ jako klíčovou složku systému, který podporuje proces elektronické identifikace a autentizace. Správce národního bodu musí zajistit, že systém splňuje všechny stanovené technické a operativní požadavky.
- Právní následky nesplnění povinností: Zákon také definuje, jaké právní důsledky nastanou v případě, že akreditované osoby neplní své povinnosti, včetně možnosti udělení pokut a odnětí akreditace.

Explicitně o elektronickém hlasování zde není zmínka, nicméně implementace tohoto zákona do systému elektronického hlasování by mohla zahrnovat vytvoření bezpečného a kvalifikovaného systému elektronické identifikace, který by byl použit k verifikaci totožnosti voličů. Tento systém by musel splňovat všechny technické

specifikace a normy stanovené příslušnými právními předpisy EU. Voliči by se museli prokazovat prostřednictvím tohoto systému před samotným hlasováním, čímž by byla zajištěna jejich jednoznačná a ověřitelná identifikace.

Dalším důležitým dokumentem, je pro Českou republiku (obdobně jako u Estonska) doporučení rady Evropy CM/Rec(2017)5, které vydal Výbor ministrů členským státům o standardech pro elektronické hlasování, zdůrazňuje význam dodržování demokratických zásad v elektronických hlasovacích systémech. Některé klíčové body z dokumentu: [13]

- Všeobecné a rovné volební právo: Systémy elektronického hlasování by měly být přístupné a použitelné pro všechny voliče, včetně osob se zdravotním postižením, měly by zajistit, aby každý volič mohl bezpečně hlasovat pouze jednou.
- Svobodné a tajné volební právo: Elektronické hlasování musí zajistit, aby se úmysl voliče nezměnil, aby byla zachována tajnost hlasů po celou dobu hlasování a aby si voliči mohli ověřit, že hlasovali tak, jak zamýšleli, aniž by poskytli třetím stranám prostředky k prokázání obsahu hlasování.
- Spolehlivost a bezpečnost: Systémy by měly být odolné proti selháním a útokům a měly by být vybaveny opatřeními, jako je šifrování, která chrání data. K zajištění trvalého souladu se standardy jsou nutné pravidelné aktualizace a audity.
- Transparentnost a pozorování: Proces elektronického hlasování by měl být transparentní s ustanoveními pro pozorovatele a jasnými informacemi pro veřejnost o fungování systémů a jejich použití ve volbách.
- Regulační a organizační požadavky: Členské státy by měly zavádět elektronické hlasování opatrně s vhodnými právními rámci a kontrolou ze strany orgánů pro řízení voleb, aby bylo zajištěno dodržování demokratických zásad.
- Odpovědnost: Státy musí vypracovat, vyhodnocovat a pravidelně aktualizovat technické a certifikační standardy tak, aby odrážely demokratické zásady. Nezávislé orgány by měly certifikovat soulad systémů elektronického hlasování.

Národní identitní autorita

Národní bod pro identifikaci a autentizaci, provozovaný českým státem, je informační systém veřejné správy, který umožňuje elektronickou identifikaci a autentizaci pomocí kvalifikovaného systému. Tento systém slouží k bezpečnému a spolehlivému ověřování totožnosti uživatelů na dálku. Zákon č. 250/2017 Sb. o elektronické identifikaci stanoví definici a pravidla pro Národní bod, jehož správcem je Správa základních registrů. Poskytovatelé služeb tohoto bodu jsou kvalifikované systémy elektronické identifikace, které jsou spravovány akreditovanými subjekty. Tyto systémy operují jako uzly podle nařízení Evropské unie č. 910/2014 eIDAS. Pro eGovernment

služby, které poskytuje zejména veřejná správa, je nutné získat určité údaje pro identifikaci uživatelů v jejich systémech, což se děje automaticky z registru obyvatel s výhradou souhlasu uživatele během přihlašovacího procesu.

1.5.2 eGovernment a Portál občana

Obecně eGovernment je zkratkou z angličtiny pro electronic government - elektronická vláda. Jedná se o digitální interakci, ve které se veřejná správa nějakým způsobem angažuje. Je zde kladen důraz na využívání informačních a komunikačních technologií a elektronických systémů pro poskytování a zlepšování služeb veřejné správy a interakce mezi vládou a občany, podniky a dalšími entitami. Cílem eGovernmentu je zvýšit efektivitu a transparentnost veřejné správy, usnadnit občanům a firmám přístup k informacím a službám a zjednodušit administrativní postupy. E-Government může zahrnovat různé aspekty, včetně online vládních webových stránek, digitálního zpracování dokumentů a dalších technologií, které pomáhají modernizovat a zefektivnit veřejnou správu. Jedním z prostředků v rámci moderního e-Governmentu je využití aplikace e-občanky a Portálu občana.[18]

Možnosti zabezpečených služeb e-Governmentu jsou dostupné pro občany skrze různé platformy, jako je například Portál občana, kde se prokážou svou identitou za použití elektronického ověření (například elektronického občanského průkazu, obdobně jako je možné volit v Estonsku).

Občanský průkaz s aktivovaným čipem – eObčanka

Od 1. 7. 2018 dostávají všichni občané České republiky občanské průkazy s čitelnými údaji pro stroje a s elektronickým čipem. [28] Do 30. 6. 2018 bylo možné na občanský průkaz s čipem nahrát pouze kvalifikované certifikáty pro elektronický podpis a autentizační certifikáty. Na rozdíl od toho eObčanka umožňuje ověření identity uživatele na propojených portálech veřejné správy. Dobrovolnou výměnu starého občanského průkazu za novou eObčanku má možnost každý zažádat bezplatně. [29] V rámci e-občanky hraje klíčovou roli elektronická identifikace. Tato forma identifikace je nedílnou součástí transformace veřejné správy směrem k digitalizaci, s cílem ulehčit občanům i celé veřejné správě čas i finanční prostředky. Koncepce digitalizace usiluje o možnost, aby občané mohli vyřizovat mnoho záležitostí online, eliminujíc tak potřebu fyzické návštěvy úřadu.

Elektronická identifikace zahrnuje proces využívání osobních identifikačních údajů ve formě elektronického záznamu, které slouží k unikátní identifikaci konkrétní fyzické nebo právnické osoby nebo fyzické osoby zastupující právnický subjekt. Tento

postup zajišťuje bezpečné a jednoznačné elektronické ověření identity osoby. Elektronická identifikace se uplatňuje například při přihlašování do elektronického bankovnictví nebo k online službám poskytovaným úřady. V České republice jsou státem zaručené prostředky pro elektronickou identifikaci, mezi něž patří e-občanka a také metody jako Jméno, heslo a SMS. [30]

Osoba, která vlastní eObčanku, má možnost přihlašovat se do online služeb a portálů, zvláště těch, které jsou poskytovány veřejnou správou, a tím využívat nabízené služby z domova. Například živnostník (OSVČ) může pohodlně a rychle komunikovat se správou sociálního zabezpečení a předejít trestům z prodlení při pozdní platbě pojistného, což úřad neinformuje prostřednictvím telefonních hovorů. [30]

Aby bylo možné se přihlašovat do Portálu občana, je nezbytné povolit funkci elektronické identifikace u občanského průkazu (výchozím nastavením je, že tato možnost není aktivovaná, ale je možné ji zapnout při vydání nového občanského průkazu nebo kdykoliv později).

Tento občanský průkaz, by se tedy obdobně jako například v Estonsku mohl využívat pro případné elektronické hlasování.

Portál občana

Portál občana představuje část Portálu veřejné správy, která umožňuje přístup k elektronickým službám poskytovaným státem. Do provozu byl zaveden 8. 7. 2018. Při svém debutu v roce 2018 měl Portál v nabídce jen 38 různých služeb, ale dnes otevírá přístup ke 600 službám. Současně došlo k významnému nárůstu uživatelů – jejich počet stoupl z 30 tisíc na téměř 1 milión. Počet vlastníků datových schránek dosáhl 1,37 milionu a počet držitelů eIdentity vzrostl na 4,3 milionů. Celkový počet přihlášení k 31.12.2022 (od spuštění Identity občana) je 33 333 900 (a z toho jen za rok 2022 je 20 705 413) [31] [32] [33] Tento prostor je určený pro osobní použití občanem ve vztahu k službám veřejných institucí. Poskytuje možnost kompletního elektronického podání, získání výstupů z informačních systémů veřejné správy, informace o průběhu konkrétních kroků provedených občanem u jednotlivých veřejných institucí a také například osobní archiv dokumentů. Občané mohou vstoupit do Portálu občana přes ověřenou elektronickou identitu, jako je například e-občanka, datová schránka nebo jednorázové heslo. To lze provést samostatně (pomocí počítače, tabletu nebo mobilního zařízení) nebo prostřednictvím kontaktních míst veřejné správy. [30] Portál občana je tedy webová platforma, která funguje jako vstupní brána a navigace pro občany k online službám poskytovaným státem. Po přihlášení a prokázání své identity, získá uživatel přístup do personalizované sekce Portálu veřejné správy, nazývané Portál občana. Zde může spravovat svůj osobní profil, komunikovat s veřejnou správou prostřednictvím datové schránky a využívat dostupné

online služby veřejné správy. Tento portál slučuje služby webových aplikací úřadů veřejné správy, propojuje různé prvky e-Governmentu (například eIdentitu, datové schránky, Czech POINT a další) a zahrnuje přehled informací uchovávaných státem v základních registrech. Zároveň umožňuje občanům žádat o přístup k těmto datům. Díky propojení základních registrů se systémy jako datové schránky nebo Czech POINT má každý občan neustálý přehled o informacích, které o něm jsou v registrech uloženy a také o tom, kdo, kdy a za jakým účelem tyto informace využívá. [30]

Vybrané služby, které Portál občana umožňuje: [34]

- Založení datové schránky (fyzické nebo podnikající fyzické osoby)
- Přidání datové schránky (fyzické nebo podnikající fyzické osoby)
- Žádost o nový řidičský průkaz z důvodu konce platnosti
- Potvrzení o studiu
- Výpis bodového hodnocení řidiče
- Výpis z Rejstříku trestů
- Výpis z živnostenského rejstříku
- Informace z katastru nemovitostí
- Informace z registru silničních vozidel
- Informace z registru řidičů
- Informace z živnostenského rejstříku
- Přístup k podání daňového přiznání na portálu MOJE daně
- Přístup k eReceptu
- Přístup do ePortálu ČSSZ pro informace o pracovní neschopnosti
- Přístup do ePortálu ČSSZ pro přehled o důchodovém pojištění
- Přístup do portálu Úřadu práce a jeho službám
- A mnohé další

Portál občana v době psaní této práce prochází kompletním redesignem.

1.5.3 Další služby eGovernmentu v České republice

Jedním z nejrychleji se rozvíjejících oblastí e-governmentu je regionální samospráva. Překvapivě však zároveň jde o oblast, kde legislativa ukazuje významné nedostatky s ohledem na budoucí rozvoj. Dvě největší města podle počtu obyvatel v České republice, tedy Praha a Brno, nabízejí nejširší škálu služeb prostřednictvím svých platforem.[18]

Portál Pražana

Systém eGovermentu, který je využíván na území Praze. Umožňuje přihlášení prostřednictvím elektronického nebo bankovního identifikátoru nebo datové schránky

(není nutné být občanem Prahy pro přihlášení). Hlavně se zaměřuje na otázky samosprávy a umožňuje platbu za svoz odpadu a poplatky za vlastnictví psa, podání různých formulářů, rezervaci schůzky s úředníkem nebo správu parkovacích povolení. Portál stále prochází dalším vývojem, přičemž se pracuje na různých dalších službách, jako je specifický modul pro podnikatele, pronájem městských bytů nebo dotace pro samosprávu.[18]

Brno iD

Systém elektronické vlády, který se používá v Brně. BrnoiD nabízí podobné služby po registraci. Například umožňuje občanům platit poplatek za svoz odpadu, spravovat parkovací povolení nebo obnovovat nájemní smlouvy na hroby na městském hřbitově. Navíc umožňuje správu dlouhodobých jízdenek ve veřejné dopravě (jelikož město Brno vlastní dopravní společnost) nebo spravovat účet v městské knihovně Knihovna Jiřího Mahena.[18]

Služby regionální samosprávy postupně získávají na popularitě a rozvíjejí se i v dalších městech a obcích. Nicméně rozvoj je vždy vázán na dostupné financování a dosažení kritického počtu uživatelů, aby mohly být poskytovány přínosné služby. V důsledku toho mají velká města lepší výchozí pozici. Avšak stávající legislativa prokazuje vážné nedostatky a může nakonec omezit snahu samospráv rozvíjet své e-Government platformy a služby dále. Například pro elektronický formulář poskytovaný samosprávou k přístupu k datům základních registrů musí samosprávný orgán požádat Ministerstvo vnitra, aby zaregistrovalo příslušnou digitální službu v Katalogu služeb (jako součásti Rejstříku práv a povinností). Ministerstvo však zaregistruje orgán (a službu poskytovanou jím) pouze tehdy, pokud konkrétní právní ustanovení požaduje takovou činnost. Toto omezení představuje závažný problém, protože většina digitálních služeb poskytovaných samosprávami není poskytována kvůli zákonem nařízené povinnosti, ale proto, že je přátelská k občanům a rozumná.[18]

1.6 Zabezpečení hlasovacích údajů

1.6.1 Kryptografické závazky

Kryptografické závazky jsou důležitým konceptem v kryptografii, který umožňuje odesílateli (Sender) skrýt zvolenou hodnotu, zatímco zároveň garantuje příjemci (Receiver) neměnnost této hodnoty během trvání protokolu. Tato funkce má dvě základní vlastnosti:

- Skrytí (Hiding): Tato vlastnost zaručuje, že odesílatel může předat tajnou hodnotu příjemci, aniž by byl obsah této hodnoty příjemci odhalen. Potenciálně v našem případě předání „hodnoty“ elektronického hlasu do databáze.
- Svázání (Binding): Díky této vlastnosti je odesílatel pevně svázán s tajnou hodnotou předanou příjemci, což mu brání v hodnotu měnit během trvání protokolu.

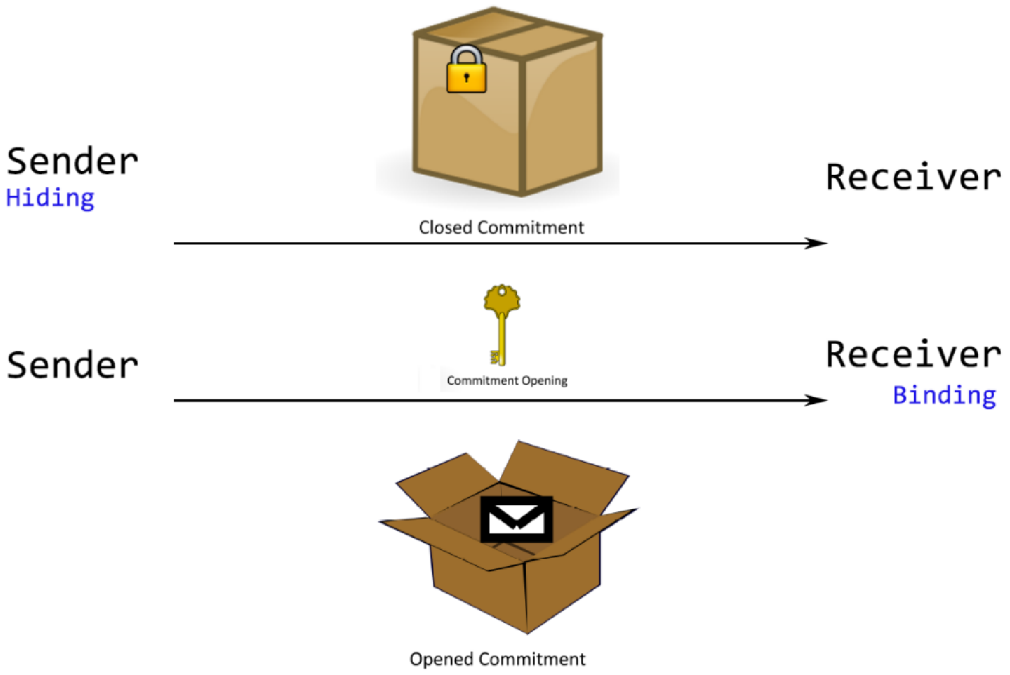
Kryptografické závazky mohou být použity k zajištění integrity a anonymního hlasování v elektronickém hlasování. Odesílatel (v tomto případě volič) může zaslat svůj hlas jako kryptografický závazek, který zajistí, že až do momentu odhalení (konec hlasovacího období) nebude možné zjistit, jaký byl hlas odevzdán, ale zároveň bude garantováno, že volič nemůže svůj hlas změnit.

Jednoduchým příkladem pro pochopení principu kryptografických závazků je princip uzamčené krabice s tajným dopisem, kde odesílatel nemůže změnit obsah tajného dopisu, jakmile je krabice v držení příjemce, a příjemce nemůže zjistit obsah dopisu, dokud mu odesílatel neposkytne klíč k odemčení krabice. Viz 1.13. Tento princip lze aplikovat na proces hlasování tak, že volič vloží svůj hlas do „digitální krabice“, která je uzamčena kryptografickým závazkem. Toto zajistí, že voličův hlas zůstane tajný až do momentu sčítání hlasů.

Kryptografické závazky lze formalizovat pomocí závazkových schémat, která se skládají z fáze svázání, kde odesílatel generuje závazek na svou hodnotu a posílá jej příjemci, a fáze odhalení, kde odesílatel odhaluje původní hodnotu příjemci, který pak může ověřit, že závazek odpovídá odhalené hodnotě.

Existují různé typy závazkových schémat, například DL závazkové schéma, založené na problému diskrétního logaritmu, které je charakterizováno jako perfektně svazující a výpočetně skrývající, což znamená, že je nemožné nalézt jinou hodnotu, která by generovala stejný závazek, a zároveň je v současní době (se současnými výpočetními možnostmi) výpočetně nerealizovatelné zjistit jakékoli informace o skryté hodnotě z závazku.

Závazková schémata hrají klíčovou roli v různých kryptografických protokolech, včetně protokolů s nulovou znalostí a důkazů znalosti, kde umožňují uživatelům prokázat znalost určitých informací, aniž by je museli přímo odhalit. Tato vlastnost



Obr. 1.13: Princip uzamčené krabice.

Obrázek byl převzat z [37]

je zásadní pro zachování soukromí a zabezpečení v digitálním světě.

Úrovně vlastností kryptografických závazků

- Perfektní (Perfect) Bezpečnost: V kontextu kryptografických závazků znamená perfektní bezpečnost, že prolomení vlastnosti (buď skrytí nebo svázání) není možné žádným algoritmem, ani kdyby útočník měl neomezený výpočetní výkon. To znamená, že bezpečnost schématu je absolutní a nezávisí na jakýchkoli předpokladech o výpočetní složitosti problémů.
- Statistická (Statistical) Bezpečnost: Tato úroveň bezpečnosti znamená, že existuje pouze zanedbatelná pravděpodobnost úspěšného prolomení vlastnosti schématu, i když útočník disponuje neomezeným výpočetním výkonem. Statistická bezpečnost poskytuje velmi vysokou míru jistoty, že závazek je bezpečný, avšak ne absolutní jistotu jako v případě perfektní bezpečnosti.
- Výpočetní (Computational) Bezpečnost: Výpočetní bezpečnost znamená, že prolomení vlastnosti schématu je nepraktické s ohledem na současný výpočetní výkon a známé algoritmy. To obvykle znamená, že bezpečnost závazku je založena na předpokladech o výpočetní složitosti určitých matematických problémů, jako je problém faktorizace velkých čísel nebo problém diskrétního

logaritmu. I když tato úroveň bezpečnosti není absolutní, v praxi poskytuje dostatečnou ochranu vzhledem k současným technologiím a očekávanému vývoji v dohledné budoucnosti.

Je důležité poznamenat, že obě vlastnosti kryptografických závazků – skrytí a svázání – nemohou být současně na úrovni perfektní bezpečnosti. Pokud jedna vlastnost poskytuje perfektní úroveň bezpečnosti, druhá musí být na úrovni výpočetní, aby bylo schéma prakticky použitelné. Tato omezení vycházejí z fundamentálních teoretických principů kryptografie.

1.6.2 Anonymní atributová pověření

Ochrana soukromí uživatelů je klíčová z několika důvodů, například pro zachování jejich práv a svobody v digitálním prostředí, pro zajištění důvěry v digitální služby, a pro splnění právních a etických norem. Mezi hlavní body patří:

- Zvýšený důraz uživatelů na ochranu soukromí: V současné době je zřejmý rostoucí požadavek uživatelů na ochranu jejich soukromí, což se odráží ve veřejných a regulatorních iniciativách, jako je GDPR v Evropě, které požadují „privacy-by-design“ a „privacy-by-default“ přístupy. [38]
- Regulační požadavky a standardy: Existence a vývoj regulačních norem, jako je GDPR, naznačuje, jak je ochrana soukromí brána vážně na institucionální úrovni a jak je důležité pro organizace dodržovat tyto normy pro zajištění právního souladu a ochrany svých uživatelů.
- Agentura Evropské unie pro kybernetickou bezpečnost, známá jako ENISA (European Union Agency for Cybersecurity), se věnuje technologiím pro ochranu soukromí uživatelů. ENISA jmenuje i některé PETs (Privacy-Enhancing Technologies, technologie pro podporu soukromí) - jako jsou šifrování, protokoly pro anonymní komunikaci či soukromé prohledávání databází. [39]
  Anonymní atributová pověření v kotenxtu elektronického hlasování mohou být využita pro autentizaci voličů bez nutnosti odhalení jejich identity. Voliči by mohli prokázat vlastnictví určitých atributů (např. občanství, věk) potřebných k hlasování, aniž by museli odhalit svou plnou identitu. Tím by se zajistila anonymita hlasování a ochránilo soukromí voličů.

Privacy-Enhancing Technologies (PETs)

PETs jsou navrženy tak, aby rozšířily standardní bezpečnostní funkce a zajistily vyšší úroveň ochrany soukromí a bezpečnosti pro uživatele. Tyto technologie se zaměřují na minimalizaci osobních dat potřebných pro splnění požadované funkcionality a zároveň maximalizují ochranu těchto dat. Mezi standardní bezpečnostní funkce, které PETs rozšiřují, patří:

- Integrita: Zajištění, že data nebyla neoprávněně změněna nebo poškozena.
- Utajení: Ochrana před neoprávněným přístupem k informacím, zajistit, že data jsou přístupná pouze autorizovaným stranám.
- Autentičnost: Ověření identity uživatele nebo zařízení, které se snaží přistupovat k systému nebo provádět operace, a zajištění, že jsou, kým tvrdí, že jsou.
- Nepopiratelnost: Zabránění subjektu v popření vykonání akce, jako je odeslání zprávy nebo provedení transakce, což umožňuje důvěryhodnou výměnu informací.

PETs přidávají další klíčové vlastnosti pro zvýšení ochrany soukromí:

- Anonymita (Anonymity): Umožňuje uživatelům provádět akce nebo komunikovat bez odhalení jejich identity.
- Nespojitelnost (Unlinkability): Zajištění, že dvě nebo více akcí provedených stejným uživatelem nebo objektem nelze spojit dohromady, čímž se chrání soukromí uživatelů tím, že se ztěžuje sledování jejich činnosti.
- Nesledovatelnost (Untraceability): Zajišťuje, že akce nebo komunikace nemůže být sledována zpět k uživateli, čímž se chrání jeho identita a aktivity před neoprávněným sledováním.

PETs jsou často založeny na pokročilých kryptografických protokolech a algoritmech, jako jsou asymetrická kryptografie, protokoly pro anonymní autentizaci, blind signatures (zaslepené podpisy), group signatures (skupinové podpisy) a zero-knowledge proofs (důkazy bez odhalení znalostí). Tyto technologie jsou navrženy tak, aby zajišťovaly, že digitální operace a transakce mohou být provedeny s minimálním odhalením osobních informací a přitom stále zachovávaly nezbytné úrovně bezpečnosti a důvěry

V kontextu elektronického hlasování mohou být použity k zabezpečení komunikace mezi voličem a hlasovacím serverem. PETs by zajistily, že preference voliče zůstanou soukromé a že hlasování nemůže být spojeno s konkrétním voličem, čímž se zvýší důvěra ve volební systém.

Přístupy k autentizaci

Přístupy k autentizaci se liší podle toho, jaký typ důkazu je vyžadován k ověření identity uživatele. Základní princip spočívá v tom, že uživatel musí prokázat svou identitu poskytnutím něčeho, co zná, má, nebo jím je. Toto rozdělení do tří hlavních kategorií vám poskytuje široký přehled o různých metodách, které mohou být použity k autentizaci. Podívejme se na tyto přístupy podrobněji: [40]

- Něco, co uživatel zná (Something the user knows): Tato kategorie zahrnuje všechny typy informací, které musí uživatel znát a které může při autentizač-

ním procesu poskytnout. Typickým příkladem je heslo, PIN kód, nebo tajná fráze. Tento přístup je široce používán, ale může být zranitelný vůči útokům, jako je odposlech nebo sociální inženýrství.

- Něco, co uživatel má (Something the user has): Tato metoda vyžaduje, aby uživatel měl fyzický předmět, který slouží jako důkaz jeho identity. Příklady zahrnují bezpečnostní tokeny, smart karty, mobilní telefony (používající SMS nebo aplikace generující jednorázové přihlašovací kódy) nebo jiné zařízení. Tento přístup je obecně bezpečnější, protože zneužití vyžaduje fyzický přístup k autentizačnímu zařízení.
- Něco, co uživatel je (Something the user is): Tato metoda, známá také jako biometrická autentizace, využívá jedinečné fyzické nebo behaviorální charakteristiky uživatele, jako jsou otisky prstů, rozpoznání obličeje, hlasová biometrie nebo dynamika psaní na klávesnici. Biometrická autentizace nabízí vysokou míru bezpečnosti, protože biometrické charakteristiky jsou těžko napodobitelné nebo ukradené. Nicméně, tato metoda také vyvolává otázky týkající se soukromí a potřebuje silné ochranné mechanismy pro uchování biometrických dat.

V praxi jsou často nejefektivnější kombinované metody, známé jako vícefaktorová autentizace (MFA), které vyžadují více než jednu formu důkazu k ověření identity. MFA kombinuje dva nebo více z výše uvedených přístupů, například něco, co uživatel zná (heslo), a něco, co má (mobilní telefon). Tím se výrazně zvyšuje bezpečnost autentizačního procesu, protože útočník musí kompromitovat více nezávislých faktorů, aby získal přístup.

MFA by mohla být v kontextu elektronického hlasování použita k zajištění, že osoby hlasující v systému elektronického hlasování jsou skutečně oprávnění voliči. MFA by využívala kombinace něčeho, co volič zná (heslo, id), má (bezpečnostní token nebo mobilní telefon) a případně (biometrické údaje), aby se minimalizovala rizika neautorizovaného přístupu.

Autentizace na základě identity

Autentizace na základě identity se zaměřuje na ověření totožnosti subjektu pomocí jeho jednoznačné identity, obvykle v podobě uživatelského jména nebo jiného jednoznačného identifikátoru (i například X.509 certifikát). Při tomto přístupu se obvykle používá kombinace uživatelského jména a hesla, přičemž heslo slouží jako tajný klíč, který pouze daný uživatel zná. Autentizace na základě identity může také zahrnovat použití digitálních certifikátů nebo veřejných klíčů, které jsou asociovány s konkrétním uživatelským jménem nebo identitou. Hlavní nevýhodou je, že identita uživatele je vždy odhalena během procesu autentizace, což může být nežádoucí v situacích,

kdy je požadována anonymita. Další nevýhodou je, že všechny transakce mohou být vzájemně spojitelné, což umožňuje sledování aktivit uživatele.

Autentizace na základě atributů

Autentizace na základě atributů je flexibilnější přístup, který umožňuje uživatelům prokázat svou oprávněnost k přístupu k zdrojům nebo službám na základě vlastnictví určitých atributů nebo vlastností, aniž by museli odhalit svou plnou identitu. Atributy mohou být různé charakteristiky, jako je věk, zaměstnání, členství v organizaci nebo dokonce oprávnění, která uživatel má. Tento přístup umožňuje uživatelům odhalit pouze minimální množství informací potřebných pro danou transakci nebo interakci. Autentizace na základě atributů poskytuje vyšší úroveň soukromí, protože identita uživatele zůstává skryta a pouze relevantní atributy jsou odhaleny. Tento přístup také podporuje nespojitelnost, což znamená, že jednotlivé transakce nebo interakce nemohou být vzájemně spojeny, čímž se dále chrání soukromí uživatele.

1.6.3 Budoucí problémy s elektronickým hlasováním

Kvantové počítače představují zcela nový přístup k výpočetní technice, založený na principech kvantové mechaniky. Na rozdíl od klasických počítačů, které využívají bity pro reprezentaci dat ve stavu 0 nebo 1, kvantové počítače používají qubity. Qubity mohou existovat v superpozici, což umožňuje reprezentovat oba stavy současně, a provázání, které umožňuje, aby stav jednoho qubitu byl přímo závislý na stavu jiného.

Kvantové počítače mají potenciál revolučně změnit výpočetní techniku díky své schopnosti provádět paralelní výpočty a řešit problémy, které jsou pro klasické počítače příliš náročné. To zahrnuje úlohy jako faktorizace velkých čísel, což je základ některých současných šifrovacích metod, nebo hledání v neuspořádaných databázích, což umožňuje kvantový algoritmus Grovera.

Kvantové počítače by mohly mít zásadní dopad na oblasti jako kryptografie, materiálové vědy, farmacie a mnoho dalších. Například Shorův algoritmus, který je založen na kvantových principech, může efektivně řešit problém faktorizace velkých čísel, což by mohlo ohrozit bezpečnost současných šifrovacích systémů založených na veřejných klíčích, jako je RSA. Tedy teoreticky problém se zjištěním výsledků voleb či narušení procesu těchto voleb.

Vývoj a nasazení kvantových počítačů je stále ve velmi rané fázi, a proto aktuální přímé hrozby pro elektronické hlasování jsou spíše teoretické. Nicméně, vzhledem k potenciálnímu vývoji v této technologii, je důležité, aby se vývojáři elektronických hlasovacích systémů připravovali na budoucí kvantovou éru, zahrnující výzkum a

implementaci postkvantových kryptografických technik do svých systémů pro zajištění jejich dlouhodobé bezpečnosti. Avšak je nutné mít na paměti, že použití i některých post kvantových protokolů může být nebezpečné, jelikož se v blízké době může prolomit užitím pouze hrubou silou (brute force attack) klasických současných počítačů. Jako příklad lze uvést útok na algoritmus Rainbow, který se probojoval až mezi finalisty ve třetím kole soutěže. Dalším případem jsou chyby v simulaci náhodného orákula u některých novějších post-kvantových algoritmů typu KEM, což v určitých situacích zapříčinilo jejich prolomení.

2 Praktická část studentské práce

Návrh webové stránky jako praktický výstup práce, která umožňuje uživatelům elektronicky volit. Tento projekt demonstruje technickou proveditelnost elektronického hlasování a jeho potenciální přínosy pro demokratický proces v České republice.

V současné době v České republice není možné elektronicky volit pro žádnou skupinu lidí. Jedna možnost zahájení elektronického hlasování v ČR spočívá v následování příkladu Spojených států a umožnění online hlasování například pro české občany pracující v zahraničí. Další skupinou, která by mohla využívat tohoto systému, jsou lidé se zdravotním postižením. Avšak důvěra v tuto možnost je klíčovým aspektem, což je aktuální hlavní problém v zemích jako je USA, kde panuje veliká nedůvěra v tento systém. V tuto chvíli se zdá, že Česká republika čerpá inspiraci zejména z estonského modelu, především kvůli členství obou zemí v EU, což poskytuje možnost vzájemné inspirace a spolupráce v oblasti digitální demokracie. V Estonsku existuje vysoká úroveň důvěry v elektronické hlasování, a to včetně možnosti hlasovat pro všechny obyvatele Estonska. Tuto možnost rovněž každým rokem využívá více lidí. Estonsko začalo již rokem s určitým procesem elektronizace v roce 2002, kdy byl přijat zákon, který nařizoval občanům, aby si pořídili identifikační kartu s kódem a mikročipem obsahujícím osobní údaj – obdobný jako ČR začala využívat od roku 2018. Tímto průkazem mohou Estonci elektronicky volit.

V České republice je volební právo zakotveno v ústavě. Základní zásady svobodných voleb, které se vztahují na volební právo obecně, jsou stejné i pro volební právo v České republice a musí být: [43]

- Rovnost – 1 volič = 1 hlas, hlasy voliče mají stejnou váhu
- Tajnost – nikdo není oprávněn zjišťovat, pro koho volič hlasoval
- Přímost – volič hlasuje osobně, zastoupení není přípustné
- Všeobecnost – právo volit mají všichni bez ohledu na rasu, pohlaví, sociální původ atd., avšak s ohledem na podmínky stanovené zákonem - např. věk

Rovnost a tajnost na platformě je zajištěna tím, že každý volič může odevzdat pouze jeden hlas. Tento hlas je následně zašifrován a uložen do databáze, kde není možné spojit odvolený hlas s konkrétním voličem. Všeobecnost je řešena tím, že registrace je otevřená a přístupná všem, kteří splňují základní volební kritéria.

2.1 Cíle webové stránky

Zkoumáním situace v některých zemích, kde už elektronické hlasování funguje, identifikujeme výhody a odstraníme nepotřebné aspekty. Budeme se snažit dosáhnout následujících cílů:

- Analýza současného stavu: Prozkoumat existující systémy elektronického hlasování a identifikovat jejich silné a slabé stránky.
- Návrh a implementace uživatelsky přívětivé webové platformy pro elektronické hlasování: Vytvoření uživatelsky přívětivé webové stránky s intuitivním uživatelským rozhraním, které umožní registrovaným uživatelům snadný přístup k hlasování a navigaci v systému. Cílem je usnadnit přístupnost všem bez ohledu na znalosti v oblasti IT. Snažit se o minimalizaci nabídek a funkcí na stránce, aby zůstaly pouze nezbytné prvky.
- Zajištění bezpečnosti a integrity hlasování: Navrhnout a implementovat bezpečnostní mechanismy pro ověření totožnosti uživatele, šifrování dat a zabezpečení před manipulací s výsledky hlasování, aby byla zachována důvěryhodnost celého procesu.
- Pokusit se o podporu různých typů hlasování, jako jsou volby, ankety nebo rozhodování o různých otázkách a zajištění flexibility systému pro různé formáty a požadavky hlasování, pokusit se o co největší univerzálnost.
- Testování a ověření funkcionality: Provést rozsáhlé testování výkonu, funkcionality a bezpečnosti systému.

2.2 Použité technologie

2.2.1 WordPress

WordPress je velmi populární open-source systém pro správu obsahu (CMS), který se používá k vytváření a správě webových stránek. WordPress, který byl původně spuštěn v roce 2003 jako platforma pro blogování, se od té doby vyvinul v robustní nástroj, který pohání širokou škálu webových stránek, od jednoduchých blogů po složité zpravodajské weby, e-shopy i aplikace na podnikové úrovni. Podle údajů z mého posledního školení se odhaduje, že na systému WordPress běží více než 40 procent všech webových stránek na internetu, což svědčí o jeho širokém rozšíření a všestrannosti. [44]

Ve své podstatě WordPress umožňuje uživatelům vytvářet a spravovat obsah svých webových stránek a zároveň poskytuje vývojářům také rozsáhlou flexibilitu pro přizpůsobení a rozšíření svých funkcí. WordPress je postaven na PHP a MySQL, což jsou technologie na straně serveru, které spravují dynamický obsah a interakce s databází, které webové stránky často vyžadují. Uživatelé komunikují se systémem WordPress prostřednictvím uživatelsky přívětivého ovládacího panelu, který poskytuje přístup ke všem funkcím správy webu.

WordPress funguje na architektuře založené na pluginech a tématech, což je jeden z jeho nejsilnějších aspektů. Témata řídí vizuální vzhled webu a umožňují

uživatelům snadno měnit vzhled a rozvržení. K dispozici jsou tisíce bezplatných i prémiových témat, která lze libovolně instalovat a přepínat. Pluginy naproti tomu rozšiřují funkčnost webu. Dalším důvodem popularity WordPressu je jeho aktivní komunita. Jako projekt s otevřeným zdrojovým kódem těží WordPress z celosvětové komunity přispěvatelů, kteří neustále vyvíjejí a vylepšují software, témata a pluginy. Tato komunita také nabízí rozsáhlou podporu prostřednictvím fór a návodů, které je neocenitelný pro nové i zkušené uživatele.

2.2.2 RS512

RS512 označuje podpisový algoritmus používaný v kryptografických aplikacích, konkrétně v kontextu vytváření digitálních podpisů jako součásti webových tokenů JSON (JWT) a dalších bezpečnostních tokenů. Jedná se o jeden z několika algoritmů definovaných v rámci rodiny RSA pro použití v digitálních bezpečnostních protokolech, zejména pro ověřování pomocí tokenů a bezpečný přenos dat.

Základní informace o RSA

RSA, pojmenovaný po svých vynálezcích Rivestovi, Shamirovi a Adlemanovi, je kryptografický systém s veřejným klíčem, který zahrnuje generování klíčových párů (veřejný a soukromý klíč). RSA podporuje jak šifrování dat, tak digitální podpisy pro ověřování a integritu. Síla a bezpečnost RSA vyplývá z výpočetní náročnosti faktorizace velkých celých čísel, který je základní součástí jeho algoritmu.

Specifikace RS512

RS512 používá konkrétně algoritmus RSA spolu s hashovacím algoritmem SHA-512. Číslo „512“ ve slově RS512 označuje použití hashovacího algoritmu SHA-512, který je součástí rodiny algoritmů SHA-2 navržených Národní bezpečnostní agenturou (NSA). SHA-512 je kryptografická hashovací funkce, jejímž výstupem je 512bitová hashovací hodnota, často zobrazovaná jako 128místné hexadecimální číslo. Je vysoce odolná proti kolizním útokům a je považována za bezpečnou pro moderní aplikace. RS512 funfuje následovně:

1. Generování klíčů – RS512 vyžaduje pár klíčů, veřejný klíč a soukromý klíč. Soukromý klíč používá podepisující (např. server) k vytvoření podpisu, a veřejný klíč je distribuován verifikátoru (např. klientovi nebo jinému serveru) pro ověření podpisu.
2. Proces podepisování – Data, která mají být podepsána (typicky payload nebo zpráva), jsou nejprve hashována pomocí SHA-512, čímž se vytvoří hash s pev-

nou velikostí – Tento hash je poté zašifrován soukromým klíčem RSA podepisující osoby. Tento zašifrovaný hash tvoří digitální podpis.

3. Proces podepisování – Ověřovatel použije stejnou hashovací funkci (SHA-512) na přijatou zprávu a vytvoří nový hash. Současně je digitální podpis dešifrován pomocí veřejného klíče podepisující osoby. Pokud se dešifrovaný podpis shoduje s nově vygenerovaným hashem, je potvrzena platnost podpisu, což znamená integritu a pravost zprávy.

Využití v JWT

V kontextu webových tokenů JSON (JWT) se RS512 běžně používá v případě, že je nutná vyšší úroveň zabezpečení. Tokeny JWT podepsané pomocí RS512 poskytují záruku, že s nimi nebylo manipulováno a že pocházejí z důvěryhodného zdroje. To je důležité zejména v distribuovaných systémech nebo aplikacích s přísnými požadavky na zabezpečení, jako jsou transakce s finančními nebo zdravotními údaji.

Výhody RS512

Bezpečnost – SHA-512 nabízí vysokou úroveň zabezpečení, takže RS512 je odolný proti různým kryptografickým útokům.

Nepopiratelnost – Protože podpis lze vygenerovat pouze pomocí soukromého klíče podepisující osoby, poskytuje silnou nepopiratelnost, což znamená, že podepisující osoba nemůže popřít svůj záměr a integritu zprávy.

Souhrnně lze říci, že RS512 je bezpečnou a robustní volbou pro digitální podepisování v prostředích, kde nelze ohrozit bezpečnost. Jeho použití v protokolech JWT a dalších bezpečnostních protokolech pomáhá zajistit integritu dat a ověřování napříč komunikačními kanály.

Plugin „Simple JWT Login“ je nástroj určený pro WordPress, který umožňuje ověřování JWT (JSON Web Tokens) pro náš WordPress web. Tento plugin poskytuje jednoduchý způsob nastavení ověřování založeného na JWT, který je užitečný zejména pro zabezpečení koncových bodů rozhraní WordPress REST API, usnadnění funkcí jednotného přihlášení (SSO) a integraci s dalšími systémy, které pro ověřování využívají JWT.

Klíčové funkce jednoduchého přihlášení JWT

- Ověřování JWT – Plugin umožňuje ověřování uživatelů systému WordPress prostřednictvím JWT, což z něj činí ideální volbu pro konfigurace systému WordPress, kde je frontend oddělen od backendu systému WordPress.

- Snadné přihlášení uživatelů – Uživatelé se mohou přihlásit odesláním JWT v hlavičce požadavku. Tento token je pak ověřen pluginem pro ověření uživatele, čímž se efektivně obejde tradiční přihlašovací formuláře WordPressu.
- Vytváření a správa uživatelů – Plugin lze nakonfigurovat tak, aby automaticky vytvořil uživatele WordPressu, pokud je JWT platný a uživatel ještě neexistuje v databázi WordPressu. To je užitečné zejména pro aplikace, které externě spravují přihlašovací údaje uživatelů.
- Přizpůsobitelné nastavení zabezpečení – Je možné konfigurovat nastavení zabezpečení, včetně tajného klíče použitého k podpisu tokenů, doby platnosti tokenů a uživatelských rolí, které se mohou ověřovat pomocí JWT.
- Háčky (hooks) a přesměrování – Poskytuje možnost pro přizpůsobení procesů hooks přihlášení a odhlášení a nastavení přesměrování na základě uživatelské role nebo konkrétních ID uživatelů po úspěšném ověření.
- Kompatibilita s rozhraním REST API – Plugin se bezproblémově integruje s rozhraním WordPress REST API a umožňuje uživatelům s ověřením JWT přistupovat ke koncovým bodům API. To má zásadní význam pro aplikace, které se spoléhají na backend WordPressu jako na poskytovatele dat a zároveň používají moderní frameworky JavaScriptu (například React nebo Angular) pro frontend.

Scénáře použití

Stránky WordPress bez hlavy (headless) – V bezhlavém nastavení, kde WordPress slouží pouze jako rozhraní API pro obsah, může tento doplněk zabezpečit požadavky na rozhraní API a zajistit, aby soukromá data získávaly pouze ověřené požadavky. Jednotné přihlášení (SSO) – Podniky nebo sítě webů mohou využívat JWT pro SSO, což uživatelům umožňuje přihlásit se jednou a získat přístup k více službám bez nutnosti ověřovat se pro každou zvlášť.

Bezpečnostní aspekty

Při nastavování ověřování JWT je nutné reflektovat následující osvědčené bezpečnostní postupy:

- Zabezpečení tajného klíče – Zajistit, aby byl tajný klíč JWT složitý a bezpečně uložený, aby se zabránilo neoprávněnému přístupu.
- SSL/HTTPS – K šifrování přenosu dat včetně tokenů mezi klientem a serverem používat protokol HTTPS.
- Ověření integrity tokenu – Pravidelně aktualizovat nastavení zabezpečení, aby byla zajištěna správná validace tokenů a zabránilo se neoprávněnému přístupu.

2.2.3 Argon2

Argon2 je moderní funkce pro odvozování klíčů, která byla v červenci 2015 vybrána jako vítěz soutěže Password Hashing Competition. Je navržena tak, aby poskytovala bezpečný a efektivní způsob odvozování kryptografických klíčů z hesel. Argon2 řeší klíčové problémy, jako je odolnost proti útokům hrubou silou, ochrana proti útokům na bázi GPU a současná odolnost proti útokům postranními kanály, díky čemuž je obzvláště vhodný pro hashování hesel a související bezpečnostní aplikace. [45]

Klíčové vlastnosti systému Argon2

Argon2 má několik důležitých vlastností, které zvyšují jeho bezpečnost a použitelnost pro ukládání hesel například:

- Náročnost na paměť – Argon2 je navržen tak, aby využíval značné množství paměti, které lze nakonfigurovat na základě požadavků. Tato paměťová náročnost pomáhá chránit před útoky GPU a ASIC, protože tato zařízení jsou obecně omezena z hlediska dostupné, rychlé paměti.
- Časové náklady – Tento parametr určuje množství realizovaných výpočtů a tím i dobu provádění, čímž poskytuje zpomalení proti útokům hrubou silou.
- Paralelní výpočty (Parallelism) – Argon2 podporuje možnost vyladit úroveň paralelizmu, což je počet vláken nebo linek, které používá. To umožňuje funkci efektivně využívat vícejádrové procesory při zachování odolnosti proti útokům na paralelní výpočty.

Varianty Argon2

Argon2 má tři varianty, které vyhovují různým scénářům:

- Argon2d – Optimalizovaná pro scénáře, kde hashovací funkce není vystavena hrozbám časových útoků postranními kanály (např. kryptoměny). K paměťovému poli přistupuje ve vysoce závislém vzorci, který může být rychlejší, ale méně bezpečný ve sdíleném prostředí.
- Argon2i – Argon2i je optimalizován pro hashování hesel a odvozování klíčů na základě hesel a je navržen tak, aby dobře fungoval proti útokům postranními kanály. K paměti přistupuje podle vzoru nezávislého na tajných datech, takže je vhodný pro scénáře, kde je třeba taková data chránit.
- Argon2id – Jedná se o hybrid systémů Argon2i a Argon2d, který nabízí rovnováhu mezi oběma těmito systémy. Začíná jako Argon2i (odolný proti postranním kanálům) a přechází k Argon2d (rychlejší a více závislý na vstupních datech), čímž poskytuje dobrý kompromis mezi bezpečností Argon2i a efektivitou Argon2d.

Implementace a použití

Argon2 je implementován v různých programovacích jazycích a platformách, běžně se používá v aplikacích vyžadujících bezpečné ukládání hesel. Při konfiguraci Argon2 je třeba vyvažovat mezi bezpečností (větší paměť, větší časové náklady) a použitelností (menší využití zdrojů). Při ukládání hesel se Argon2 obvykle používá takto:

1. Vytvoření soli – Bezpečně vygenerujte náhodnou sůl.
2. Hashování hesla – Použijte Argon2 s heslem, solí a zvolenými parametry (paměťové náklady, časové náklady).
3. Uložení hesla a soli – Sůl i hash se uloží do databáze. Obecně nikdy se nesmí ukládat heslo v plain textu.

Bezpečnostní aspekty

Přestože je Argon2 považován za bezpečný, jeho účinnost závisí na správné implementaci a konfiguraci. Je nutné vybrat vhodné parametry – V závislosti na požadavcích aplikace na zabezpečení a dostupných systémových prostředcích zvolit velikost paměti, časové náklady. Jak se zlepšují možnosti hardwaru, je nutné revidovat parametry systému Argon2, k zajištěné, že zůstanou bezpečné proti novým pokrokům v technologiích útoků. Dále je nutno vždy využívat kryptograficky bezpečnou metodu generování jedinečné soli pro každé heslo.

Přizpůsobivost systému Argon2 různým scénářům útoků a hardwaru z něj činí vynikající volbu pro hashování hesel a bezpečnostní aplikace, které potřebují robustní obranu proti více typům útoků.

2.2.4 Webové tokeny JSON (JWT)

Webové tokeny JSON (JWT) jsou otevřenou standardní průmyslovou metodou (RFC 7519) pro bezpečnou reprezentaci nároků mezi dvěma stranami. Tokeny JWT se běžně používají ve webových aplikacích pro správu ověřování a autorizace uživatelů a jsou obzvláště užitečné ve scénářích, kdy je potřeba jednotné přihlášení (SSO) v různých doménách nebo pro bezstavové ověřování v architektuře mikroslužeb.

Jak fungují JWT

Autentizace – Poté, co se uživatel přihlásí pomocí svých přihlašovacích údajů, je vrácen JWT. Protože je uživatel identifikován při každém požadavku, stačí, aby se v zařízení přihlásil pouze jednou, aby mohl přistupovat ke službám nebo zdrojům, které mají stejné nastavení ověřování. Po úspěšné autentizaci server vygeneruje JWT, který obsahuje uživatelské údaje a další relevantní informace. Token je zakódován a podepsán pomocí tajného klíče nebo veřejného/privátního klíčového páru.

Obvyklá struktura JWT se skládá ze 3 částí: hlavička (specifikuje typ tokenu (např. JWT) a použitý hashovací algoritmus (např. HMAC SHA256 nebo RSA), payload (obsahuje tvrzení o uživateli a další metadata, jako jsou oprávnění uživatele, datum vypršení platnosti tokenu atd.) a podpis (zabezpečuje token proti manipulaci. Podpis je vytvořen hashováním hlavičky a payloadu spolu s tajným klíčem)

Autorizace – Po vydání se token odesílá zpět klientovi, který ho pak bude posílat jako součást hlavičky (obvykle s použitím schématu Bearer) při každém dalším požadavku na server. Při přijetí požadavku server extrahuje JWT, ověří jeho podpis, aby zjistil, zda nebyl manipulován, a zkontroluje, zda je token stále platný (např. nevypršel). Pokud je vše v pořádku, server zpracuje požadavek na základě oprávnění uvedených v tokenu.

Mezi výhody JWT tedy patří kompaktnost, jelikož Lze odeslat prostřednictvím adresy URL, parametru POST nebo v hlavičce HTTP. A dále samostatnost payload obsahuje všechny požadované informace o uživateli, takže není nutné se vícekrát dotazovat do databáze.

Bezpečnostní aspekty

Vždy je nutné zajistit, aby byly tokeny přenášeny zabezpečenými kanály (např. HTTPS). Podpis by měl být ověřen na přijímající straně, aby se potvrdila pravost tokenu. Citlivá data v rámci payloadu JWT by měla být šifrována, protože kódování base64 není bezpečné. Tokeny by měly mít nárok na vypršení platnosti (‘exp‘), aby se snížilo riziko zneužití ukradeného tokenu. Je nutné využívat silné, soukromé klíče (při využití u RSA) nebo dlouhé, složité, tajné klíče (při využití u HMAC).

Protokoly JWT poskytují robustní a efektivní způsob bezpečného přenosu informací mezi stranami ve formě objektu JSON a staly se důležitou součástí architektur moderních webových aplikací.

2.2.5 Ukázky kódu a webu

Na obrázku 2.1 je zachyceno nastavení argon2 pepře (pepper), při integraci vlastního pluginu Wordpress, který mění nativní MD-5 se solí password_hash na argon2. [46]. Na obrázku 2.2 je zachycena funkce, která změní auth_cookie pro přihlášené uživatele a donutí jej se po každé hodině znovu přihlásit. [47] Na obrázku 2.3 je zachyceno nastavení pluginu JWT a nastavení veřejného a soukromého klíče. Pomocí rs512 a klíčů se podepíše token JWT a při ověřování se token zkontroluje.

Pro registraci jsem využil plugin fluent forms který mi pomohl vytvořit registrační formulář a snadno doprogramovat průchod registrací. Po vyplnění všech nutných polí se vytvoří uživatelský účet v systému autentizační autority (náhrada za

```
define('WP_PASSWORD_ARGON_TWO_PEPPER', '=ajoApm(N2tF+rgl7.uLQor@pPqap6miqa^r=-KU%Sz3^n8mj3');
define('WP_PASSWORD_ARGON_TWO_FALLBACK_PEPPERS', []);
define('WP_PASSWORD_ARGON_TWO_OPTIONS', []);
```

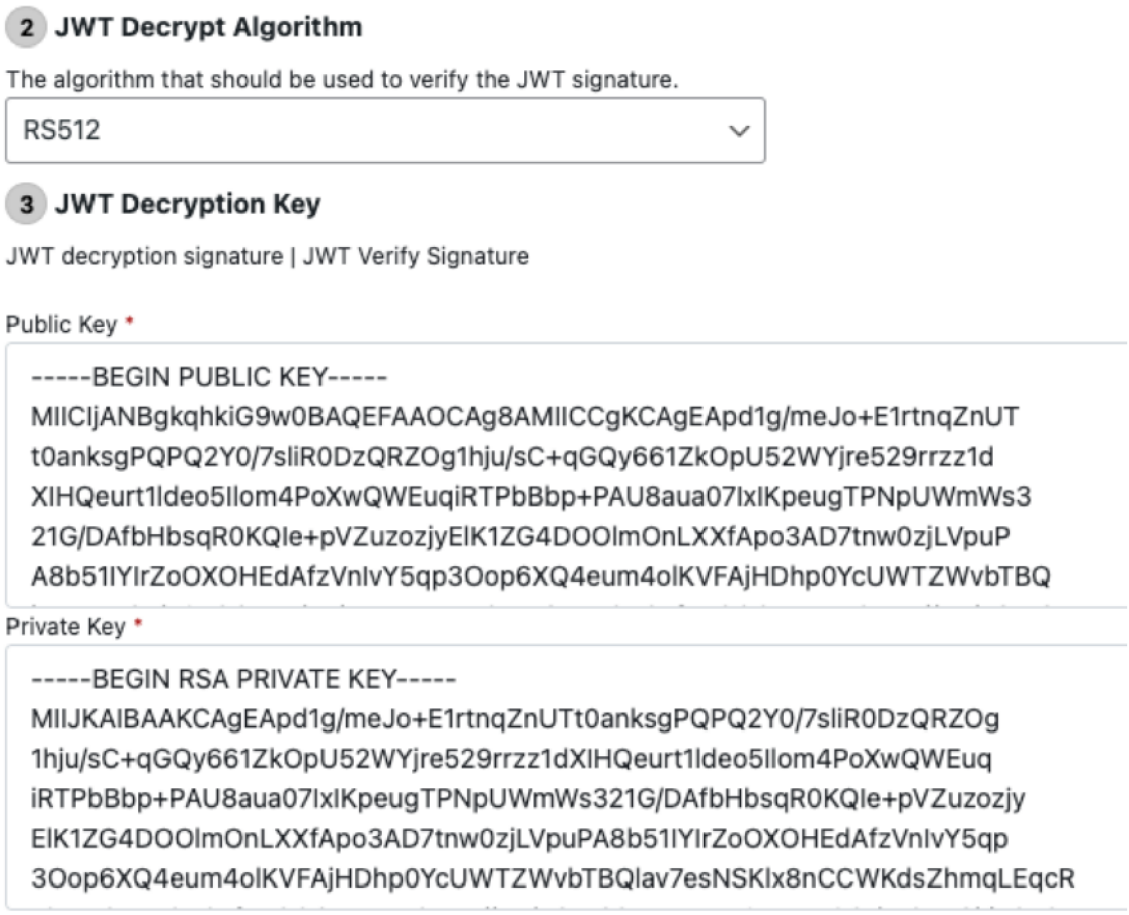
Obr. 2.1: Nastavení Argon2.

```
add_filter( 'auth_cookie_expiration', 'stay_logged_in_for_1_hour' );
function stay_logged_in_for_1_hour( $expire ) {
return 3600; // 1 hour in seconds
}
```

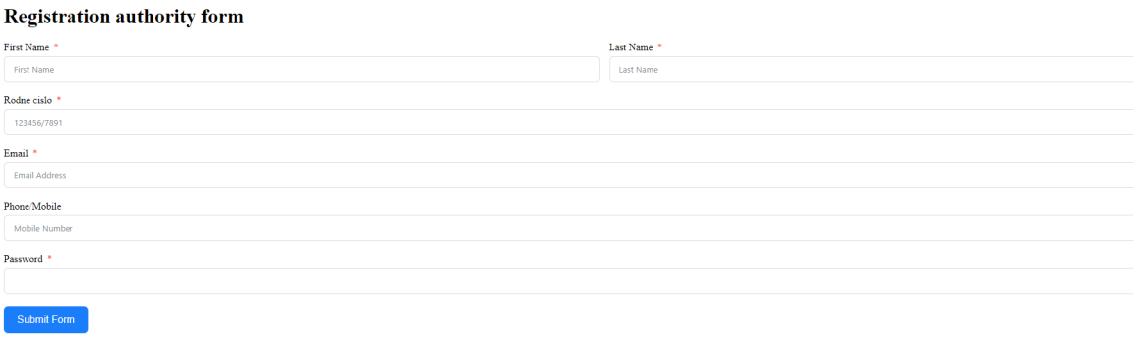
Obr. 2.2: Funkce měnící auth_cookie.

NIA) 2.4. Vytvořený uživatelský účet a heslo se zašifruje pomocí knihovny pro argon2i. Ukázka databáze je zachycena na obrázku 2.5. Následně se napojím na nativní Wordpress hook pro registraci uživatele a spustíme další funkce v procesu. Pomocí různých dat je vytvořeno uuid pro účet na webu pro volby, který však jen vygenerován, ale nikam neukládán. 2.6 Registrace je povolena pouze z dané IP adresy. Poslední krokem je registrace, web autorizační autority pošle všechna data na web, který umožňuje volby, ten vygeneruje uživatele, vygeneruje JWT token a zašle zpět web autorizační, přiřadí JWT token k registrované osobě. Více informací o sobě oba systémy nesdílí. Registrace je umožněna pouze ze zvolené IP adresy, takže registraci nemůže vyvolat uživatel samotný, ale je nutné vyvolat ho skrze server. JWT token je vygenerovaný skrze RS512 algoritmus a web ho vždy ověřuje. 2.7 K danému uživateli se přiřadí JWT token 2.8. Při přihlašování se automaticky ověří jaký typ uživatele se přihlašuje, zda zadal správné heslo, ověří se platnost jeho JWT tokenu, pokud je expirovaný, tak se token obnoví, uloží se nový a uživatel se automaticky přihlásí a přesměruje na web s volbami. V našem případě se autorizační cookie nastaví na jednu hodinu 2.2 Uživatel je automaticky přesměrován na domovskou stránku kde vidí aktivní volby a výsledky již neaktivních (proběhlých) voleb. 2.9

Ukázka výsledků prezidentských a parlamentních voleb. 2.11



Obr. 2.3: Nastavení veřejného a soukromého klíče.



Obr. 2.4: Vytvoření uživatelského účtu v systému autentizační autority.

☐	Upravit	Kopírovat	Odstranit	13	cirepis949@etopys.com	$argon2i$v=19$m=65536,t=4,p=1$BT4OjUsXn8XeLYTZGErk...	cirepis949etopys-com
☐	Upravit	Kopírovat	Odstranit	14	sogig74683@togito.com	$argon2i$v=19$m=65536,t=4,p=1$GvmDTM7tJN0gsjxa5Dh7...	sogig74683togito-com
☐	Upravit	Kopírovat	Odstranit	15	yepav72175@ociun.com	$argon2i$v=19$m=65536,t=4,p=1$11FPIOttrRwwrbXqlXxg...	yepav72175ociun-com

Obr. 2.5: Ukázka databáze.

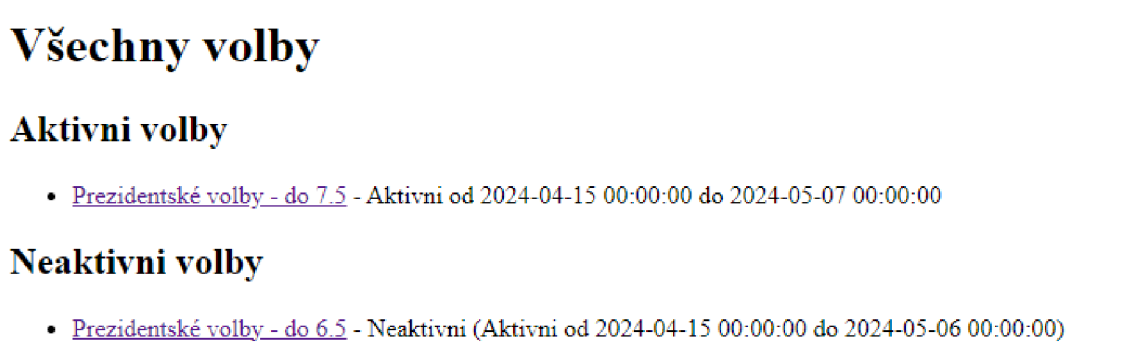
```php
function generate_random_uuid_from_user($user_id) {
    // Retrieve user data
    $user_info = get_userdata($user_id);
    if (!$user_info) return '';

    // Prepare data parts
    $emailPart = $user_info->user_email;
    $namePart = $user_info->first_name . $user_info->last_name; // Assuming you have these fields
    $rcPart = get_user_meta($user_id,'rc');
    // You might want to include more user-related data here

    // Combine parts to form a base string
    $baseString = $emailPart . $namePart .$rcPart. uniqid(). time(); // Adjust 'yourAdditionalData' as needed

    // Hash the base string to get a consistent format
    $hashedString = hash('sha256', $baseString);

    // Generate a random 10-letter UUID from the hashed string
    $uuid = substr(str_shuffle(preg_replace('/[^a-zA-Z0-9]/', '', $hashedString)), 0, 20);

    return $uuid;
}

add_action('user_register', 'on_user_register_create_uuid', 10, 1);
```

Obr. 2.6: Vytvoříme uuid.

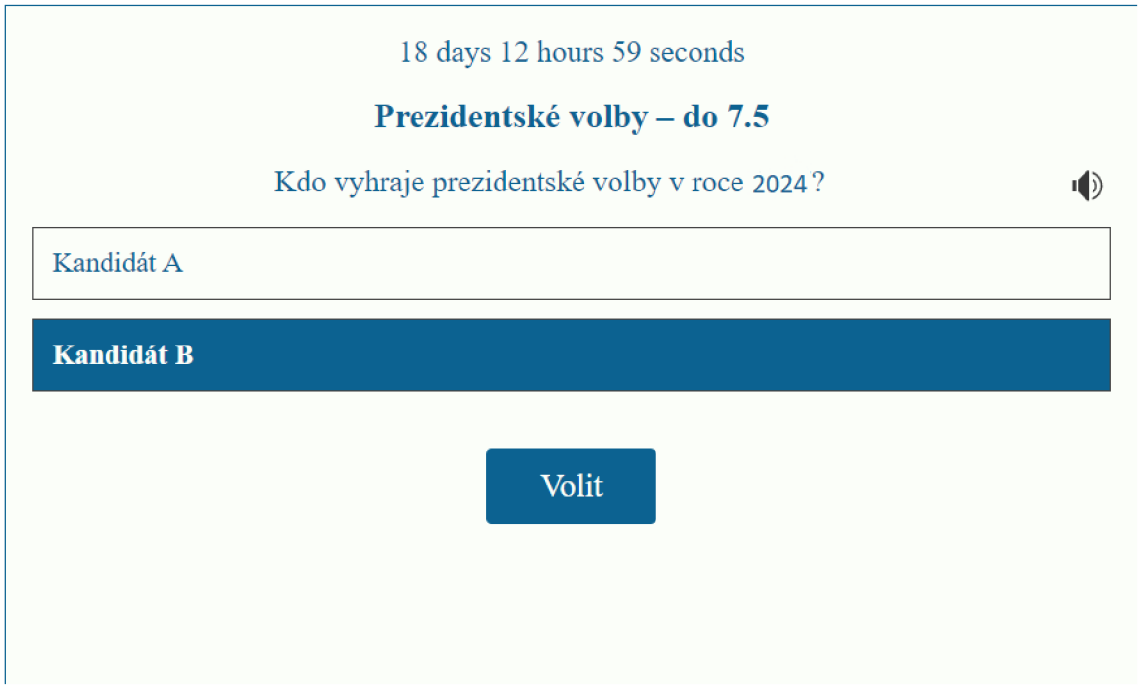
```php
function redirect_user_with_jwt($user_id, $auth_key = null) {
    $jwt = get_user_meta($user_id, 'jwt_token', true);
    if (!$jwt) {
        // Handle case where JWT is missing
        error_log('JWT missing for user ID ' . $user_id);
        return;
    }

    $simpleJwtLogin = new SimpleJwtLoginClient($domain, '/poll');
    $autologinUrl = $simpleJwtLogin->getAutologinUrl($jwt, $auth_key, $domain); // Specify the redirect URL after login

    wp_redirect($autologinUrl);
    exit;
}
```

Obr. 2.7: JWT token

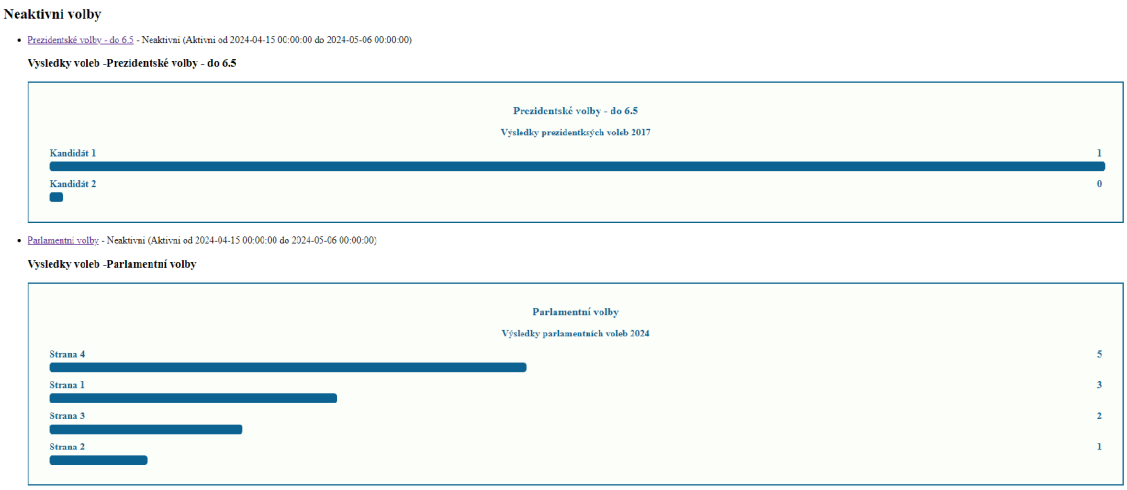
Obr. 2.8: JWT token přiřazený k uživateli



Obr. 2.9: Ukázka webu s volbami.



Obr. 2.10: Ukázka hlasování.



Obr. 2.11: Ukázka výsledků.

Závěr

V rámci této diplomové práce byl proveden komplexní návrh systému pro elektronické hlasování a zkoumány jeho právní specifika. Cílem této práce bylo vytvořit efektivní a bezpečný elektronický hlasovací systém, který by splňoval nejen technické požadavky, ale také právní normy a zásady týkající se hlasování a ochrany dat.

Práce se zaměřila na analýzu existujících elektronických hlasovacích systémů, identifikaci jejich nedostatků a následně na navržení nového systému, který by tyto nedostatky eliminoval. Byly zohledněny nejen technické aspekty, jako je zabezpečení dat a uživatelská přívětivost, ale také právní otázky spojené s elektronickým hlasováním, jako je autentizace voličů, způsob ověření hlasů a záruka anonymity.

V úvodních kapitolách práce ukázala, jak se elektronického hlasování ujaly Spojené státy americké, které celonárodně nikdy do praxe elektronické hlasování neaplikovaly. V praxi se ukazuje, že důvěra v tento systém občany USA příliš není rozvinutá. Další stát, který tato práce rozebírá, je Estonsko. Estonsko je stejně jako Česká republika, členem Evropské unie a je tak cenným zdrojem inspirace pro ČR. Estonsku se podařilo vybudovat velikou důvěru v tento systém a rovněž se podařilo elektronické hlasování umožnit všem svým občanům bez rozdílu.

V rámci práce byl také proveden průzkum právních předpisů týkajících se elektronického hlasování v České republice a dalších relevantních zemích. Byly identifikovány klíčové právní normy a směrnice, které by měl nový elektronický hlasovací systém respektovat, aby bylo zajištěno jeho legální a transparentní fungování.

Díky analýze existujících systémů a právních předpisů byl vytvořen konkrétní návrh systému pro elektronické hlasování, který kombinuje technologické inovace s právními požadavky. Tento návrh představuje komplexní řešení pro elektronické hlasování, které by mohlo být implementováno s ohledem na aktuální legislativu a technologické možnosti. Tento návrh je konceptuální ukázka, jak by mohla vypadat webová stránka pro elektronické hlasování v České republice.

Literatura

[1] *The Evolution of Ballot Papers.* Online. Dostupné z: https://www.tiki-toki.com/timeline/entry/1461250/The-Evolution-of-Ballot-Papers/. [cit. 2023-11-01].

[2] STROMBERG, Joseph. *Herman Hollerith's Tabulating Machine. Online. Smithsonianmag.* 2011. Dostupné z: https://www.smithsonianmag.com/smithsonian-institution/herman-holleriths-tabulating-machine-2504989/. [cit. 2023-11-01].

[3] *Absentee voting or voting by mail.* Online. Dostupné z: https://www.usa.gov/absentee-voting. [cit. 2023-11-01].

[4] *Citáty.* Online. Dostupné z: https://www.databazeknih.cz/citaty/josif-vissarionovic-dzugasvili-20600. [cit. 2023-11-01].

[5] *US, Election Assistance Commission, A Survey of lnternet Voting.* Online. Dostupné z: https://www.eac.gov/sites/default/files/eac_assets/1/28/SIV-FINAL.pdf. [cit. 2023-11-01].

[6] *A Threat Analysis on UOCAVA Voting Systems (NIST IR 7551).* Online. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7551.pdf. [cit. 2023-11-01].

[7] *Department of Defense: Expanding the Use of Electronic Voting Technology for UOCAVA Citizens.* Online. Dostupné z: https://www.fvap.gov/uploads/FVAP/Reports/ivas2007.pdf. [cit. 2023-11-01].

[8] *Election Administration and Voting Survey 2022 Comprehensive Report.* Online. Dostupné z: https://www.eac.gov/sites/default/files/2023-06/2022_EAVS_Report_508c.pdf. [cit. 2023-11-01].

[9] *Voting online.* Online. Dostupné z: https://www.npr.org/2023/09/07/1192723913/internet-voting-explainer. [cit. 2023-11-01].

[10] *These States Allow Online Voting for Citizens. Does Yours?* Online. Dostupné z: https://www.eballot.com/blog/these-states-allow-online-voting-for-their-citizens-is-your-state-one-of-the [cit. 2023-11-01].

[11] EHIN, Piret, et al. Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly,* 2022, 39.4: 101718.

[12] Council of Europe. (2004). *Recommendation CM/Rec(2004)11 on legal, operational and technical standards for e-voting.* Online. Dostupné z: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/Rec(2004)11_Eng_Evoting_and_Expl_Memo_en.pdf.

[13] Council of Europe. (2017). *Recommendation CM/Rec(2017)5 of the committee of ministers to member states on standards for e-voting.* Online. Dostupné z: https://rm.coe.int/0900001680726f6f.

[14] *Statistics about Internet voting in Estonia.* Online. Dostupné z: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia. [cit. 2023-11-01].

[15] *Internet voting in Estonia.* Online. Dostupné z: https://www.valimised.ee/en/internet-voting-estonia. [cit. 2023-11-01].

[16] *ID.ee.* Online. Dostupné z: https://www.id.ee/en/. [cit. 2023-11-01].

[17] *Estonské digitální království se těší podpoře místních obyvatel i e-rezidentů.* Online. 2020. Dostupné z: https://pealinn.ee/2020/06/04/eesti-digiriik-naudib-nii-kohalike-elanike-kui-e-residentide-toetust/. [cit. 2023-11-01].

[18] POLČÁK, Radim, Jakub HARAŠTA, Pavel KOUKAL, Tereza KYSELOVSKÁ, Pavel LOUTOCKÝ, Matěj MYŠKA, Michal PETR, Tomáš GŘIVNA, Josef DONÁT, Tomáš ŠČERBA a Miroslav UŘIČAŘ. *Privacy and Technology Law Czech Republic: Information Technology Law. 1. vyd. Alphen aan den Rijn: Kluwer Law International B.V.,* 2023. 345 s. International Encyclopaedia of Laws: Privacy and Technology Law. ISBN 978-90-411-2188-2.

[19] *Koaliční smlouva.* Online. Dostupné z: https://www.vlada.cz/assets/media-centrum/dulezite-dokumenty/koalicni_smlouva_ods_top09_vv.pdf. [cit. 2023-11-01].

[20] *USNESENÍ VLÁDY ČESKÉ REPUBLIKY.* Online. Dostupné z: https://odok.cz/portal/services/download/attachment/KORN97AU7TXU/. [cit. 2023-11-01].

[21] *Elektronické hlasování umožní volit na dálku.* Online. Dostupné z: https://www.vlada.cz/cz/media-centrum/aktualne/elektronicke-hlasovani-umozni-volit-na-dalku-99951/. [cit. 2023-11-01].

[22] *Návrh zákona o správě voleb 2019.* Online. Dostupné z: https://odok.cz/portal/veklep/material/KORNBH2MHKS9/. [cit. 2023-11-01].

[23] *Návrh zákona o správě voleb 2022.* Online. Dostupné z: https://odok.cz/portal/veklep/material/ALBSCERHSHDS//. [cit. 2023-11-01].

[24] *České korespondenční volby na obzoru.* Online. Dostupné z: https://e-politics.cz/ceske-korespondencni-volby-na-obzoru/. [cit. 2023-11-01].

[25] *Další změny u voleb. Část poslanců chce znovu otevřít korespondenční volbu nebo hlasování nezletilých.* Online. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3626274-dalsi-zmeny-u-voleb-cast-poslancu-chce-znovu-otevrit-korespondencni- [cit. 2023-11-01].

[26] *Korespondenční volbu prosadíme, přestože to bude stát hodiny obstrukcí, slibuje Rakušan.* Online. Dostupné z: https://www.forum24.cz/korespondencni-volbu-prosadime-prestoze-to-bude-stat-hodiny-obstrukci-slibuj [cit. 2023-11-01].

[27] *Korespondenční volba se odkládá. Obstrukcí ve Sněmovně by už teď bylo moc.* Online. Dostupné z: https://www.novinky.cz/clanek/domaci-korespondencni-volba-se-odklada-obstrukci-ve-snemovne-by-uz-ted-bylo- [cit. 2023-11-01].

[28] *EObčanka.* Online. Dostupné z: https://ockodoc.mzcr.cz/napoveda/identitaobcana/eobcanka/. [cit. 2023-11-01].

[29] *EObčanka.* Online. Dostupné z: https://gov.cz/rozcestniky/eobcanka-RZC-105. [cit. 2023-11-01].

[30] HEJDUK, PhDr Marek. *e-Government–elektronické občanské průkazy, Portál občana.* 2020.

[31] *Nový Portál občana.* Online. Dostupné z: https://www.dvs.cz/clanek.asp?id=6938457. [cit. 2023-12-01].

[32] *Identita občana v roce 2022: souhrnné vybrané statistiky.* Online. Dostupné z: https://nakit.cz/identita-obcana-v-roce-2022-souhrnne-vybrane-statistiky/. [cit. 2023-12-01].

[33] MLADÁ, Pavlína. *Postup digitalizace v ČR a Portál občana.* 2023.

[34] *Služby Portálu občana.* Online. Dostupné z: https://portal.gov.cz/informace/sluzby-portalu-obcana-INF-278. [cit. 2023-12-01].

[35] *Portál Pražana.* Online. Dostupné z: https://www.portalprazana.cz/nastenka. [cit. 2023-11-01].

[36] *Brno iD.* Online. Dostupné z: https://www.brnoid.cz/cs/. [cit. 2023-11-01].

[37] HAJNÝ, Jan. Přednáška předmětu SIB. Presentation presented at: [Information Security Seminar] Dostupné z: https://moodle.vut.cz/mod/resource/view.php?id=412210 [cit. 2024-04-04]

[38] *What does data protection 'by design' and 'by default' mean?* Online. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protec [cit. 2024-04-04].

[39] *NISA: Potřebujeme více technologií na ochranu soukromí, nejenom šifrování.* Online. Dostupné z: https://www.lupa.cz/clanky/enisa-potrebujeme-vice-technologii-na-ochranu-soukromi-nejenom-sifrovani/ [cit. 2024-04-04].

[40] *Authentication.* Online. Dostupné z: https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.2%3A_Authentication [cit. 2024-04-04].

[41] *NÚKIB připravil podpůrné materiály pro ochranu před hrozbou v podobě kvantových počítačů.* Online. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/1984-nukib-pripravil-podpurne-materialy-pro-ochranu-pred-hrozbou-v-podobe-kv [cit. 2024-04-04].

[42] National Security Agency | Cybersecurity Information Sheet, The Commercial National Security https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

[43] *Všeobecné, rovné a přímé volební právo tajným hlasováním.* Online. Dostupné z: https://www.psp.cz/sqw/hp.sqw?k=301. [cit. 2023-11-01].

[44] *WordPress.* Online. Dostupné z: https://cs.wordpress.org/. [cit. 2023-11-01].

[45] *Argon2.* Online. Dostupné z: https://github.com/P-H-C/phc-winner-argon2. [cit. 2023-11-01].

[46] *WP Password Argon Two.* Online. Dostupné z: https://github.com/TypistTech/wp-password-argon-two

[47] *Filters the authentication cookie.* Online. Dostupné z: https://developer.wordpress.org/reference/hooks/auth_cookie/

Seznam symbolů a zkratek

ČR Česká republika

eGovernment Electronic government

EU Evropská unie

e-voting Elektronické hlasování

FVAP Federal Voting Assistance Program

GDPR General Data Protection Regulation

MFA Multi-factor authentication

PETs Privacy-Enhancing Technologies

SERVE Secure Electronic Registration and Voting Experiment

UOCAVA The Uniformed and Overseas Citizens Absentee Voting Act

USA Spojené státy americké

VC Vote Collector

VOI Voting Over the Internet