

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH
STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE**

BAKALÁŘSKÁ PRÁCE

**Bezpečnost elektronické komunikace ve veřejné
správě**

Autor práce: Dominik Golian
Studijní obor: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Vedoucí práce: RNDr. Růžena Ferebauerová
Katedra: Bezpečnostně právní činnost

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.

Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Dominik Golian

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Místo studia: České Budějovice

Název bakalářské práce: Bezpečnost elektronické komunikace ve veřejné správě

Název bakalářské práce v anglickém jazyce: Security of Electronic Communication in Public Administration.

Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce (jméno a příjmení, titul): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): březen 2022

Cíl bakalářské práce:

1/ Hlavním cílem bakalářské práce bude charakteristika bezpečnosti elektronické komunikace ve veřejné správě, včetně otázky ochrany soukromí uživatelů.

2/ Vedlejším cílem práce bude porovnání bezpečnosti a elektronické komunikace ve veřejné správě ve vybraných zemích Evropské unie a konkrétně na Slovensku a v České republice.

Student: Dominik Golian	14.5.2022 datum	 podpis
Vedoucí práce: RNDr. Růžena Ferebauerová	16.5.2022 datum	 podpis

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	30.5.2022 datum	 podpis
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	1.6.2022 datum	 podpis
Rektor: doc. Ing. Jiří Dušek, Ph.D.	10.6.2022 datum	 podpis



Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí(mu) bakalářské RNDr. Růžena Ferebauerová za cenné rady,
připomínky a metodické vedení práce.

ABSTRAKT

Golian Dominik: Bezpečnosť elektronickej komunikácie vo verejnej správe: bakalárska práca. 2023 České Budějovice. Vysoká škola evropských a regionálních studií, 2023. Vedúca práce: RNDr. Ružena Ferebauerová.

Predkladaná bakalárska práca sa venuje problematike bezpečnosti v elektronickej komunikácii verejnej správy. Cieľom práce bola charakteristika bezpečnosti elektronickej komunikácie vo verejnej správe, vrátane otázky ochrany súkromia užívateľov. Vedľajším cieľom práce bolo porovnanie bezpečnosti a elektronickej komunikácie vo verejnej správe vo vybraných krajinách Európskej únie a konkrétne na Slovensku a v Českej republike. Následne po spracovaní teoreticko-metodickej analýzy dospejeme k vyhodnoteniam, ktoré budú tvoriť súčasť záveru predkladanej bakalárskej práce.

Kľúčové slová: verejná správa, e-Government, komunikácia, bezpečnosť.

ABSTRACT

Golian Dominik: Security of electronic communication in public administration: Bachelor thesis. České Budějovice. The College of European and Regional Studies, 2023. Supervisor: RNDr. Ružena Ferebauerová.

The presented bachelor's thesis is devoted to the issue of security in electronic communication of public administration. The aim of the work was to characterize the security of electronic communication in public administration, including the issue of protecting users' privacy. A secondary goal of the work was a comparison of security and electronic communication in public administration in selected countries of the European Union, specifically in Slovakia and the Czech Republic. Subsequently, after processing the theoretical-methodical analysis, we will arrive at the evaluations, which will form part of the conclusion of the submitted bachelor's thesis

Keywords: public administration, e-Government, communication, security.

OBSAH

ÚVOD.....	8
1 CIEĽ A METODIKA PRÁCE	10
2 VEREJNÁ SPRÁVA	11
2.1 Definovanie verejnej správy	11
2.2 Riadenie a organizácia verejnej správy.....	14
2.3 Portál verejnej správy.....	16
2.3.1 Informačná časť	18
2.3.2 Transakčná časť	20
3 E-GOVERNMENT.....	23
3.1 E-Government zákon	25
3.2 Štruktúra, princípy a faktory verejnej správy.....	27
3.3 Elektronické služby a informačné systémy verejnej správy	30
3.4 Výhody a nevýhody e-Governmentu	32
4 ELEKTRONICKÁ KOMUNIKÁCIA VO VEREJNEJ SPRÁVE A JEJ ZABEZPEČENIE	34
4.1 Druhy elektronickej komunikácie	34
4.2 Bezpečná komunikácia.....	37
4.3 Elektronické schránky	39
4.4 Elektronický podpis a značka.....	44
4.5 Elektronické certifikáty	48
4.6 Banková identita.....	50
ZÁVER	53
ZOZNAM POUŽITÝCH ZDROJOV.....	55
ZOZNAM OBRÁZKOV, TABULIEK A GRAFOV.....	61

ÚVOD

V súčasnom svete sa ľudia obklopujú počítačmi, mobilmi a tabletmi, a tak spoločnosť speje k všade prítomnej elektronickej komunikácii. Už aj pre bežnú komunikáciu je stále viacej využívaná nová informačná a komunikačná technológia.

Aj v týchto situáciách musí každý z nás dbať na to, že aj táto forma komunikácie nám neposkytuje 100% ochranu. Túto skutočnosť je potrebné si uvedomiť stále aj pri komunikácii s verejnou správou, nakoľko práve táto inštitúcia prichádza do každodenného kontaktu s informáciami o ľuďoch.

Verejná správa je spoločenský fenomén, ktorý tvorí súčasť všetkých oblastí spoločenského života a tak je možné ju vnímať ako prakticky realizovanú činnosť, ako vednú disciplínu a taktiež aj ako študijný odbor. Zároveň je veľmi zložitou verejnou skutočnosťou a tak sa k nej pristupuje ako k správe verejných záležitostí uskutočnenej ako prejav výkonnej moci v štáte.

Na základe vyššie uvedeného bol stanovený hlavný cieľ bakalárskej práce, ktorým je charakteristika bezpečnosti elektronickej komunikácie vo verejnej správe, vrátane otázky ochrany súkromia užívateľov.

Predkladaná bakalárska práca je rozdelená do troch základných kapitol s príslušnými podkapitolami. V rámci prvej kapitoly sa venujeme problematike verejnej správy, teda jej základnej definícii, jej činnosti, resp. riadeniu a fungovaniu, ako aj portálu verejnej správy, ktorý priblížime z hľadiska jeho transakčnej a informačnej časti.

V druhej kapitole práce sa venujeme eGovernmentu, ktorý spočíva v zavádzaní informačno-komunikačných technológií vo verejnej správe, a to spolu s organizačnými zmenami, novými postupmi a zručnosťami za účelom zvýšenia efektívnosti, transparentnosti a posilnenia verejnej politiky, pričom sa konkrétnejšie zameriame na zákon, ktorý sa mu venuje, ako aj štruktúram, princípom a faktorom verejnej správy, elektronickým službám a informačným systémom verejnej správy. V rámci poslednej podkapitoly uvedieme jeho výhody a nevýhody.

V rámci tretej kapitole práce sa zameriam na stanovenie si hlavného a vedľajšieho cieľa práce a taktiež metodike práce, ktorú sme použili pri spracovaní bakalárskej práce.

V poslednej štvrtej kapitole práce sa venujeme elektronickej komunikácii vo verejnej správe a jej zabezpečeniu. Súčasťou tejto kapitoly budú aj druhy elektronickej komunikácie,

elektronické schránky, bezpečná komunikácia, elektronický podpis, certifikáty a značka, pričom veľmi dôležitou súčasťou celej práce bude aj následné porovnanie bezpečnosti a komunikácie vo verejnej správe na Slovensku a v Českej republike.

1 CIEĽ A METODIKA PRÁCE

Vzhľadom na problematiku, ktorej sa v bakalárskej práci venujeme sme si stanovili nielen hlavný, ale aj vedľajší cieľ práce.

Hlavným cieľom práce bude charakteristika bezpečnosti elektronickej komunikácie vo verejnej správe, vrátane otázky ochrany súkromia užívateľov.

Vedľajším cieľom práce bude porovnanie bezpečnosti a elektronickej komunikácie vo verejnej správe vo vybraných krajinách Európskej únie a konkrétne na Slovensku a v Českej republike.

Následne po spracovaní teoreticko-metodickej analýzy dospejeme k vyhodnoteniam, ktoré budú tvoriť súčasť záveru predkladanej bakalárskej práce.

V súvislosti s typom práce, ktorým je teoreticko-metodická analýza sme sa ako prvé zamerali na najdôležitejšiu metódu, ktorou je rešerš, resp. vyhľadanie dostupnej literatúry týkajúcej sa problematiky práce, ktorou je bezpečná elektronická komunikácia vo verejnej správe.

V rámci spracovania práce sme ďalej použili metódy analýzy a syntézy, ktoré sú teoretickými metódami. Analýza spočíva v rozložení získaných skutočností na jednotlivé časti a tak sa vytvorili podmienky na poznanie týchto častí, ako napr. v prípade portálu verejnej správy. Metóda syntézy spočívala v spájaní častí, vzťahov a súvislostí do uceleného celku, ako napr. pri e-Governmente a jeho faktorov, princípov a štruktúry, výhod a nevýhod, ako aj elektronických služieb a informačných systémov.

V druhej časti bakalárskej práce využijeme metódu komparácie, resp. porovnania, ktorá spočíva v zhodnotení rôznych či rovnakých vlastností predmetov alebo javov, a to napríklad porovnávanie kvality alebo kvantity skúmaného javu či v iných prípadoch napríklad porovnanie názorov rôznych autorov na určitý problém, ako napr. pri porovnaní skúmanej problematiky elektronickej komunikácie verejnej správy vybraných krajín Európskej únie.

2 VEREJNÁ SPRÁVA

Verejná správa je spoločenským fenoménom, ktorý tvorí súčasť všetkých oblastí spoločenského života a zároveň je aj činnosťou, ktorá je vykonávaná aj prakticky. Na tomto základe je možné ju vnímať ako prakticky realizovanú činnosť, ako vednú disciplínu a taktiež aj ako študijný odbor.

Verejná správa je veľmi zložitou verejnou skutočnosťou, ktorú je nutné aj popísať a tak sa k nej pristupuje ako k správe verejných záležitostí realizovanej ako prejav výkonnej moci v štáte.¹

Verejná správa je oblasťou, ktorá je bohatá nielen do svojej šírky, ale aj hĺbky a každý z nás sa s ňou stretáva po celý život, ako napr. cez matričný záznam pri narodení, cez školskú dochádzku alebo vybavovanie rozličných potvrdení a povolení na úradoch a pod.

Verejnú správu, resp. aktivity jej organizačných jednotiek, môže vidieť alebo inak zaznamenať každý občan napr. pri pohľade na kontajnery s odpadom, chodníky a cesty, policajtov hliadkujúcich na uliciach, prostriedky hromadnej dopravy, zeleň v obecných parkoch, historické a kultúrne pamiatky, alebo dokonca aj pri pohľade na televíznu obrazovku či pri počúvaní rozhlasového vysielania.²

2.1 Definovanie verejnej správy

Vzhľadom k vyššie uvedeným skutočnostiam je pre teoretikov zaoberajúcich sa problematikou verejnej správy je ťažké stanoviť jednoznačnú definíciu verejnej správy tak, aby vystihovala celú jej šírku a hĺbku. Autori pri jej definovaní kladú dôraz hlavne na rozličné aspekty jej fungovania na základe hodnotenia a výsledkov vlastných poznatkov a skúseností, ktoré ú zároveň ovplyvňované politickým prostredím, aktivitami vlády a politikov.³

Pre vymedzenie termínu verejnej správy nájdeme niekoľko jej významov, ktoré sú si síce podobné, avšak pri ich hlbšom pohľade zistíme, že sa navzájom po obsahovej stránke značne odlišujú. Všeobecne je možné povedať, že je verejná správa termínom, ktorý má

¹ KOVÁČOVÁ, E. *Teória a prax verejnej správy v podmienkach Slovenskej republiky*. Banská Bystrica, 2014, s. 5

² KLIMOVSKÝ, D. *Základy verejnej správy*. Košice, 2008, s. 7

³ ADAMCOVÁ, M. *Teória verejnej správy*. Bratislava, 2018, s. 12

viacdimenzionálny charakter a tak je možné ju vnímať ako oblasť spoločenskej reality, ako vedeckú disciplínu a ako študijný odbor.

Z hľadiska spoločenskej reality je verejná správa porovnávaná v kontexte verejného sektora, pričom je verejný sektor chápaný ako oblasť spoločenskej reality nachádzajúcej sa vo verejnom vlastníctve a ktorej objektom sú spoločenské vzťahy, zahŕňajúc spoločenský život a vzťahy v rámci správania sa fyzických a právnických osôb k veciam verejným. Ak teda hovoríme o verejnej správe ako o oblasti spoločenskej reality považujeme ju za sociálny jav, ktorý je hlavne:

- typom dynamicky sa vyvíjajúcej komplexnej organizácie, ktorej základné úrovne sú tvorené orgánmi štátnej správy, samosprávy a orgánmi verejnoprávných korporácií, pričom jednotlivé orgány sú horizontálne i vertikálne usporiadané;
- je zaisťovateľom správy vecí verejných a to vo verejnom záujme a na verejný účet;
- ako praktická činnosť je prejavom výkonnej moci, ktorá je vymedzená právnymi reguláciami;
- je mediátorom medzi politickými komunitami a ich obyvateľmi, ako aj medzi politickými komunitami navzájom;
- zároveň je oblasťou ľudských vzťahov, v jej rámci dochádza k výmene najrozličnejších hodnôt a tak je nutné zdôrazniť, že objektom záujmu sú bežní ľudia a nie materiálne veci;
- je politicky ovplyvňovanou sférou a to nielen z hľadiska personálneho, ale aj materiálneho, organizačného a funkčného;
- je integrálnou, nevyhnutnou súčasťou akéhokoľvek štátneho útvaru.⁴

Z hľadiska vedeckej disciplíny sú základy verejnej správy v náuke o verejnej správe skúmajúcej činnosti a funkcie jednotlivých subsystémov verejnej správy a tak má výrazný interdisciplinárny charakter. Pohľad odborníkov na verejnú správu ako vednú disciplínu vychádza z dvoch rozdielnych konštelácií zastúpených na jednej strane Spojenými štátmi americkými a na strane druhej v rámci kontinentálnej Európy a tak je možné hovoriť o disciplinárnej a multidisciplinárnej paradigme.⁵

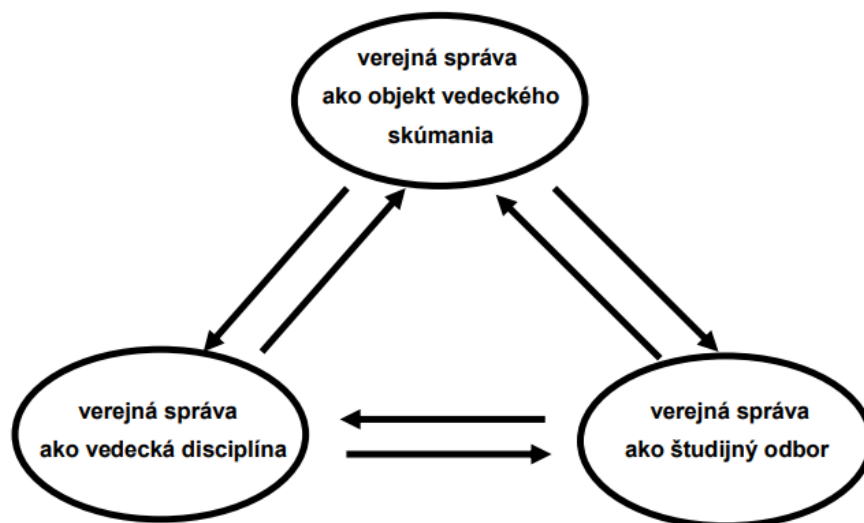
Z hľadiska verejnej správy ako študijného odboru, v rámci ktorého sa jedná hlavne o bádanie a štúdium jej rozličných oblastí prameniacych zo samostatnej požiadavky spoločnosti moderného štátu. Práve táto požiadavka má nielen vedecké, ale aj sociálne

⁴ MACHYNIÁK, J. *Verejná správa a verejná politika*. Trnava, 2020, s. 6 – 7

⁵ MACHYNIÁK, J. *Verejná správa a verejná politika*. Trnava, 2020, s. 6 – 7

prostredie, ktoré pramení v reformných procesoch štátu a správy siahajúcich až do 19. storočia.⁶

Obrázok 1 Významové dimenzie pojmu verejnej správy⁷



Najrozsiahlejšiu definíciu verejnej správy nájdeme v publikácii od Kosorína, ktorý ju definuje ako „*usporiadanú sústavu rozhodovacích procesov, politických, právnych, organizačných, rozpočtových a iných vzťahov a činností, ktorými verejnoprávne orgány ako právnické osoby na základe zákonom pridelených kompetencií transformujú, aplikujú, implementujú zákony štátu do konkrétnych práv a povinností jednotlivých fyzických a právnických osôb.*“⁸

Bolfíková hovorí o verejnej správe ako o type organizácie, ktorý zaist'uje špecifické služby pre občanov a na tomto základe ju definuje z hľadiska jej aktivít, a preto je možné povedať, že „*verejnej správe prislúcha pozícia realizátora výstupov, resp. outputov zákonodarnej moci.*“⁹

Gášpar definuje verejnú správu z hľadiska funkčného prístupu ako „*prvotné usporiadanie prostriedkov tak, aby sa dali využívať v záujme danej politickej komunity – štátu, regiónu, okresu, mesta či obce.*“¹⁰

⁶ MACHYNIÁK, J. *Verejná správa a verejná politika*. Trnava, 2020, s. 6 – 7

⁷ KLIMOVSKÝ, D. *Základy verejnej správy*. Košice, 2008, s. 9

⁸ KOSORÍN, F. 2003. *Verejná správa*. Bratislava, 2003, s. 31

⁹ BOLFÍKOVÁ, E. 2000. In: KOVÁČOVÁ, E. *Vplyv decentralizácie na výkon a riadenie územnej samosprávy v SR*. Banská Bystrica, 2020, s. 5

¹⁰ GAŠPAR, M. *Moderná verejná správa*. Bratislava, 1993, s. 16

Hamalová a kol. definujú verejnú správu nasledovne a to ako „*cieľavedomý druh ľudskej činnosti, ktorý je zameraný na zachovanie, rozvíjanie a starostlivosť o určité veci.*“¹¹

Kocks a kol. hovoria o verejnej správe, ako o časti výkonnej moci, ktorá je zodpovedná za implementáciu legislatívnych rozhodnutí. Pritom si však kladú otázku aká verejná je vlastne verejná správa? Čo je pre oblasť vlády stále samozrejmé, sa stále nevzťahuje na administratívne, najmä klasické orgány, v porovnateľnom zmysle. Stále však platí, že dodržiavanie transparentnosti je nevyhnutné a taktiež v rámci verejnej správy existujú osobitné podmienky, za ktorých verejná správa vykonáva svoju právomoc.¹²

2.2 Riadenie a organizácia verejnej správy

Riadenie v rámci verejnej správy prešlo v posledných dvoch desaťročiach viacerými zmenami a tak riadenie verejnej správy predstavuje akúkoľvek činnosť pracovníka verejnej správy, ktorá je zameraná na konkrétny objekt alebo proces, ako vykonávateľa činnosti subjektu správy, ktorý disponuje informáciami, s ktorými pracuje z dôvodu počiatočného podnetu či príčiny, ako napr. administratívne rozhodnutia, písomné odpovede a pod.

Riadiaci pracovník sa v rámci riadenia verejnej správy zameriavajú na dosiahnutie výsledkov a prijímanie zodpovednosti a tak je v jej koncepciách každý manažér vnímaný ako aktívny agent politického procesu, nie iba ako vykonávateľ daných politík.

Vzhľadom k vyššie uvedeným skutočnostiam je filozofia riadenia verejnej správy zameraná na nasledovné:

- nielen na kvantitu a kvalitu poskytovaných služieb, ale aj na ich účinok;
- na občana ako na hlavného zákazníka a spotrebiteľa verejnej služby;
- na efektívnosť vynaložených nákladov;
- na výsledok ako na výstupný efekt poskytnutej služby;
- na komplementaritu poskytovaného verejného produktu.

Jej subsystémy úzko súvisia s jej organizáciou a jedným z jej významným indikátorom je štátoprávne usporiadanie, v rámci ktorého sa rozlišujú hlavne unitárne štáty, ktoré sa vyznačujú tým, že ich územie sa nedelí na časti, ktoré by mali charakter a práva štátnych útvarov a zložené štáty, ktoré sa vyznačujú ústavnými inštitúciami, výrazne sa odlišujúcimi od inštitúcií unitárneho štátu a pre tento typ štátu je typický dualizmus

¹¹ HAMALOVÁ, M. a kol. *Teória, riadenie a organizácia verejnej správy*. Bratislava, 2014, s. 31

¹² KOCKS, K. Koll. *Öffentliche Verwaltung – Verwaltung in der Öffentlichkeit*. Wiesbaden, 2020, s. 243

rozhodovacích centier, v rámci ktorých je štátna moc rozdelená medzi orgány federácie a orgány členských štátov.¹³

Ďalšími významnými indikátormi tvorby organizačnej štruktúry verejnej správy na území daného štátu sú hlavne vývoj územného a správneho členenia, počet a veľkosť územných jednotiek, uplatňovaná miera decentralizácie, resp. centralizácie, politická situácia, rozsah originálnych, ale aj prenesených kompetencií, možnosti miestneho finančného systému a pod.¹⁴

Obrázok 2 Štruktúra verejnej správy v SR¹⁵

Verejná správa	Ústredná štátna správa	Ústredné orgány štátnej správy, na čele ktorých je člen vlády (ministerstvá napr. financií, školstva, zdravotníctva, kultúry a pod.)
		Ostatné ústredné orgány štátnej správy napr. Úrad vlády, Protimonopolný úrad, Štatistický úrad a pod.
	Miestna štátna správa	Úrady všeobecnej miestnej štátnej správy (obvodné úrady)
		Úrady špecializovanej miestnej štátnej správy (pozemkové úrady, lesné úrady a pod.)
	Územná samospráva	Miestna – obce
		Regionálna – vyššie územné celky
	Verejnoprávne korporácie	Ustanovené právnou normou rôznej sily napr. NBS, Matica slovenská, ARDAL a pod.

¹³ MACHYNIÁK, J. *Verejná správa a verejná politika*. Trnava, 2020, s. 16

¹⁴ NEUBAUEROVÁ, E., DUBROVINA, N. *Verejná správa v Slovenskej republike – aktuálne problémy*. Verejná správa 2010: sborník příspěvků z vědecké konference s mezinárodní účastí: Seč u Chrudimi, 20. – 21. 9. 2010. s. 156

¹⁵ NEUBAUEROVÁ, E., DUBROVINA, N. *Verejná správa v Slovenskej republike – aktuálne problémy*. Verejná správa 2010: sborník příspěvků z vědecké konference s mezinárodní účastí: Seč u Chrudimi, 20. – 21. 9. 2010. s. 157

2.3 Portál verejnej správy

Portál verejnej správy, resp. ústredný portál verejnej správy je dostupný na internetovej stránke <https://www.slovensko.sk>, na ktorom nájdú firmy, ako aj občania všetky potrebné informácie.

Ústredný portál verejnej správy (ďalej len „ÚPVS“) zaisťuje nielen centrálny, ale aj jednotný prístup k službám verejnej správy, ako aj k rozličným zdrojom informácií, ktoré tvoria v súčasnosti súčasť informačných serverov jednotlivých rezortov. Základným cieľom tohto portálu je služby a informácie zintegrovat' a za pomoci prehľadnej a prístupnej formy poskytnúť všetkým užívateľom.

ÚPVS je na základe zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) je definovaný ako *„informačný systém verejnej správy, prostredníctvom ktorého je možné centrálnne vykonávať elektronickú úradnú komunikáciu s ktorýmkoľvek orgánom verejnej moci a prístupovať k spoločným modulom, a to najmä prostredníctvom siete internet.“*¹⁶

Najvýznamnejšími úlohami tohto portálu je presmerovanie jeho užívateľov na využitie konkrétnej elektronickej služby verejnej správy za využitia relevantných zdrojov informácií.¹⁷

Vytvorenie tohto portálu bolo spolufinancované Európskou úniou z prostriedkov Európskeho fondu regionálneho rozvoja ako súčasť projektu *„Elektronické služby spoločných modulov ÚPVS a prístupových komponentov“*¹⁸ ako aj projektu *„Elektronické služby spoločných modulov ÚPVS a prístupových komponentov II.“*¹⁹

Prevádzkovateľom ÚPVS je Národná agentúra pre sieťové a elektronické služby (ďalej len „NASES“), ktorá je príspevkovou organizáciou Ministerstva investícií,

¹⁶ Slovensko. Zákon č. 305/2013 Z. z. elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente), § 5 ods. 2

¹⁷ O portáli. [online]. 2022. [cit. 2022-11-25]. Dostupné z WWW: <<https://www.slovensko.sk/sk/o-portali>>.

¹⁸ Projekt – Elektronické služby spoločných modulov ÚPVS a prístupových komponentov. 2012. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.uvo.gov.sk/vyhľadavanie-dokumentov/document/3153117/content/1186766/download>>.

¹⁹ Projekt II – Elektronické služby spoločných modulov ÚPVS a prístupových komponentov II. [online]. 2015. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://metais2.vicepremier.gov.sk/detail/Projekt/1919aafb-895a-4471-9bec-b72c834e62c4/cimaster?tab=basicForm>>.

regionálneho rozvoja a informatizácie Slovenskej republiky. Táto agentúra bola zriadená k naplneniu úloh plynúcich § 10 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy, ako aj § 4 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe, pričom sa jedná predovšetkým o naplnenie odborných úloh v oblasti informatizácie spoločnosti, správy a prevádzkovania elektronických komunikačných sietí a služieb pre Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.²⁰

NASES má niekoľko kľúčových kompetencií, ktorých súčasťou sú nasledovné:

- prevádzka a rozvoj siete GOVNET a sTESTA pre Slovensko, ako aj ÚPVS;
- rozvoj infraštruktúry širokopásmového internetu;
- poradenská, konzultačná, školiaca a sprostredkovateľská činnosť v oblasti informatiky, informačných sietí, elektronických komunikačných sietí a výpočtovej techniky.²¹

Správcom ústredného portálu bol do 1. januára 2019 Úrad vlády SR a následne do 1. júla 2020 Úrad podpredsedu vlády SR pre investície a informatizáciu, ktorý sa v zmysle § 40a zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy premenoval na Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.

Tento portál na základe zákona č. 305/2013 Z. z. umožňuje centrálné vykonávať elektronickú úradnú komunikáciu s akýmkoľvek orgánom verejnej moci a zároveň pristupovať aj k spoločným modulom formou internetu.²²

Súčasť ÚPVS tvorí digitálny obsah formou podporných informácií pre využívanie služieb, ako aj poskytovanie elektronických služieb, pričom sa obsah portálu riadi dvomi základnými princípmi a to:

1. organizácia informácií a služieb podľa okruhu životných situácií, na základe ktorej sú služby rozdelené z hľadiska logiky na základe toho, komu sú určené, ako napr. občan, podnikateľ alebo inštitúcia, ako aj okruhov životných situácií sprístupňujúcich informácie a služby v abecednom poradí a tak tento koncept

²⁰ O portáli. [online]. 2022. [cit. 2022-11-25]. Dostupné z WWW: <<https://www.slovensko.sk/sk/o-portali>>.

²¹ O portáli. [online]. 2022. [cit. 2022-11-25]. Dostupné z WWW: <<https://www.slovensko.sk/sk/o-portali>>.

²² Ústredný portál verejnej správy. [online]. 2022. [cit. 2022-11-25]. Dostupné z WWW: <<https://www.indprop.gov.sk/o-urade/elektronicke-sluzby/elektronicke-sluzby-vseobecne/ustredny-portal-verejnej-spravy-upvs>>.

umožňuje prístupovať k dostupným zdrojom štruktúrované a na základe požiadaviek používateľa a zároveň cielene filtrovať obsah portálu, pričom práve táto štrukturalizácia je rozhodujúcim prínosom portálu v súvislosti s distribuovanými informáciami na stránkach pripojených subjektov;

2. virtuálna centralizácia, ktorá tvorí centralizované riešenie, z ktorého sú dostupné všetky informácie a elektronické služby prístupné jednotným spôsobom, pričom centralizácia nie je riešená presunom služieb, ale jedná sa o jeden virtuálny centralizovaný systém tvoriaci integračnú platformu pre všetky služby.²³

2.3.1 Informačná časť

Informačná časť portálu ÚPVS dostupná internetovej stránke poskytuje, tak ako sme to už spomenuli vyššie a predstavuje jednotný prístup k informáciám a elektronickým službám rozdeleným do viacerých úrovní, ako napr. prihlásenie, vyhľadávanie má užívateľ prístup k požadovaným informáciám na základe jeho požiadaviek a tak si vyhľadať požadovaný obsah.

Po prihlásení je portál štruktúrovaný na základe cieľových skupín, pričom si ich môže používateľ vyhľadávať a selektovať na základe toho, či sa prihlási ako občan, podnikateľ alebo inštitúcia.²⁴

Úvodná časť portálu je rozdelená do logických častí, ktorých je celkovo 9 a patria k nim nasledovné:

1. Hlavička portálu súčasťou ktorej sú rôzne sekcie a to *O portáli* obsahujúca definíciu ÚPVS a jeho prevádzkovateľa, všeobecné podmienky prevádzky a poskytovania elektronických služieb, ďalej *Pomoc* obsahujúca návody a postupy, ako aj otázky a odpovede, sekciu *Kontakt*, ktorej súčasťou tvoria kontaktné údaje na Ústredné kontaktné centrum a napokon sekcie *Zmena kontrastu* a *English*, ktorej súčasťou tvoria vybrané informácie portálu ÚPVS v anglickom jazyku;
2. Prihlasovací panel, ktorý umožňuje prihlásenie na portál;
3. Bočný panel umožňujúci rýchly prístup do sekcií *Ako začať*, *Na stiahnutie*, *Životné situácie* a *Otázky a odpovede*, ako aj *Všeobecnú agendu*, ktorá slúži na realizáciu všeobecných elektronických podaní vybraných inštitúcií, *Nájsť službu*, za pomoci

²³ O portáli. [online]. 2022. [cit. 2022-11-25]. Dostupné z WWW: <<https://www.slovensko.sk/sk/o-portali>>.

²⁴ Návod na použitie portálu. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.slovensko.sk/sk/navody/navod-na-pouzitie/>>.

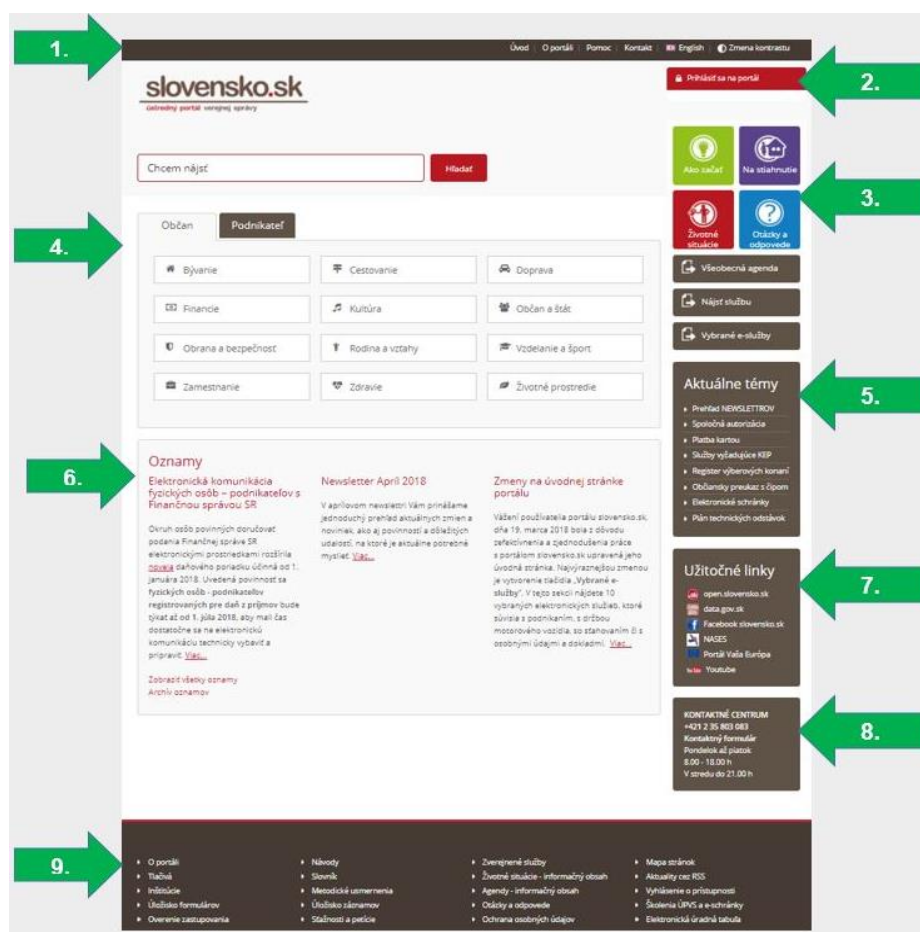
ktorej je možné vyhľadať konkrétne elektronické služby a napokon *Vybrané e-služby*, ktorých súčasť tvoria elektronické služby najčastejšie využívané v rámci praxe;

4. Hlavná navigácia tvoriaca elektronické služby rozdelené podľa životných situácií a cieľových skupín;
5. Aktuálne témy, ktorých súčasťou sú dôležité okruhy tém a otázok týkajúcich sa využívania elektronických služieb;
6. Oznamy obsahujúce aktuálne oznamy súvisiace s elektronickými službami a ich prevádzkou;
7. Užitočné linky poskytujúce prístup k externým portálom a sociálnym sieťam s ÚPVS;
8. Kontaktné centrum, ako napr. technická podpora, telefónne čísla, online formulár a úradné hodiny Ústredného kontaktného centra ÚPVS;²⁵
9. Pätička portálu obsahujúca odkazy na informačný obsah orgánov verejnej správy a redakcie ÚPVS, Dokumenty a tlačivá, kontaktné údaje inštitúcií, Návody a Video-návody, Metodické usmernenia, Slovník pojmov ÚPVS, Centrálné úložisko formulárov a záznamov, Overenie zastupovania právnickej osoby, postup pri podaní sťažnosti a petície, Elektronickú úradnú tabuľu a ďalšie – vid' obrázok 3.²⁶

²⁵ Návod na použitie portálu. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.slovensko.sk/sk/navody/navod-na-pouzitie/>>.

²⁶ Návod na použitie portálu. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.slovensko.sk/sk/navody/navod-na-pouzitie/>>.

Obrázok 3 Úvodná informačná stránka ÚPVS²⁷



2.3.2 Transakčná časť

Transakčná časť ÚPVS spočíva v prihlasovaní sa na portál. Pomocou tejto časti má každý užívateľ – občan, podnikateľ alebo inštitúcia prístup k vlastnej elektronickej schránke zriadenej zo strany ÚPVS. Táto elektronická schránka slúži každému používateľovi na komunikáciu s orgánmi verejnej moci.

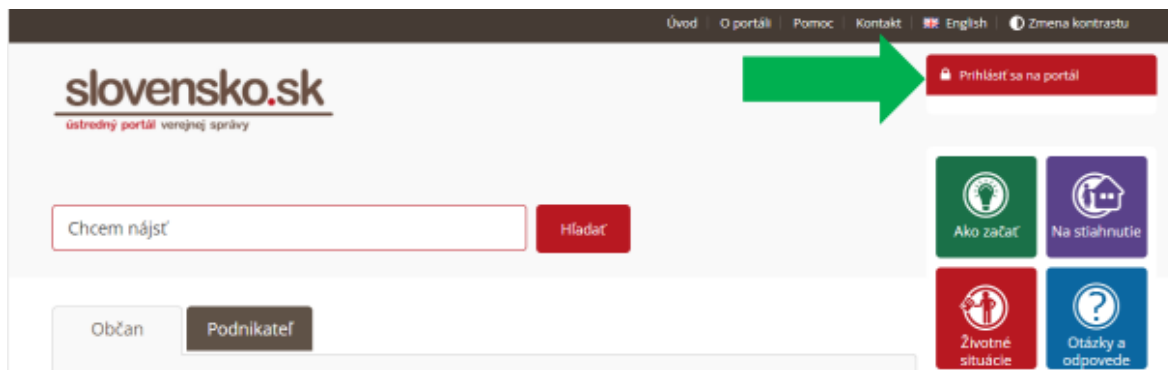
K prihláseniu sa do elektronickej schránky, ako aj na portál ÚPVS je potrebné disponovať nasledovnými:

- počítačom s internetovým pripojením;
- občianskym preukazom s elektronickým čipom alebo dokladom o pobyte s elektronickým čipom alebo iným alternatívnym autentifikátorom (ďalej len „eID“);
- čítačkou čipových kariet;

²⁷ Návod na použitie portálu. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.slovensko.sk/sk/navody/navod-na-pouzitie/>>.

- bezpečnostným kódom BOK a samozrejme aplikáciou eID a ovládačom k čítačke čipových kariet, ktoré musí mať nainštalovanú vo svojom počítači – vid' obrázok 4.²⁸

Obrázok 4 Prihlásenie na portál ÚPVS



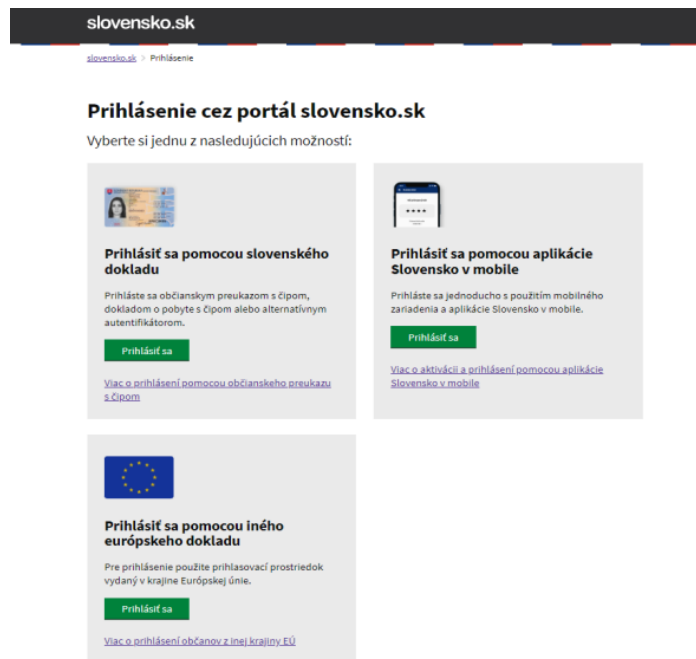
Po stlačení ikony *Prihlásiť sa na portál* sa používateľovi zobrazia tri možnosti prihlásenia, ktorými sú:

1. prihlásiť sa pomocou slovenského dokladu;
2. prihlásiť sa pomocou aplikáciou Slovensko v mobile;
3. prihlásiť sa pomocou iného európskeho dokladu – vid' obrázok 5.²⁹

²⁸ Prihlásenie cez portál slovensko.sk. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <https://www.slovensko.sk/_img/CMS4/Navody/postup_prihlasenie_na_portal.pdf>.

²⁹ Prihlásenie cez portál slovensko.sk. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <https://www.slovensko.sk/_img/CMS4/Navody/postup_prihlasenie_na_portal.pdf>.

Obrázok 5 Výber spôsobu prihlásenia³⁰



Na základe vyššie uvedených informácií funguje základná časť transakčnej časti ÚPVS, na základe ktorej sa každý užívateľ dostane do svojej elektronickej schránky. Pomocou nej môže následne elektronicky a predovšetkým bezpečne komunikovať s úradmi a orgánmi verejnej správy v rôznych oblastiach, ako napr. Financie – komunikácia s Finančnou správou, Rodina a vzťahy – komunikácia s Úradom práce, sociálnych vecí a rodiny a ďalšie.

³⁰ Prihlásenie cez portál slovensko.sk. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://prihlasenie.slovensko.sk>>.

3 E-GOVERNMENT

Informatizácia, digitalizácia alebo E-Government môže priniesť zvýšenú efektívnosť spočívajúcu buď v redukcii celkových výdavkov a alokovaním zdrojov do dôležitejších oblastí alebo môže poskytovať vyššiu kvalitu služieb zameranú na zákazníka alebo posilniť dôveru vo vládu na základe možnosti spojenia informácií a nezávislého vyhľadávania a transparentnosti.³¹

E-Government spočíva v zavádzaní informačno-komunikačných technológií do verejnej správy spolu s organizačnými zmenami, novými postupmi a zručnosťami za účelom zvýšenia efektívnosti pri poskytovaných službách, ako aj zvýšenia transparentnosti a posilnenia verejnej politiky, teda sa jedná o aktivity verejnej správy sprístupnené elektronicky a to cez príslušné informačné a komunikačné technológie.

V rámci e-Governmentu sa rozoznávajú štyri okruhy služieb verejnej správy, ktoré je možné realizovať aj v elektronickej a podobe a sú nimi:

- poskytovanie informácií občanom prostredníctvom internetu;
- obojsmerná komunikácia medzi úradom a občanmi či podnikateľmi a medzi úradmi navzájom;
- vykonávanie peňažných transakcií;
- E-governance alebo Správa vecí verejných, pri ktorej sa jedná o rozšírenie princípov E-governmentu aj na obyvateľstvo, vďaka čomu sa toto môže podieľať na správe vecí verejných prostredníctvom využívania informačných a komunikačných technológií.³²

E-Government býva definovaný za pomoci troch základných adresátov jeho výkonu, ktorými sú komunikácia medzi rôznymi časťami štátnej moci slúžiaca na zvýšenie efektívnosti výkonu štátnej moci za pomoci IKT, ako napr. rýchla výmena informácií medzi orgánmi verejnej moci a pod., ďalej je to komunikácia medzi štátnou mocou a podnikateľskou sférou obsahujúca použitie elektronických prostriedkov na zníženie nákladov pri obstaraní verejných statkov a napokon sa jedná o komunikáciu medzi štátnou

³¹ ŠPAČEK, D. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*. Praha, 2012, s. 19 – 20

³² E-Government. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/Sylaby/e-Government_power_point.pdf>.

mocou a občanmi obsahujúca používanie elektronických prostriedkov na poskytovanie služieb orgánov verejnej moci, ako napr. platenie súdnych a správnych poplatkov.³³

Na základe vyššie uvedeného je k dispozícii niekoľko definícií tohto termínu. Pre účely našej práce si ich uvedieme len niekoľko.

E-Government pochádza z anglického slova *electronic government*, teda elektronickej vlády a jedná sa „o elektronicú interakciu, na ktorej sa účastní verejná správa a pri ktorej sa využívajú informačné a komunikačné technológie a ktorej cieľom je lepšie, lacnejšie, spoľahlivejšie a efektívnejšie poskytovanie služieb verejnej správy.“³⁴

Pod pojmom elektronická vláda sa rozumie „využívanie elektronických prostriedkov vo všetkých troch oblastiach výkonu štátnej moci, teda zákonodarnej, výkonnej ale aj súdnej.“³⁵

Portál eGov.sk tento termín definuje ako „elektronická forma výkonu verejnej správy prostredníctvom informačno-komunikačných technológií (ďalej len „IKT“).“³⁶

Lidinský definuje e-Government ako „využívanie informačných technológií verejnými inštitúciami pre zaistenie výmeny informácií s občanmi, súkromnými organizáciami a inými verejnými inštitúciami za účelom zvyšovania efektivity vnútorného fungovania a poskytovania rýchlych, dostupných a kvalitných informačných služieb.“³⁷

História tohto termínu sa v rámci Slovenska začala po prijatí zákona č. 261/1995 Z. z. o informačných systémoch verejnej správy, pričom samotný termín nie je v slovenskej právnej úprave jednoznačne definovaný aj napriek tomu, že tvorí súčasť strategických dokumentov vlády Slovenskej republiky (ďalej len „SR“), ktoré sa venujú informatizácii spoločnosti, verejnej správy a informačnej bezpečnosti.

Jeho ekvivalentnými pojmami sú napr. elektronická verejná správa, elektronicizácia verejnej správy a elektronická vláda, ktorý tento pojem definujú ako „využívanie informačných a komunikačných technológií on-line vo verejnej správe spojené

³³ ŠEBESTA, M. a kol. *eGovernment a jeho vplyv na podnikateľský sektor*. Bratislava, 2020, s. 11

³⁴ BIZNÁR, M. 2018. Čo je to e-Government, utópia pre Slovensko? [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.techbox.sk/co-je-to-e-government-utopia-pre-slovensko/>>.

³⁵ ŠEBESTA, M. a kol. *eGovernment a jeho vplyv na podnikateľský sektor*. Bratislava, 2020, s. 11

³⁶ eGov.sk. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://portal.egov.sk/sk/content/egovernment>>.

³⁷ LIDINSKÝ, V. a kol. *eGovernment bezpečne*. Praha, 2008, s. 7

*s organizačnými zmenami a novými zručnosťami s cieľom zlepšiť služby verejnej správy a uplatňovanie demokratických postupov, ako aj posilniť podporu verejných politík.*³⁸

Pre vývoj e-Governmentu na Slovensku sú kľúčovými dokumentmi dva, ktorými sú Stratégia digitálnej transformácie Slovenska 2030, ktorej cieľom je, aby sa slovenská spoločnosť premenila z industriálnej spoločnosti na spoločnosť informačnú, pričom kladie dôraz na rozvoj inovatívnych technológií ako technológia 5G, veľké dáta a analytické spracovanie dát, technológia block-chain, super-výkonné počítače a umelá inteligencia, ako aj Akčný plán digitálnej transformácie Slovenska na roky 2019 – 2022, ktorého priority spočívajú v oblasti elektronizácie verejnej správy a konkrétne v:

- zmodernizovaní a zjednodušení právneho rámca v oblasti údajov – príprava nového zákona o údajoch;
- vybudovaním konsolidovanej analytickej vrstvy a sprístupnenie dôležitých analytických nástrojov pre potreby inštitúcií verejnej správy na tvorbu verejných politík na základe údajov;
- vytvorením systému na zdieľanie priestorových informácií;
- testovaním použitia technológie blockchain vo verejnej správe v pilotných projektoch.³⁹

3.1 E-Government zákon

Zákon, ktorý v rámci SR upravuje e-Government je v súčasnosti zákon č. 305/2013 Z. z. . o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente), ktorý vstúpil do platnosti dňa 01. novembra 2013 a v SR tak položil základy právnej úpravy elektronickej podoby výkonu pôsobnosti orgánov verejnej moci.

Hlavný cieľ tejto právnej úpravy spočíval vo vytvorení právneho prostredia pre uskutočnenie výkonu verejnej moci elektronicou formou a tak zjednodušiť, zrýchliť, sprehľadniť a zjednotiť komunikačné procesy a tak odstrániť nadbytočnú fragmentáciu právnej úpravy.

V rámci a v podmienkach SR tento zákon predstavuje prvý právny predpis kodifikujúci elektronicú komunikáciu ako ťažiskovú formu komunikácie s verejnou mocou

³⁸ GREGUŠOVÁ, D., HALÁSOVÁ, Z. *Zákon o e-Governmente – Komentár*. Bratislava, 2018, s. 4

³⁹ ŠEBESTA, M. a kol. *eGovernment a jeho vplyv na podnikateľský sektor*. Bratislava, 2020, s. 15 – 19

a taktiež aj komunikáciu v rámci orgánov verejnej moci navzájom, a to popri historickej základnej, doteraz stále rozhodujúcej a nevyhnutnej klasickej listinnej, resp. papierovej podobe.⁴⁰

Týmto zákon však nedochádza k nahradeniu už existujúcich právnych predpisov, ktoré upravujú občianskoprávne, trestnoprávne a správne konanie novou právnou úpravou, ktorá je zameraná výlučne len na elektronickú formu, ako napr. doručovanie, podanie alebo konverziu dokumentov a zároveň vytvoril aj funkčný model elektronických služieb orgánov verejnej moci a správy a za pomoci prijatých ustanovení dokázal prepojiť základné registre verejnej správy a tak vytvoriť spoločné modelové rozhranie pre interoperabilitu a využívanie už dostupných súborov dát a údajov, ktoré sa v nich nachádzajú.⁴¹

Zákon o e-Governmente upravuje niektoré informačné systémy pre výkon pôsobnosti orgánov verejnej moci v elektronickej podobe, elektronické podanie, elektronický úradný dokument a niektoré podmienky a spôsob výkonu verejnej moci elektronicky a elektronickej komunikácie, elektronické schránky a elektronické doručovanie, identifikáciu osôb a autentifikáciu osôb, autorizáciu, zaručenú konverziu, referenčné registre a spôsob vykonania úhrady orgánu verejnej moci.⁴²

Zákon o e-Governmente sa skladá celkovo zo siedmich základných častí, ktorými sú:

1. Základné ustanovenia upravujú § 1 – 3 a tvoria ich predmet a pôsobnosť zákona, ako aj vymedzenie základných pojmov;
2. Informačné systémy pre podporu výkonu verejnej moci elektronicky a elektronické schránky upravujú § 4 – 16 zákona o e-Governmente a obsahom týchto paragrafov sú základné ustanovenia, prístupové miesta, ústredný portál, informačný systém, spoločné moduly, elektronické schránky – jej zriadenie, deaktiváciu, zrušenie a aktiváciu a prístup;
3. Výkon verejnej moci elektronicky upravujú § 17 – 34 tohto zákona, ktorých súčasťou sú základné ustanovenia, notifikácie, elektronická identita osoby a jej preukazovanie, ako aj identifikáciu osoby, autentifikátor, elektronické podanie a dokument, ako aj elektronické doručovanie;

⁴⁰ GREGUŠOVÁ, D., HALÁSOVÁ, Z. *Zákon o e-Governmente – Komentár*. Bratislava, 2018, s. 4

⁴¹ GREGUŠOVÁ, D., HALÁSOVÁ, Z. *Zákon o e-Governmente – Komentár*. Bratislava, 2018, s. 4

⁴² Slovensko. Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente), § 1.

4. Konverziu, ktorej úpravu obsahujú § 35 – 39 a ich súčasť tvorí konverzia a zaručená konverzia, ako aj jej postup, obmedzenie, osvedčovací doložku a spoločné ustanovenia o konverzii;⁴³
5. Úhrady orgánom verejnej moci sú úpravou § 40 – 44, pričom súčasťou týchto paragrafov sú základné pojmy, pôsobnosť, príkaz na úhradu, ako aj vykonanie úhrad cez osvedčujúcu osobu a povinnosti správcu komunikačnej časti platobného modulu;
6. Referenčné registre sú upravené v § 49 – 55 tohto zákona a upravujú referenčné registre a zoznam referenčných údajov spolu s jeho používanými hodnotami, ako aj opravy týchto hodnôt a zdrojových údajov, ďalej povinnosti správcu a registrátora registra, stotožnenie údajov a poskytovanie hodnôt údajov z registra;
7. Spoločné, prechodné a záverečné ustanovenia, ktoré sú v príslušnom zákone upravené v § 56 a 61a a súčasťou týchto paragrafov sú všetky prechodné ustanovenia tohto zákona, ktoré vstúpili do platnosti počas jeho existencie, čiže od roku 2013, ako aj zrušovacie ustanovenia, pričom súčasť tejto časti zákona tvoria aj správne delikty a ich kontrola, postupy, ochrana osobných údajov a splnomocňovacie ustanovenia.⁴⁴

3.2 Štruktúra, princípy a faktory verejnej správy

V rámci informačného systému verejnej správy a jej správneho fungovania vystupujú dve strany a to orgány verejnej správy a iné orgány verejnej správy alebo ďalšie subjekty. Kvôli lepšej prehľadnosti komplikovaných interakčných vzťahov sú strany zúčastnených na týchto vzťahoch rozdelené na štyri segmenty, ktorými sú:

1. G2P – Government to Public je interakcia medzi verejnou správou a verejnosťou skladajúca sa z dvoch zložiek a to:
 - G2C – Government to Citizen, resp. komunikácia medzi verejnou správou a občanmi, ktorá má zaistiť prístup občanov k informáciám a službám verejnej správy, ako napr. vybavovanie dokladov,
 - G2B – Government to Businesses, resp. komunikácia medzi verejnou správou a podnikateľským sektorom, pričom sa v prvom rade jedná o efektívnejšie verejné

⁴³ Slovensko. Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente), § 1.

⁴⁴ Slovensko. Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

obstarávanie alebo posielanie výkazov elektronickou formou, ako napr. daňové priznania;⁴⁵

2. G2G – Government to Governments, resp. elektronická komunikácia medzi dvomi a viacerými inštitúciami verejnej správy s ohľadom na komunikáciu medzi rôznymi úrovňami verejnej správy, ako napr. Ministerstvo kultúry SR a Krajský pamiatkový úrad;
3. G2E – Government to Employees alebo aj komunikácia v rámci subjektov verejnej správy obsahujúca problematiku elektronickej podateľne;
4. G2A – Government to Administration, teda komunikácia medzi verejnou správou a ostatným okolím.⁴⁶

Verejná správa je na základe jej subjektov aj poskytovateľom špecifických elektronických služieb, v rámci ktorých môžu prebiehať štyri aktivity, resp. formu e-Governmentu, ku ktorým patria informačné služby poskytujúce všeobecné informácie občanom a podnikateľom cez internet, pričom verejná správa výrazne zjednodušila prístup verejnosti k týmto službám. Ďalej sú to komunikačné služby na obojstrannej úrovni na účely ktorej sa využíva elektronická schránka, ako aj platobné služby, pri ktorých sa jedná o realizáciu peňažných transakcií vo verejnej správe, ako napr. hradenie správnych poplatkov.

Poslednou službou, resp. aktivitou verejnej správy v rámci poskytovanie špecifických služieb je správa vecí verejných, ktorej predchádzajú jej štyri vyššie uvádzané formy. Táto piata otvára možnosť priamej účasti občanov na správe vecí verejných a jej obsahom je rozšírenie princípov e-Governmentu na obyvateľov, a ktorá súvisí s vyjadrením podľa ktorého je e-Government procesom zmeny vrchnostenskej verejnej správy na verejnú správu chápanú ako službu verejnosti.⁴⁷

Aby boli dosiahnuté základné ciele e-Governmentu verejnej správy je nutné, aby boli dodržané nasledovné princípy, ktorých súčasť tvoria:

- služby občanom, nakoľko poskytovanie služieb má byť zamerané na občanov a nie obrátené proti nim;

⁴⁵ SOPÚCHOVÁ, S. *Informatizácia verejnej správy e-Government*. Bratislava, 2021, s. 47

⁴⁶ SOPÚCHOVÁ, S. *Informatizácia verejnej správy e-Government*. Bratislava, 2021, s. 47

⁴⁷ SOPÚCHOVÁ, S. *Informatizácia verejnej správy e-Government*. Bratislava, 2021, s. 47 – 48

- efektívnosť, nakoľko by mali byť služby poskytované elektronicky efektívnejšie ako konvenčne poskytované služby a tak musí aj verejná správa prehodnocovať už existujúce administratívne procesy;
- bezpečnosť, pretože elektronická komunikácia je uskutočňovaná na základe bezpečnostnej politiky riadenej pravidlami a praktikami a v súlade s dokumentom 2001/264/EC;⁴⁸
- transparentnosť súvisiaca so všetkými zúčastnenými do procesu plánovania a zavedenia internetových služieb, ako aj zaistenia dostupnosti pre všetkých vrátane znevýhodnených skupín;
- ochrana súkromia zaisťujúca ochranu osobných údajov;
- viacúrovňová spolupráca spočívajúca v zaistení vzájomnej komunikácie pre všetky systémy za dodržania Európskeho rámca interoperability, ako aj dostupných medzinárodných štandardov a riešení;
- používanie Open standards ako prostriedkov na dosiahnutie interoperability;
- technologická a softvérová neutralita, ktoré musia byť prístupné novým technológiám.⁴⁹

Podobne ako aj v iných krajinách, aj v SR vplýva na e-Government viacero faktorov, ku ktorým patria faktory ekonomické, politické a technologické, zákonný rámec, sociálne a kultúrne faktory, akcelerátory a inhibítory.

Ekonomické faktory majú dopad hlavne na firmy a domácnosti, v ktorých sa nachádza počítač, ako aj na vývoj trhu v súvislosti s internetovými službami. Na základe rýchleho hospodárskeho rastu dochádza k navýšeniu počtu počítačov a pripojení na internet, pričom sa očakáva, že ekonomický rast bude aj naďalej narastať. Narastajúci záujem inštitúcií o online služby súvisí so zvýšeným záujmom týchto firiem o tieto služby a tak musia zamestnávať aj zamestnancov z oblasti IKT.⁵⁰

Technologické faktory súvisia s používaným softvérom a hardvérom v jednotlivých inštitúciách verejnej správy, pričom do roku 2006 neexistoval žiadny zákon upravujúci a určujúci štandardy používaných systémov, čo viedlo k ich značnej rozmanitosti, resp.

⁴⁸ Princípy e-Gov. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<http://info.egov.sk/node/90>>.

⁴⁹ Princípy e-Gov. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<http://info.egov.sk/node/90>>.

⁵⁰ BELÁŇOVÁ, V. a kol. Otvorený softvér vo verejnej správe SR. *Dialógy o ekonomike a riadení*. 2006, č. 24.

k skutočnosti, že každá vládna inštitúcia využíva iný a tak je aj kvalita služieb rôzna, čo súvisí aj s hackerskými útokmi.

Politické faktory, ktoré mali značný vplyv na zavedenie e-Governmentu a až v roku 2004 vznikla prvá inštitúcia venujúca sa problematike informačnej spoločnosti. Pomalý pokrok na úrovni samospráv spôsobila decentralizácia a presun kompetencií z jednej inštitúcie na druhú, pričom e-Government v rámci samospráv zastáva čoraz väčšiu pozornosť.⁵¹

Sociálne a kultúrne faktory, ktoré súvisia s orientovaním sa na občana a klienta, čo bol donedávna na SR vážny problém, nakoľko štátny sektor nemá záujem o zmeny a inštitúcie nechceli poskytovať online služby, čo sa však zavedením zákona z roku 2013 v značnej miere zmenilo.

Akcelerátory súvisiace so zvýšeným záujmom niektorých segmentov spoločnosti o online služby. Toto úzko súvisí s rýchlejšim rozvojom e-Governmentu, ako aj lepšom spravovaní a transparentnosti a slobodnému prístupu k informáciám. Za dôležitý zdroj podpory rozvoja je považované aj jeho financovanie zo štrukturálnych fondov Európskej únie, ako aj snaha o zlepšenie podnikateľského prostredia s cieľom prilákania zahraničných investorov a podpory domácich podnikateľov.⁵²

Inhibítory, ktoré úzko súvisia s reformou verejného sektora a skvalitnenia služieb občanom, nakoľko bez ďalších zmien vo verejnej správe súvisiacimi s informatizáciou a rozšírením e-Governmentu nedôjde k zlepšeniu kvality poskytovania online služieb.⁵³

3.3 Elektronické služby a informačné systémy verejnej správy

Vývoj elektronických služieb verejnej správy zaznamenal na celom svete značný nárast a tak je možné povedať, že jeho hlavnou podstatou je využívanie IKT vo verejnej správe s cieľom zlepšenia jej služieb. V dnešnej dobe pracuje verejná správa hlavne z termínmi e-government alebo e-governance, ktoré sú už medzinárodnými pojmami.⁵⁴

⁵¹ BELÁŇOVÁ, V. a kol. Otvorený softvér vo verejnej správe SR. *Dialógy o ekonomike a riadení*. 2006, č. 24.

⁵² VELŠIC, M. *E-Government na Slovensku*. Bratislava, 2008.

⁵³ SALNER, A., MIŠINA, J. *Stav eGovernmentu na Slovensku, príčiny a riešenia: výskumná správa*. [online]. Bratislava: Inštitút pre dobre spravovanú spoločnosť, 2007. [cit. 2022-11-26]. Dostupné z WWW: <https://www.governance.sk/wp-content/uploads/2016/10/eGov_sk.pdf>.

⁵⁴ OCHRANA, F. a kol. *Veřejná správa*. Brno, 2015, s. 542

Z pohľadu Európskej únie spočívalo toto zlepšenie hlavne v poskytovaní služieb elektronickou formou. Na tomto základe sa rozlišuje šesť úrovní elektronických služieb a to:

- Úroveň 0, kedy nie je služby online elektronicky dostupná;
- Úroveň 1, informácia na začatie služby je v elektronickej forme dostupná, ako napr. miesto, čas a spôsob vybavenia služby, ale služba sa elektronicky neposkytuje a ani k nej nie je dostupný elektronický formulár;
- Úroveň 2, v ktorej už dochádza k jednostrannej komunikácii, v ktorej je možné si už stiahnuť na príslušnej webovej stránke príslušný úrad online, ale podanie ešte nie je možné spraviť elektronicky;⁵⁵
- Úroveň 3, v ktorej dochádza k obojstrannej komunikácii s vybavovaním služieb elektronicky, avšak pri preberaní výsledku je nutný osobný alebo listinný kontakt;
- Úroveň 4 umožňujúca plynulé vybavenie elektronickou formou a to vrátane rozhodnutia, zaplataenia alebo doručenia výsledku, ak je to nutné, pričom je vylúčený akýkoľvek osobný alebo listinný kontakt;
- Úroveň 5, ktorá má funkčnosť úrovne 3 alebo 4 a najviac používanými sú personalizované nastavenia užívateľov.⁵⁶

Vzhľadom na jednotlivé úrovne fungovania eGovernmentu vo verejnej správe je nutné aj zabezpečenie právnych a technických podmienok pre jeho správne fungovanie. Aj vzhľadom k tomuto došlo k prijatiu potrebnej podpory z oblasti legislatívy, ako napr. informačné systémy verejnej správy, elektronické schránky, dokumenty, doručovanie a veľa ďalších.

Informačné systémy verejnej správy tvoria primárny a kľúčový prvok modernizácia verejnej správy, pričom aspekt IKT je možné pozorovať aj v tejto oblasti. Aj úpravu týchto systémov nájdeme v príslušnom zákone o eGovernmente a konkrétne skutočnosť, ako musia orgány verejnej moci povinné zabezpečiť vytvorenie a prechádzku nasledovných systémov:

- prístupových bodov, ktorými sú komunikačné rozhrania, za pomoci ktorých sa realizuje elektronická komunikácia a ktoré sú určené na zaistenie kontaktu medzi orgánom verejnej správy a občanmi, ako napr. ÚPVS, špecializovaný portál, integrované obslužné miesto alebo ústredné kontaktné centrum;
- spoločných modulov, ktorými sú informačné systémy verejnej správy centrálnie zaisťujúce jednotný výkon základných funkcií elektronickej komunikácie a na účely

⁵⁵ SOPÚCHOVÁ, S. *Informatizácia verejnej správy e-Government*. Bratislava, 2021, s. 52 – 53

⁵⁶ SOPÚCHOVÁ, S. *Informatizácia verejnej správy e-Government*. Bratislava, 2021, s. 52 – 53

- výkonu verejnej správy elektronickou formou, ako napr. platobný a autentifikačný modul, modul elektronického doručovania a ďalšie;
- agendových systémov, ktoré sú tiež informačnými systémami verejnej správy a ktoré sú ňou aj spravované a určené na zaistenie výkonu verejnej správy v rozsahu pôsobnosti a oprávnení týchto orgánov.⁵⁷

3.4 Výhody a nevýhody e-Governmentu

Rovnako ako väčšina prvkov informačnej spoločnosti aj e-Government má svoje výhody a nevýhody, resp. pozitíva a negatíva.

Medzi výhody e-Governmentu patria ľahká dostupnosť informácií, vyššia rýchlosť prenosu, eliminácia vzdialenosti, uľahčenie styku verejnosti s úradmi. Vďaka evidencii základných registrov nebude musieť občan zadávať stále rovnaké údaje na jednotlivých úradoch pomocou prepojenosti jednotlivých úradov. Neskôršie zmeny si už úrady dokážu vymeniť medzi sebou navzájom a každá takáto zmena je automaticky zaznamenaná vo všetkých registroch.⁵⁸

Podľa Peterku je takýchto výhod viac a siahajú až od prehľadnejšieho podnikateľského prostredia, možného skrátenia na možnosť začatia podnikania, až po flexibilnejšiu komunikáciu medzi úradmi, do ktorých nie je nutné ísť osobne. Medzi ďalšie výhody patrí aj minimalizácia chýb a odstránenie viacnásobného uskutočňovania rovnakých úkonov.⁵⁹

Na druhej strane medzi nevýhody e-Governmentu patria zhoršujúca sa dostupnosť internetu, upadajúca kvalita poskytovaných služieb na lokálnej úrovni, ako aj netransparentnosť verejných zákaziek e-Governmentu, ako napr. realizácia základných registrov,

Pre efektívne fungovanie e-Governmentu je potrebná aj skutočnosť, jeho využívania zo strany občanov, čo však nie je možné, ak nie takýto typ pripojenia dostupný v celej krajine. K nevýhodám patrí aj nedostatočná digitálna gramotnosť staršej generácie, obyvateľov s nižším vzdelaním, ako aj úradníkov. Niektorí občania sú skeptickí ohľadom

⁵⁷ SOPÚCHOVÁ, S. *Informatizácia verejnej správy e-Government*. Bratislava, 2021, 54 – 55

⁵⁸ Co je to e-Government? [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://sites.google.com/site/cojetoegov/vyhody-a-nevyhody-e-governmentu>>.

⁵⁹ PETERKA, J. *Báječný svet elektronického podpisu*. Praha, 2011. s. 48

bezpečnosti uloženia a prenosu dát a osobných údajov cez internetu a iní zas spochybňujú spoľahlivosť poskytovaných informácií online a uprednostňujú priamy kontakt s úradníkmi a to buď telefonickou formou alebo osobne.⁶⁰

Madleňáková, Madleňák uvádzajú nasledovné výhody a nevýhody e- Governmentu, ktoré zobrazuje nasledujúci obrázok 6.⁶¹

Obrázok 6 Výhody a nevýhody e-Governmentu⁶²

Výhody	Nevýhody
Rýchlosť procesov vo verejnej správe	Neosobnosť – absencia osobného kontaktu
Kvalitnejšie služby	Nedostatočná digitálna gramotnosť
Väčšia účasť občanov (vyjadrenie názorov)	Možnosť straty dát
Menšia spotreba papiera	Nekompatibilita s niektorými systémami
Menšie náklady na prevádzkovanie	Možnosť zachytenia dát neautorizovanými osobami
Lepšia informovanosť obyvateľstva	Náklady na vzdelávanie obyvateľstva
Nepretržitá dostupnosť	
Nové služby	
Menšia nezamestnanosť	

⁶⁰ Co je to e-Government? [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://sites.google.com/site/cojetoegov/vyhody-a-nevyhody-e-governmentu>>.

⁶¹ MADLEŇÁKOVÁ, L., MADLEŇÁK, R. 2012. Analýza využívania služieb e-Governmentu v SR. *Pošta, Telekomunikácie a Elektronický obchod*. II/2012, s. 59

⁶² MADLEŇÁKOVÁ, L., MADLEŇÁK, R. 2012. Analýza využívania služieb e-Governmentu v SR. *Pošta, Telekomunikácie a Elektronický obchod*. II/2012, s. 59

4 ELEKTRONICKÁ KOMUNIKÁCIA VO VEREJNEJ SPRÁVE A JEJ ZABEZPEČENIE

Elektronická komunikácia je v dnešnej modernej dobe plnej technologického pokroku považovaná za najefektívnejší druh komunikácie, ktorú využívajú skoro všetky organizácie pre efektívnu komunikáciu. Táto prebieha rozličnými formami, ktoré si priblížime v rámci tejto kapitoly.⁶³

Pri elektronickej komunikácii vo verejnej správe sa zameriame na túto formu komunikácie v rámci dvoch vybraných krajín a to Českej a Slovenskej republiky, v ktorých budeme porovnávať jednotlivé druhy komunikácie, ako aj elektronické schránky, bezpečnú komunikáciu, elektronický podpis a napokon elektronické certifikáty a značky.

4.1 Druhy elektronickej komunikácie

V rámci elektronickej komunikácie sa využíva niekoľko druhov komunikovania. Jedným z najrozšírenejších je v rámci analyzovaných krajín – Českej a Slovenskej republiky, elektronická pošta, resp. e-mail. Tento typ komunikácie označuje systém neinteraktívnej komunikácie textov, údajov, obrazov a aj reči medzi odosielateľom a príjemcom elektronickej pošty. Elektronickú poštu je možné poslať dvomi spôsobmi a to prostredníctvom lokálnej počítačovej siete – intranetu a prostredníctvom internetu do každej komerčnej siete.⁶⁴

S neustálym rozširovaním možností internetu a zároveň za pomoci dokonalejšieho technického vybavenia už plní elektronická pošta význam telefonického alebo faxového spojenia, nakoľko správu, ktorú prostredníctvom elektronickej pošty odošleme dostane adresát na celom svete už počas niekoľkých minút, a preto je možná komunikácia prostredníctvom elektronickej pošty s účastníkmi na celom svete a teda aj medzi našimi analyzovanými krajinami aj medzi jednotlivými verejnými správami – teda slovenskou a českou.

Tento typ komunikácie je v dnešnej modernej dobe už uprednostňovaný pred telefonickou komunikáciou. Každý užívateľ elektronickej pošty musí mať na internetovom serveri založenú elektronickú schránku, ktorá je jedinečná. Táto schránka musí na vybranom

⁶³ HARAUSOVÁ, M. a kol. *Teória, riadenie a organizácia verejnej správy*. Košice, 2014, s. 47

⁶⁴ HARAUSOVÁ, M. a kol. *Teória, riadenie a organizácia verejnej správy*. Košice, 2014, s. 47

serveri fungovať a jej spojenie so serverom musí byť zabezpečené pre správny prístup k elektronickej schránke a k správam, ktoré sa v nej nachádzajú. Každý e-mail zasielaný prostredníctvom elektronickej pošty pozostáva z troch hlavných častí:

- prvá časť je e-mailová adresa, ktorú je povinné zadať, pretože stanovuje príjemcu správy;
- druhá časť je predmet, pričom táto časť e-mailu nie je povinná a hovorí o téme, ktorá je predmetom správy;
- tretia časť je samotný text e-mailu, ktorý chceme adresovať príjemcovi, avšak jej súčasťou môže byť aj prílohu, ktorá môže tvoriť ľubovoľné dáta v obmedzenom objeme.⁶⁵

Podobne ako pre niekoho má bežná forma komunikácie svoje výhody a nevýhody, aj komunikácie prostredníctvom elektronickej pošty má svoje nevýhody, ku ktorým patria hlavne veľké množstvo nevyžiadaných správ, šírenie nepravdivých neúplných a zavádzajúcich informácií a správ, nesprávna interpretácia informácií alebo správ obdržaných prostredníctvom elektronickej pošty, neexistencia medziľudských vzťahov a mnoho ďalších.⁶⁶

V prípade druhej elektronickej komunikácie, ktorá je v oboch krajinách využívaná, je IP telefónia, resp. telefonovanie cez internet, vďaka ktorému môžeme taktiež komunikovať s rozličnými osobami na celom svete. Pomocou tejto formy komunikácie sa prenáša hlas internetovou sieťou formou signálu, pričom sa jedná o priamy spôsob komunikácie.

Vzhľadom na tento spôsob komunikácie sa využíva veľké množstvo počítačových programov, z ktorých je najznámejší Skype. Aj napriek jeho rozšírenosti musíme skonštatovať, že v rámci verejnej správy, táto forma komunikácie nie je až taká využívaná, nakoľko jej zabezpečenie nie je verejnú správu dostačujúce.⁶⁷

Ak sa zameriame na elektronickú komunikáciu verejnej správy musíme podotknúť, že táto prebieha, v súvislosti s informáciami, ktoré sa prostredníctvom nej zasielajú, prostredníctvom elektronických alebo dátových schránok, ktoré si priblížime neskôr v rámci kapitoly 4.3. Tieto schránky sú pri komunikácii využívané v rámci nami skúmaných krajín

⁶⁵ BOCAK, M. a kol. Texty elektronických médií: Stručný výkladový slovník. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<http://obornik.sk/images/Slovník.pdf>>.

⁶⁶ HARAUSOVÁ, M. a kol. *Teória, riadenie a organizácia verejnej správy*. Košice, 2014, s. 50

⁶⁷ Elektronická komunikace. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.sslch.cz/files/163/3-elektronicka-komunikace-u.pdf>>.

v komunikácii medzi orgánom a účastníkmi konania, resp. medzi občanom/ podnikateľom a verejnou správou. V prípade komunikácie verejnej správy s iným orgánom verejnej moci, ktorý v konkrétnom prípade nie je účastníkom konania, môžu komunikovať aj mimo schránok, a to za pomoci modulu úradnej komunikácie alebo iným "priamym" spôsobom, ako napr. telefonicky.⁶⁸

Pri elektronickej komunikácii s verejnou správou sa v Českej republike (ďalej len „ČR“) využívajú Elektronická podateľňa, Czech POINT, Portál verejnej správy a napokon už spomenuté Dátové schránky. Elektronická podateľňa je webová aplikácia, ktoré je dostupná od roku 2007 a je určená pre odosielanie podania v elektronickej forme spolu s prílohami súdom. Určená je užívateľom využívajúcim elektronický podpis, teda zaručený elektronický podpis na kvalifikovanom certifikáte alebo kvalifikovaný elektronický podpis na základe ustanovenia § 6 ods. 1 a 2 zákona č. 297/2016 Sb., o službách vytvárajúcich dôveru pre elektronické transakcie v znení neskorších predpisov.⁶⁹

Tento typ podateľni ponúka nepretržitú možnosť realizácie elektronického podania voči orgánom verejnej správy, ktoré je možné podať počas 24 hod. a to až 7 dní v týždni. Jej fungovanie je spájané s princípom už spomenutého elektronického podpisu. Každý z nás tak môže s verejnou správou komunikovať z pohodlia domova alebo kancelárie.

V prípade Czech POINT sa jedná o Český podací overovací a informačný národný terminál, ktorý je asistovaným miestom výkonu verejnej správy v rámci ktorého obecné úrady, krajské úrady, notári a ďalšie právnické osoby môžu ľuďom vydávať výpisy, založiť dátovú schránku, autorizovane konvertovať dokument či podať podanie. Na tomto terminály môžu ľudia získať širokú škálu údajov a informácií, odpisy a výpisy, ktoré sú vedené v centrálnych verejných i neverejných evidenciách a registroch o ich osobe, majetku a právach.

Systém Czech POINT taktiež poskytuje rozhranie Czech POINT@office určené pre úradníkov, ktorí môžu pomocou formulárov využívať na výkon svojej pôsobnosti rôzne agendy a formuláre, ako napr. výpis a odpis z Registra trestov, výpisy zo základných registrov, konverziu z moci úradnej a agendy matrík, ohlasovní a súdov. Systém kontaktných miest Czech POINT je už taktiež prepojený s Portálom verejnej správy ako aj s Portálom

⁶⁸ Usmernenie k základným povinnostiam podľa zákona o e-Governmente. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.mirri.gov.sk/wp-content/uploads/2018/10/Usmernenie-k-vykonu-verejnej-moci-elektronicky-od-1.11.2016.pdf>>.

⁶⁹ Aplikace e-Podatelna. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://epodatelna.justice.cz/ePodatelna/homepage>>.

občana, ktorý je bránou k elektronickým službám štátu, samoobslužným miestom pre bezpečnú a dôveryhodnú komunikáciu medzi občanom a štátom a každý občan sa do neho môže prihlásiť pomocou dátovej schránky, elektronického občianskeho preukazu, avšak na rozdiel od Portálu verejnej správy, ktorý funguje ako hlavný informačný rozcestník služieb verejnej správy, je tento portál transakčnou časťou, ktorá zabezpečuje osobný prístup cez prihlásenia užívateľa.⁷⁰

Portál verejnej správy v ČR je informačným systémom vytvoreným na základe zákona č. 365/2000 Sb., o informačných systémoch verejnej správy, ktorý je prevádzkovaný so zámerom uľahčenie vzdialeného prístupu k informáciám a službám celej verejnej správy pre verejnosť a jeho správcom je Ministerstvo vnútra ČR.

Ak sa zameriame na druhy elektronickej komunikácie vo verejnej správe v SR využíva sa predovšetkým Ústredný portál verejnej správy, ktorý sme si bližšie definovali v kapitole 2.3 predkladanej práce, ako aj Elektronické podateľne, ktoré sú technickými zariadeniami slúžiacimi predovšetkým na odosielanie, prijímanie, a potvrdzovanie prijatia elektronických dokumentov a dokumentov podpísaných pomocou elektronického podpisu alebo zapečatených kvalifikovanou elektronickou pečaťou a samozrejme Elektronické schránky.

Ak si teda porovnáme druhy elektronickej komunikácie v analyzovaných krajinách dospejeme k záveru, že v rámci oboch krajín sa využívajú rovnaké druhy elektronickej komunikácie a to podateľňa, portál verejnej správy, ako aj elektronické, resp. dátové schránky.

4.2 Bezpečná komunikácia

Keďže pri elektronickej komunikácii dochádza k prenosu dôverných údajov, ako napr. rodné čísla, adresy a pod. je tieto údaje potrebné chrániť, ako pri ukladaní, tak aj pri ich spracovaní a prenose. K tomuto slúži bezpečná komunikácia medzi jednotlivými systémami alebo inštitúciami, ako aj občanmi a spoločnosťami, a preto je nutné si uvedomiť, že nie každá informácia dostupná elektronicky je určená pre každého.

Na to, aby mohla byť elektronická komunikácia považovaná za bezpečnú musí spĺňať medzinárodné normy, a preto je dôležité zadefinovať základné ciele bezpečnosti, ku ktorým

⁷⁰ Co je to Czech POINT? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://www.mvcr.cz/clanek/co-je-czech-point.aspx>>.

patria dôvernosť informácií, integrita a nepopierateľnosť. Dôvernosť informácií musí byť zabezpečená tak, aby prístup k informáciám mali len tie osoby, pre ktoré je informácia určená a sú k nakladaniu s nimi autorizované. V rámci integrity musia byť informácie zabezpečené proti modifikácii pri priamom prenose a nepopierateľnosť je chápaná ako vyššia forma autentizácie, resp. sa jedná o schopnosť presvedčiť nezávislú stranu o autorstve zasielanej správy.⁷¹

Bezpečnú komunikáciu je možné zabezpečiť prostredníctvom fyzickej a logickej ochrany, pričom tá fyzická je náročná na prostriedky a pri logickej sa stretávame s použitím kryptografických metód, ktorými sú šifrovanie a podpisovanie, ktorých úroveň je závislá na použitej kryptografickej metóde.

Kryptografia sa venuje teda návrhom konštrukcií spĺňajúcich konkrétne bezpečnostné požiadavky a jej úlohou, resp. cieľom je zabezpečiť dôveryhodnosť a integritu prenášanej informácie. V prípade bezpečnej komunikácie toto funguje za pomoci šifrovania, ktorého cieľom je premeniť vstupné dáta do podoby, v ktorej sú pre potenciálneho útočníka nezrozumiteľné a ktoré nie je schopný rekonštruovať na ich pôvodný tvar. Na druhej strane dešifrovanie tvorí opačný proces šifrovania a v rámci neho dochádza k prevodu zašifrovanej informácie.⁷²

Pri šifrovaní údajov sa ešte rozlišujú dve jeho formy, ktorými sú:

1. symetrické šifrovanie, ktoré je postupom využívajúcim rovnaký kľúč pre šifrovanie a dešifrovanie textu alebo dát všeobecne, pričom v rámci kryptografie sa jedná o otvorený text určený na utajenie, pri procese šifrovania prevedie do šifrovaného textu a vo všeobecnosti sa pri tomto type šifrovania využíva AES, resp. Advanced Encryption Standard, ktorý používa vláda USA na šifrovanie utajovaných a citlivých informácií;
2. asymetrické šifrovanie, pri ktorom je na šifrovanie potrebný a aj nutný jeden kľúč a na dešifrovanie zas druhý, pričom proces tohto šifrovania funguje tak, že si na začiatku vygenerujeme z náhodných hodnôt pár kľúčov a jeden kľúč, tzv. tajný kľúč, si uschováme do nejakého súboru alebo na čipovú kartu, aby sa k nemu nikto

⁷¹ BUDIŠ P. *Elektronický podpis a jeho aplikácie v praxi*. Praha, 2008, s. 27

⁷² STANEK, M. 2004. *Základy kryptológie*. [cit. 2023-01-27]. Dostupné z WWW: <<https://fmfi-uk.hq.sk/Informatika/Kryptologia/prednasky/krypto.pdf>>.

nedostal a druhý kľúč, tzv. verejný môžeme zverejniť alebo niekomu poslať v e-maili, ako napr. v systémoch, pri ktorých výkon a rýchlosť nie sú prvoradé.⁷³

Ďalším spôsobom bezpečnej komunikácie je hashing, ktorý je jedným zo spôsobov, ako povoliť bezpečnosť počas procesu prenosu správy, ktorá je určená pre konkrétneho príjemcu. Samotný vzorec vytvára tzv. hash, ktorý pomáha chrániť bezpečnosť prenosu pred neoprávneným zásahom. S hashingom súvisia aj hashingové funkcie, ktoré konvertujú údaje ľubovoľnej veľkosti na údaje určitej veľkosti.⁷⁴ Na základe týchto informácií je zrejmé, že has využívaný pri elektronickom podpisovaní správ, teda má podobu elektronického podpisu, ktorému sa budeme venovať nižšie.

V prípade bezpečnej komunikácie postupujú analyzované krajiny – SR a ČR rovnako a tak pri šifrovaní a dešifrovaní využívajú rovnaké prostriedky, pričom používajú aj hashovanie, ktoré má podobu elektronického podpisu.

4.3 Elektronické schránky

Problematika elektronických schránok je v rámci analyzovaných krajín – ČR a SR upravená príslušnými zákonmi. V prípade ČR sa jedná o zákon č. 300/2008 Sb., o elektronických úkonoch a autorizovanej konverzii dokumentov, ktorého predmetom úpravy sú elektronické úkony štátnych orgánov, územných samosprávnych celkov a fyzických alebo právnických osôb, pokiaľ týmto fyzickým alebo právnickým osobám bola zverená pôsobnosť v oblasti verejnej správy, notárov, súdnych exekútorov a insolventných správcov voči fyzickým a právnickým osobám, elektronické úkony fyzických a právnických osôb voči orgánom verejnej moci a elektronické úkony medzi orgánmi verejnej moci navzájom prostredníctvom elektronických schránok, ako aj dodávanie dokumentov fyzickým osôb, podnikajúcich fyzických osôb a právnických osôb prostredníctvom elektronických schránok, ako aj informačný systém elektronických schránok a autorizovanú konverziu dokumentov.⁷⁵

V súvislosti s informačným systémom elektronických schránok v ČR je informačným systémom verejnej správy v zmysle zákona č. 365/2000 Sb., o informačných systémoch verejnej správy v platnom znení. Predmetom tohto zákona je stanovenie práv

⁷³ Symetrická a asymetrická kryptografia. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.itnetwork.sk/bezpecnost/symetricka-a-asymetricka-kryptografia>>.

⁷⁴ Čo je hashovanie? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://sk.theastrologypage.com/hashing>>.

⁷⁵ Česko. Zákon č. 300/2008 Sb. o elektronických úkonoch a autorizovanej konverzii dokumentov.

a povinností, ktoré súvisia s tvorbou, správou, prevádzkovaním, užívaním a rozvojom informačných systémov verejnej správy spravovaných štátnymi orgánmi alebo orgánmi územných samosprávnych celkov.⁷⁶

Ďalším zákonom, resp. vyhláškou, ktorá sa v súvislosti s elektronickými schránkami v ČR spomína je vyhláška č. 194/2009 Sb. o stanovení podrobností užívania a prevádzkovania informačného systému elektronických schránok, v rámci ktorej sú definované všetky náležitosti ohľadom prístupových údajov, formáty príloh elektronických správ, maximálnu veľkosť elektronickej správy a aj dobu uloženia elektronickej správy v elektronickej schránke⁷⁷ a napokon zákon č. 111/2009 Sb. o základných registroch, ktorého predmetom je zriadenie základných registrov a niektorých ďalších informačných systémov verejnej správy a stanovenie pôsobností, práv a povinností, ktoré majú súvis s ich tvorbou, správou, prevádzkou a užívaním, ako aj zriaďuje Správu základných registrov a stanovuje podmienky pre zdieľanie údajov medzi základnými registrami navzájom a agendovými informačnými systémami, základnými registrami a informačnými systémami súkromnoprávných užívateľov údajov umožňujúce využívanie údajov zo základných registrov alebo agendových informačných systémov.⁷⁸

V rámci SR je sú informácie o elektronických schránkach súčasťou už spomenutého zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov, ktorého predmetom sú niektoré informačné systémy pre výkon pôsobnosti orgánov verejnej moci, elektronické podanie, elektronický úradný dokument a niektoré podmienky a spôsob výkonu verejnej moci elektronickej komunikácie, ako aj elektronické schránky a doručovanie, identifikácia a autentifikácia osôb, autorizácia, zaručená konverzia, spôsob vykonania úhrady orgánu verejnej moci a referenčné registre.⁷⁹

Ďalej je to aj vyhláška upravujúca niektoré ustanovenia zákona o e-Governmente, konkrétne vyhláška č. 438/2019 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente, a ktorá ustanovuje podrobnosti o spôsobe plnenia povinností orgánov verejnej moci, sadzobník úhrad za činnosť ústredného portálu verejnej správy a spoločných

⁷⁶ Česko. Zákon č. 365/2000 Sb. o informačných systémoch verejnej správy v platnom znení

⁷⁷ Česko. Vyhláška č. 194/2009 Sb. o stanovení podrobností užívania a prevádzkovania informačného systému elektronických schránok

⁷⁸ Česko. Zákon č. 111/2009 Sb. o základných registroch

⁷⁹ Slovensko. Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

modulov, ako aj funkcionality ústredného portálu a spoločných modulov nad rámec funkcionalít stanovených na základe príslušných zákonov a podrobnosti o úložnej kapacite elektronickej schránky a o postupe pri odstraňovaní elektronických správ pri naplnení úložnej kapacity elektronickej schránky.⁸⁰

Na základe jednotlivých zákonov upravujúcich problematiku elektronických schránok je zrejmé, že v rámci oboch krajín je táto tematika súčasťou príslušných zákonov týkajúcich sa ich zriadenia, používania, ako aj prevádzky a správy. V ČR je na úpravy elektronických schránok a informačných systémov verejnej správy využitých viac zákonov a príslušných vyhlášok ako je to v SR.

Pre správne pochopenie je dôležité aj vymedzenie pojmu elektronickej alebo dátovej schránky, ktorá je vlastne typom úložiska v elektronickej forme, ktoré slúži na prijímanie a odosielanie dokumentov za maximálnej ochrany s overením totožnosti vlastníka schránky. V SR sa elektronická schránka zriaďuje pre fyzické osoby – občanov SR automaticky po dovŕšení 18 rokov a pre fyzické osoby, fyzické osoby – podnikateľov, právnické osoby, orgány verejnej správy a subjekty medzinárodného práva ich zriaďuje Ministerstvo investícií, regionálneho rozvoja a informatizácie SR.⁸¹

V rámci ČR sú elektronické schránky zriaďované zo zákona a na žiadosť. Zo zákona ich automaticky zriaďuje Ministerstvo vnútra a to pre právnické osoby v Obchodnom registri, orgány verejnej moci, podnikajúce fyzické osoby napr. znalec, tlmočník a pod., podnikajúce fyzické osoby zapísané v základnom registri osôb a právnické osoby zapísané v základnom registri osôb a elektronické schránky na žiadosť sú zriaďované pre fyzické osoby a podnikajúce fyzické osoby nezapísané v základnom registri osôb a zahraničné podnikajúce fyzické osoby. V prípade žiadosti majú fyzické osoby jednu z nasledovných možností a to:

1. online po prihlásení sa cez Identitu občana;
2. osobne na kontaktných miestach Czech POINTu;
3. písomne na adrese Ministerstva vnútra.⁸²

Ako môžeme vidieť na informáciách vyššie, v analyzovaných krajinách, sú elektronické schránky zriaďované rozličnými ministerstvami a to Ministerstvom vnútra

⁸⁰ Česko. Vyhláška č. 438/2019 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente

⁸¹ Slovensko.sk – Elektronické schránky podľa zákona o e-Governmente. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.slovensko.sk/sk/titulna-stranka>>.

⁸² Dátové schránky – typy dátových schránok. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://info.mojedatovaschranka.cz/info/cs/>>.

a Ministerstvom investícií, regionálneho rozvoja a informatizácie, pričom v ČR na rozdiel od SR sú elektronické schránky zriaďované buď automaticky alebo na požiadanie, pričom zriadenie je v oboch krajinách bezplatné.

Čo sa týka výhod elektronických schránok, tak medzi ich hlavné výhody patrí prístupnosť, finančná a časová úspora, ako aj bezpečnosť a informovanosť, ako aj neobmedzená kapacita, preukázateľnosť doručenia dokumentov, dôveryhodnosť a poštové elektronické schránky. Každá z analyzovaných krajín ma na príslušných webových stránkach dostupné rozličné videá, resp. video návody ohľadom prihlásenia a prístupu k elektronickým službám, o elektronickej schránke, elektronickej podaní a podpisovaní, ako aj o elektronických službách.

Prihlásenie do elektronickej schránky prebieha niekoľkými spôsobmi. Pri prihlásení do elektronickej schránky v ČR je možné využiť nasledovné možnosti:

- prihlasovacie meno a heslo, ktoré ponúka jednoduché riešenie len pri základnej úrovni zabezpečenia;
- prihlasovacím certifikátom, ktorý je potrebné si nainštalovať pred prihlásením do schránky a registráciou do systému, pričom tento certifikát si je možné zakúpiť len na pobočkách českej pošty so službou Czech POINT;
- SMS autentizáciou, ktoré je považované za bezpečnejší spôsob prihlasovania na základe kódov zasielaných pomocou SMS správ a tak prihlasovanie prebieha za pomoci mena, hesla a kódu z SMS;
- prostredníctvom mobilného kľúča, ku ktorému je možné použiť mobil alebo tablet s operačným systémom Google Android alebo Apple iOS;
- cez identitu občana na základe identifikačných prostriedkov s vysokou mierou zabezpečenia, ako napr. eObčanka, banková identita a pod.⁸³

Na prihlasovanie do elektronických schránok v SR sa nepoužíva až toľko možností ako v ČR, tak ako môžeme vidieť na informáciách v predchádzajúcom odseku. V SR sa na prihlasovanie používa:

- občiansky preukaz s čipom a bezpečnostný osobný kód;
- doklad o pobyte s elektronickým čipom a bezpečnostný osobný kód;

⁸³ Dátové schránky – způsoby přihlašování. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://info.mojedatovaschranka.cz/info/cs/>>.

- alternatívny autentifikátor.⁸⁴

Aj pri prihlasovaní do elektronických schránok je potrebné dbať na bezpečnosť, v rámci ktorej je dôležité dbať hlavne na správne a bezpečné prihlásenie za pomoci bezpečných prístupových metód. Ďalej je nutné dávať pozor na falošné stránky, používať na prihlásenie, ak je to možné, vlastné počítače, nakoľko pri prihlasovaní sa formou cudzieho počítača, nevieme, či si náhodou tento neuloží naše prihlasovacie údaje.

V prípade prihlasovania je taktiež rizikom, prihlasovanie cez zdieľaný počítač, nakoľko prostredníctvom takéhoto počítača zdieľate aj operačný systém a v rámci neho svoje účty. Treba sa vyhýbať aj komunikácii cez verejné siete, ktoré je považované za riskantné a taktiež je dôležité pravidelne vykonávať tzv. „hygienu“, resp. čistenie vášho počítača, ako napr. zálohovanie dôležitých dát, kvalitný antivírus a ďalšie.

Dôležité je dávať si pozor aj na prácu s prílohami, ktoré niekedy tvoria súčasť elektronických správ, nakoľko zasielanie 100% nezávadných správ nie je možné zaručiť, aj napriek tomu, že stiahnutie takejto správy s prílohou ešte nie je nebezpečné a k riziku dochádza len vtedy, ak sa príloha otvorí. Samozrejme medzi najdôležitejšie v práci s elektronickými schránkami patria skutočnosti, že sa nezdieľajú údaje s tretími osobami, nakoľko zákon takéto správanie zakazuje a ak to používateľ elektronickej schránky spraví, je to na jeho vlastné riziko. Posledným bodom v rámci bezpečnosti práce s elektronickými schránkami patrí, že telefón je tiež počítač.⁸⁵

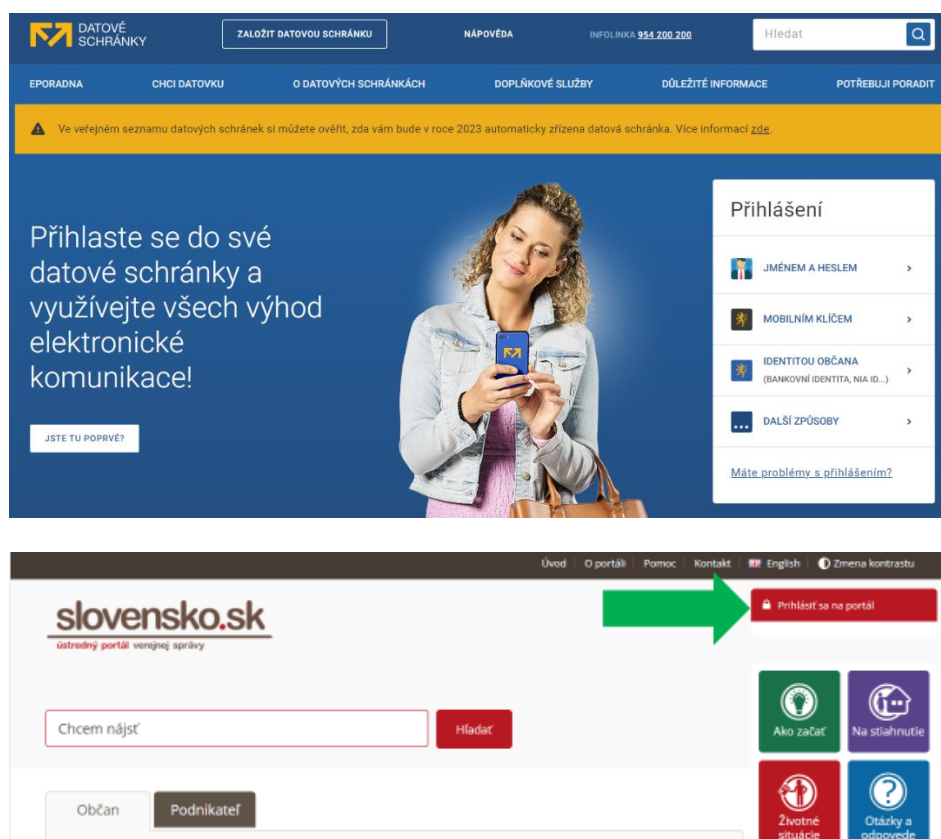
Vzhľadom k bezpečnosti sa teda používateľom odporúča, prihlasovať sa do elektronických schránok len na prislúchajúcich schránkach zriadených ministerstvami. V ČR je to webová stránka <https://info.mojedatovaschranka.cz/info/cs/> a v SR je to zas webová stránka <https://www.slovensko.sk/sk/titulna-stranka>.

⁸⁴ Slovensko.sk – Prístup do schránky. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.slovensko.sk/sk/titulna-stranka>>.

⁸⁴ Dátové schránky – typy dátových schránok. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://info.mojedatovaschranka.cz/info/cs/>>.

⁸⁵ Dátové schránky – Bezpečnosť. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://info.mojedatovaschranka.cz/info/cs/>>.

Obrázok 7 Prihlasovanie do elektronických schránok - ČR a SR⁸⁶



4.4 Elektronický podpis a značka

Pri práci s elektronickými schránkami, najmä pri podpisovaní dokumentov sa využíva v rámci SR kvalifikovaný elektronický podpis (ďalej len KEP⁸⁶), ktorý je vlastne informáciou pripojenou k elektronickému dokumentu. Na základe zákona č. 272/2016 Z. z. o dôveryhodných službách takýto podpis umožňuje jednoznačne určiť osobu, ktorá správy vyhotovila. Za pomoci KEP sú teda realizované rozličné právne úkony, namiesto bežnej písomnej formy a tak je možné skonštatovať, že KEP vlastne nahrádza vlastnoručný podpis užívateľa. V prípade KEPu sa jedná o zdokonalený elektronický podpis vystavený pomocou kvalifikovaného zariadenia na vystavenie podpisu a je založený na kvalifikovanom certifikáte pre tento typ podpisov.

⁸⁶ Slovensko.sk. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.slovensko.sk/sk/titulna-stranka>> a Dátové schránky. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://info.mojedatovaschranka.cz/info/cs/>>.

Používanie KEP v rámci elektronickej komunikácie s verejnou správou, ale aj komerčným sektorom zaisťuje najmä:

- integritu, na základe ktorej sa preukazuje, že pri podpisovaní dokumentov neprišlo k žiadnej zmene týkajúcej sa obsahu dokumentu;
- autenticitu pomocou ktorej je možné overiť identitu subjektu, ktorý podpis vytvorila;
- nepopierateľnosť, v rámci ktorej nemôže tvorca podpisu poprieť, že podpis nevyhotovil.⁸⁷

Pre získanie KEP musí užívateľ disponovať elektronickým dokumentom, súkromným kľúčom pre účely vyhotovenia elektronického podpisu, kvalifikovaným certifikátom vydaným dôveryhodným poskytovateľom a napokon prostriedkami a príslušnými softvérovými vybaveniami na jeho vyhotovenie. KEP je možné vyhotoviť len za pomoci nástrojov na jeho tvorbu, ako napr. súkromný kľúč alebo podpisová aplikácia. Pod súkromným kľúčom sa rozumie tajná informácia slúžiaca na vyhotovenie KEP dokumentu a na druhej strane verejný kľúč, ktorý je informáciou dostupnou overovateľovi a slúžiacou na overenie správnosti KEP. Obidva tieto kľúče sú navzájom prepojené a tvoria jeden kľúčový pár.

Pre používanie KEP musí užívateľ disponovať občianskym preukazom s čipom, ktorý mu vydá príslušné oddelenie odboru poriadkovej polície. Na tvorbu KEP pomocou identifikačnej karty, teda občianskeho preukazu, musí byť splnených niekoľko podmienok, ktorými sú:

1. eID alebo eDoPP s platným kvalifikovaným certifikátom pre elektronický podpis, ktorý je uložený na čipe napr. občianskeho preukazu;
2. musí byť príslušný počítač vybavený kontaktnou čítačkou čipových kariet spolu s ovládačmi, softvérovým vybavením pre eID, aplikáciou pre vytváranie KEP a znalosťou BOK a KEP PINu.⁸⁸

Vzhľadom k tomu, že v súvislosti s KEP sa využíva dvojité autentizácia, musí jeho majiteľ niečo vlastniť – občiansky preukaz s čipom a niečo poznať – KEP PIN, nakoľko bez nich nie je možné vytvoriť KEP. KEP PIN predstavuje bezpečnú ochranu pred vytvorením podpisu neoprávnenou osobou, ktorý je obmedzený nesprávnym zadaním hodnoty PINu. Po

⁸⁷ Čo je elektronický podpis a ako ho získať v roku 2022? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://podnikam.sk/co-je-elektronicky-podpis-a-ako-ho-ziskat/>>.

⁸⁸ Čo je elektronický podpis a ako ho získať v roku 2022? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://podnikam.sk/co-je-elektronicky-podpis-a-ako-ho-ziskat/>>.

jeho troch nesprávnych zadaniach je možnosť využitia kľúča na podpisovanie zablokovaná.⁸⁹

V ČR sa taktiež na podpisovanie elektronických dokumentov vytvára elektronický podpis, pričom sa rozlišuje medzi zaručeným a (ne)zaručeným elektronickým podpisom. Zaručený elektronický podpis je definovaný zákonom č. 486/2004 Sb., o elektronickom podpise a o zmene niektorých ďalších zákonov. Na účely tohto zákona sa elektronickým podpisom rozumie údaje v elektronickej podobe, ktoré sú súčasťou dátovej správy alebo sú s ňou logicky spojené a ktoré slúžia ako metóda k jednoznačnému overeniu identity podpísanej osoby vo vzťahu k dátovej správe, pričom zaručeným elektronickým podpisom je podpis, ktorý spĺňa niekoľko požiadaviek a to:

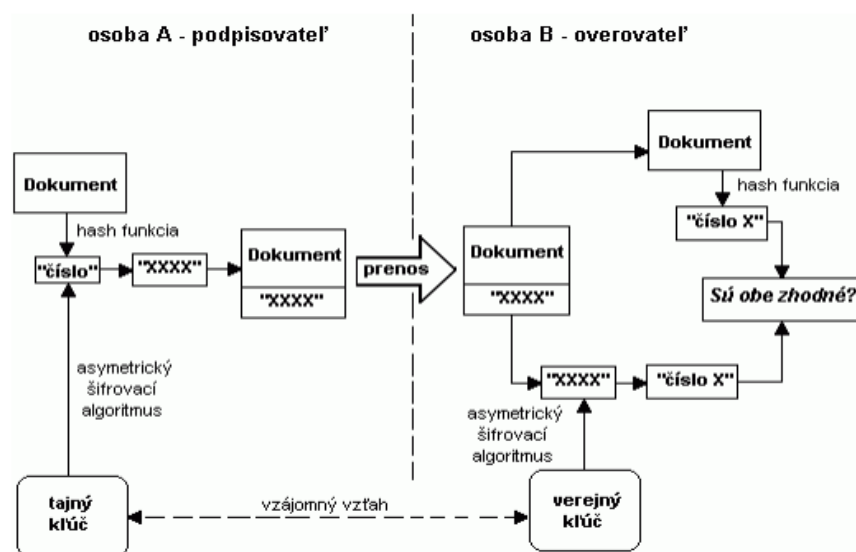
- je jednoznačne spojený s podpisujúcou osobou;
- umožňuje identifikáciu podpisujúcej osoby vo vzťahu k dátovej správe;
- bol vytvorený a pripojený k dátovej správe pomocou prostriedkov, ktoré môže podpisujúca osoba udržať pod svojou výhradnou kontrolou;
- je k dátovej správe pripojená takým spôsobom, že je možné zistiť akúkoľvek zmenu dát.⁹⁰

Pri tvorbe a overovaní elektronického podpisu sa postupuje pri kryptografii v oboch analyzovaných krajinách rovnako. Tvorba podpisu prebieha za pomoci dvoch krokov a to vytvorením hodnoty funkcie hash z vlastných dát a v druhom kroku je táto hodnota hash podpísaná pomocou súkromného kľúča odosielateľa a tak získa elektronický podpis.

⁸⁹ Čo je elektronický podpis a ako ho získať v roku 2022? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://podnikam.sk/co-je-elektronicky-podpis-a-ako-ho-ziskat/>>.

⁹⁰ Česko. Zákon č. 486/2004 Sb. o elektronickom podpise a o zmene niektorých ďalších zákonov

Obrázok 8 Princíp elektronického podpisu⁹¹



Elektronická značka (ďalej len „EZ“) funguje na rovnakom princípe ako elektronický podpis a aj požiadavky na tento typ značky sú podobné. Za pomoci elektronickej značky je možné elektronickú poštu označiť automaticky, bez zásahu označujúcej osoby.

Tieto značky sa tvoria hlavne vtedy, keď je nutné označiť väčšie množstvo správ a to dôveryhodne v krátkom čase, ako napr. v e-podateľni. Tento typ značky môžu využívať v niektorých prípadoch aj firmy alebo úrady ako napr. pri výpise z katastra nehnuteľností, pri podávaní daňových priznaní a pod.

Rozdiel medzi elektronickým podpisom a značkou je hlavne v jeho právnej charaktere, nakoľko zatiaľ čo podpis vytvorí fyzická osoba, elektronickou značkou môžu elektronické správy označovať aj právnické osoby alebo organizačná zložka štátu a tak značka slúži ako úradná pečiatka, pričom má rovnakú váhu ako elektronický podpis.⁹²

Tento typ podpisovania je využívaný v oboch analyzovaných krajinách na rozličné výstupy, tak ako to uvádzame vyššie, ako aj z fakturačných systémov a rozličných objednávkových systémov a ďalšie.

⁹¹ Národný bezpečnostný úrad, Elektronický podpis. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.nbu.gov.sk/index.html>>.

⁹² Elektronická značka. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.sslch.cz/files/163/3-elektronicka-komunikace-u.pdf>>.

4.5 Elektronické certifikáty

Certifikáty pre elektronický podpis predstavujú elektronické osvedčenie spájajúce údaje na validáciu elektronického podpisu fyzickou osobou potvrdzujúci aspoň meno alebo pseudonym fyzickej osoby. Vydavateľ takéhoto certifikátu potvrdzuje, že jeho súčasťou je verejný kľúč patriaci fyzickej osobe, ktorej identifikácia sa v ňom nachádza, v prípade, že sa nejedná o pseudonym. Samotný certifikát teda obsahuje informácie o verejnom kľúči, ako aj informáciu o totožnosti jeho držiteľa spolu s elektronickým podpisom subjektu, ktorý overil obsah certifikátu.⁹³

Presný obsah certifikátu môže byť ľubovoľný, avšak existuje celé množstvo noriem, ako aj právnych predpisov, ktoré obsah certifikátov určených pre konkrétny účel pomerne presne upravujú. Jednotlivé položky certifikátu sa usporadúvajú do štyroch logických skupín, ktorými sú:

1. osobné údaje vlastníka certifikátu ako meno, priezvisko, rodné číslo, IČO a pod.;
2. služobné údaje, ako napr. identifikačné číslo certifikátu a certifikačnej authority, ktorá certifikát vydala, informácie o použitých algoritmoch a pod.;
3. verejný kľúč, ktorý sa certifikuje;
4. digitálny podpis všetkých vyššie uvedených položiek.⁹⁴

Vzhľadom na jednotlivé položky certifikátu sú jeho obsahom na základe verejného kľúča nasledovné údaje.

Tabuľka 1 Obsah certifikátu⁹⁵

Obsah certifikátu verejného kľúča	
Položka	Popis
ID certifikátu	Jednoznačné sériové číslo
Dátum vydania	Kedy bol certifikát vydaný
Platnosť do	Časové obmedzenie platnosti
Obmedzenie certifikátu	Účel, pre ktorý je možné certifikát využiť
ID certifikačnej authority	Kto certifikát vydal
Algoritmy CA	Aké algoritmy používa pre podpisovanie certifikačná autorita

⁹³ Certifikát pre elektronický podpis. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://eid.sk/sk/certifikaty/certifikat-pre-elektronicky-podpis/>>.

⁹⁴ DOSEDEĽ, T. *Počítačová bezpečnosť a ochrana dát*. Brno, 2004, s. 91

⁹⁵ DOSEDEĽ, T. *Počítačová bezpečnosť a ochrana dát*. Brno, 2004, s. 91

Verejný kľúč CA	Nemusí tvoriť súčasť certifikátu
ID vlastníka	Rodné číslo alebo IČO
Verejný kľúč vlastníka	Vlastný certifikovaný kľúč
Podpis	Predchádzajúce dáta sú podpísané súkromným kľúčom CA

Certifikačné autority vydávajú certifikáty rôznych druhov, ktorých hlavným rozdielom sú triedy a s nimi spojená miera overovania identity vlastníka a tak nie je každý certifikát vhodný na každý účel. V prípade týchto tried hovoríme konkrétne o nasledovných:

- class 1, pri ktorej certifikačná autorita overí len meno, ktoré chceme do certifikátu zapísať;
- class 2, pri ktorom môže byť identita vlastníka overená treťou stranou a k jeho vystaveniu postačuje napr. notársky overený formulár;
- class 3 ktorá je štandardom medzi certifikátmi a žiadateľ o certifikát musí osobne navštíviť certifikačnú autoritu, ktorá overí jeho totožnosť a preto je vhodný na väčšinu účelov;
- class 4, ktorej podmienky pre získanie sú rovnaké ako pri predchádzajúcej triede, a preto sa vytvára napr. autorizovaným projektantom, ktorí môžu následne podpisovať projekty rovnakým spôsobom, ako by na nich dali svoju pečiatku.⁹⁶

V prípade kvalifikovaného certifikátu je možné aj jeho zrušenie, ktoré sa používa len vtedy, ak má užívateľ, resp. občan podozrenie, že má jeho certifikát k dispozícii iná osoba ako on sám a tá môže v jeho mene vytvoriť KEP, ako napr. pri strate občianskeho preukazu a pod. Zrušenie je častokrát využívané aj zo strany poskytovateľov dôveryhodnej služby, ktoré vydávajú kvalifikované certifikáty, ako napr. ak vyprší certifikát kvalifikovaného zariadenia pre uchovávanie kľúča, atď.

O zrušenie na občianskom preukaze môže požiadať užívateľ, resp. občan aj osobne na ktoromkoľvek Okresnom riaditeľstve Policajného zboru alebo cez elektronické služby. Tieto certifikáty môže zrušiť ďalej aj samotný vydavateľ certifikátu bez žiadosti jeho držiteľa, ako napr. ak jeho platnosť presahuje platnosť občianskeho preukazu.⁹⁷

Postup pri vydávaní, rušení, ako aj samotný obsah certifikátu je pri analyzovaných krajinách – SR a ČR rovnaký. Rozdiel sme zaznamenali len v skutočnosti, že v SR od 01.01.2023 nebudú platiť doteraz vydané certifikáty pre kvalifikovaný elektronický podpis.

⁹⁶ DOSEDĚL, T. *Počítačová bezpečnosť a ochrana dat.* Brno, 2004, s. 92

⁹⁷ Slovensko.sk – Kvalifikovaný elektronický podpis. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.slovensko.sk/sk/titulna-stranka>>.

Problém však nie je v samotných certifikátoch, ale v starších čípoch, ktoré sú súčasťou občianskych preukazov vydaných pred 20. júna 2021.

Aj napriek tejto skutočnosti zostávajú dovtedy vydané občianske preukazy v platnosti a ešte stále sa dá s nimi prihlásiť do elektronických schránok, avšak už nebude možné prostredníctvom nich podpisovať dokumenty. Na to, aby mohol užívateľ opätovne využívať aj elektronický podpis, musí požiadať o výmenu občianskeho preukazu s čipom a to osobne a následne požiadať o vydanie nového certifikátu.⁹⁸

4.6 Banková identita

Elektronická identita však neslúži len k jednaniam s orgánmi verejnej moci, ale funguje na rovnakom princípe aj pri jednaniach so subjektami komerčnými, keď sa na jej základe môžete bez nutnosti osobného jednania dohadovať na internete poistenie alebo si objednať mobilné tarify. Na tomto základe sa pod bankovou identitou rozumie identifikačný prostriedok, ktorým sa užívateľ prihlasuje k online službám.⁹⁹

Banková identita (ďalej len „BankID“) predstavuje metódu digitálneho overenia totožnosti, na základe ktorej je možné sa bezpečne prihlásiť do rôznych firiem, ako aj štátnej správy a to tak jednoducho ako sa prihlasujeme do internetového bankovníctva.¹⁰⁰

BankID uľahčuje jej užívateľom život, nakoľko v rámci elektronickej identity užívateľ používa len jedny prihlasovacie údaje a tak si nemusí pamätať veľa hesiel a prihlasovacích údajov, je bezpečná a zároveň užívateľov chráni, pretože nezdiera dáta s nikým, ak s tým nesúhlasíte. Ďalšou výhodou BankID je skutočnosť, že šetrí čas a námahu a tak už nemusíte skenovať doklady totožnosti alebo chodiť podpisovať zmluvy na pobočky, napr. bánk a je možné ju zriadiť bez registrácie a zdarma.¹⁰¹

Väčšina občanov ČR už bankovú identitu vlastní, keďže sa jedná o prístupové údaje, resp. spôsob akým sa užívatelia prihlasujú do internetového bankovníctva svojich bánk a tak ju ponúkajú rozličné banky, ako napr. Česká sporiteľňa, AirBank, ČSOB, Fio banka, Komerčná banka, Raiffeisen Bank, UniCredit a ďalšie. V prípade Fio banky a UniCredit

⁹⁸ REMOVČÍKOVÁ, L. 2022. Koniec certifikátov pre e-podpis od 1.1.2023: koho sa to týka a čo robiť? [online]. 2023. [cit. 2023-01-29]. Dostupné z WWW: <<https://www.podnikajte.sk/zakonne-povinnosti-podnikatela/koniec-certifikatov-epodpis>>.

⁹⁹ Bankovní identita. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.businessinfo.cz/navody/bankovni-identita-ppbi/2/>>.

¹⁰⁰ BankID. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.bankid.cz/>>.

¹⁰¹ Co je bankovní identita a kde sa vám hodí. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita>>.

Bank zatiaľ umožňujú využívať BankID len na prihlásenie sa do portálu verejnej správy, pričom svojim klientom plánujú ponúkať aj banky ako mBank a Banka Creditas.¹⁰²

Zabezpečenie BankID prebieha rozličnými metódami, nakoľko ju tvorí užívateľské meno a unikátne telefónne číslo, a preto musí byť každé prihlásenie maximálne zabezpečené jednou z nasledovných troch bezpečnostných metód a to:

1. mobilnou aplikáciou George kľúča, ktorý je najbezpečnejšou a pohodlnou metódou, ktorá si vyžaduje na používanie len aplikáciu, v ktorej všetko potvrdíte;
2. heslom a potvrdením cez SMS, ktoré si zvolíte sami a zadáte ho pri prihlásení a overení, pričom je následne doručená SMS obsahujúca kód, ktorým heslo potvrdíte;
3. overením za pomoci hesla, ktoré sa používa len pre volania na kontaktné centrum, kedy sa za pomoci operátora nahrá hlas užívateľa a pri ďalšom volaní je možné užívateľa hneď identifikovať.¹⁰³

Pre bližšie pochopenie BankID je nutné si uvedomiť, že ide len o prostriedok pre online prihlásenie k ponúkaným službám a nejde sa o priamy prístup k službám e-Governmentu a v prípade záujmu o tieto služby je potrebné najskôr navštíviť webovú stránku alebo portál s konkrétnou službou, ktorú chce užívateľ využiť a následne po voľbe spôsobu prihlásenia si zvolí práve prihlásenie cez BankID. Následne je presmerovaný na stránku banky, kde užívateľ zadá svoje prihlasovacie údaje alebo aj bezpečnostný prvok, ak si to prihlásenie vyžaduje.

Prihlasovanie za pomoci BankID prebieha k dvom typom službám a to verejnoprávnym a súkromnoprávnym. V prípade verejnoprávnym služieb sa užívateľ prihlasuje k službám e-Governmentu, teda sa využíva na online konanie s orgánmi verejnej moci, pri ktorom prebieha prihlasovanie cez prostredníka a to Národný bod pre autentifikáciu a identifikáciu (ďalej len „NIA“), ktorá spája elektronické identity spolu s poskytovateľom služieb e-Governmentu. A tak pri akomkoľvek prihlásení nedochádza k priamemu prihláseniu cez BankID, ale prostredníctvom NIA. Dôvodom takéhoto prihlasovania je čo najvyššia ochrana údajov o užívateľoch, na čo poukazuje aj skutočnosť, že ani banky nepoznajú k akej konkrétnej službe e-Governmentu sa klient za pomoci BankID prihlasuje.

¹⁰² BankID. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.bankid.cz/>>.

¹⁰³ Co je bankovní identita a kde sa vám hodí. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita>>.

V prípade SR si musíme na niečo také, ako je BankID, ktoré je využívané v ČR, ešte počkať, nakoľko prihlasovacie údaje do internet bankingu sa ako podpis používať nebudú. V SR, tak ako sa vyjadril hovorca Národnej banky Slovenka (ďalej len „NBS“), môžu klienti na komunikáciu s verejnou správou používať občiansky preukaz s čipom a podobné riešenie ako v prípade ČR v SR zatiaľ nie je, avšak nie je vylúčené že takéto riešenie môže do budúcnosti prísť.

Na prihlásenie sa do elektronických služieb prihlasujú za pomoci občianskeho preukazu za pomoci špeciálnej čítačky, avšak na riešenie, tak ako je vo v ČR momentálne na Slovensku nie je priestor a ani sa nepredpokladá záujem bankového sektora o komerčný projekt na tvorbu bankovej identity. V rámci Slovenska sa banky snažia o čo najjednoduchšie prihlasovanie do služieb, no z vlastného prostredia vystúpiť nechcú.¹⁰⁴

Na základe dostupných údajov je zrejmé, že v prípade ČR je už mnohými bankami využívaná banková identita, ktorá umožňuje jej užívateľom prihlásiť sa aj do iných inštitúcií verejnej správy bez nutnosti pamätania si rozličných prihlasovacích údajov a hesiel. Táto skutočnosť im napomáha k zjednodušenému spôsobu elektronickej komunikácie. Na druhej strane v prípade Slovenska, takáto možnosť ešte neexistuje a tak musia užívatelia elektronických služieb využívať na prihlasovanie, tak ako doteraz, občiansky preukaz s čipom a príslušnú čítačku kariet.

¹⁰⁴ Čechom pomôže heslo do elektronického bankovníctva komunikovať so štátom a firmami. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.trend.sk/financie/cechom-pomoze-heslo-elektronickeho-bankovnictva-komunikovat-statom-aj-firmami>>.

ZÁVER

Technický pokrok, ktorý je v dnešnej dobe značne viditeľný, nám umožnil komunikovať elektronicky s ľuďmi na celom svete. Aby sa však elektronická komunikácia stala pre nás prínosom, musí byť nielen rýchla, ale aj spoľahlivá a efektívna na jednej strane a na strane druhej samozrejme bezpečná a dôveryhodná. Už spomenutú rýchlosť a spoľahlivosť zabezpečujú práve dostupné technické možnosti a bezpečnosť spolu s dôveryhodnosťou predstavujú v súčasnosti najdôležitejšiu zložku elektronickej komunikácie.

V súvislosti s elektronickou komunikáciou v rámci verejnej správy sa objavuje, vo svete už známy pojem e-Government, ktorý museli do svojich právnych poriadkov zaviesť aj krajiny, na ktoré sme sa v rámci analýzy elektronickej komunikácie zamerali. Týmto krajinami boli Slovenská a Česká republika. Zavedenie tejto formy komunikácie prispelo k efektívnejšiemu fungovaniu verejnej správy a taktiež k zvýšeniu jej výkonnosti. Toto by však nebolo možné bez jej správneho zakotvenia v rámci príslušných zákonov a vyhlášok súvisiacich s elektronickou komunikáciou.

Elektronickú formu komunikácie využívajú nielen štátne inštitúcie, ale aj občania a firmy komunikujúce s nimi. Občania využívajú v rámci elektronickej komunikácie rozličné formy, ako napr. internet, e-maily, ako aj elektronické schránky. Tieto formy komunikácie im umožňujú z pohodlia domova komunikovať s príslušnými úradmi a takisto nájsť potrebné informácie, ako aj rôzne formuláre, ktoré môžu rovno vyplniť a za pomoci elektronického podpisu podpísať a zaslať na príslušný úrad verejnej správy, ako napr. úrady práce a pod. V ČR môžu na základe Bankovej identity vyplniť formuláre a odoslať na úrad elektronicky.

Musíme poukázať aj na skutočnosť, že formy elektronickej komunikácie čoraz častejšie využívajú aj spoločnosti na komunikáciu s úradmi, poisťovňami a pod. Dôležitým portálom v tejto oblasti je v SR portál slovensko.sk a v ČR je to mojedatovaschranka.cz prostredníctvom ktorých môžu komunikovať s inštitúciami napr. pri podávaní daňových priznaní, komunikácii so Sociálnou poisťovňou a pod.

Čo sa týka komunikácie prostredníctvom elektronických schránok, považujeme túto formu pre samotné spoločnosti za veľmi výhodnú, nakoľko funguje na báze spoľahlivosti a dôveryhodnosti a pomocou dostatočného a správneho zabezpečenia. Pri elektronickej

komunikácii vo verejnej správe na základe spracovanej analýzy nami vybraných krajín – SR a ČR sme dospeli k záveru, že právne ukotvenie problematiky elektronickej komunikácie je dostatočné a príslušné zákony sú zrozumiteľné aj pre bežných občanov. V prípade druhov elektronickej komunikácie vo verejnej správe v SR a ČR sú využívané predovšetkým Ústredný portál verejnej správy ako aj Elektronické podateľne, ktoré sú technickými zariadeniami slúžiacimi predovšetkým na prijímanie, odosielanie a potvrdzovanie prijatia elektronických dokumentov a elektronických dokumentov podpísaných pomocou elektronického podpisu alebo zapečatených kvalifikovanou elektronickou pečaťou a samozrejme Elektronické schránky a v ČR je to ešte aj Czech POINT.

V prípade bezpečnej komunikácie postupujú analyzované krajiny – SR a ČR rovnako a tak pri šifrovaní a dešifrovaní využívajú rovnaké prostriedky, pričom používajú aj hashovanie, ktoré má podobu elektronického podpisu. Na druhej strane na prihlasovanie do elektronických schránok v SR sa nepoužíva až toľko možností ako v ČR, tak ako môžeme vidieť na informáciách v predchádzajúcom odseku. V oboch krajinách je na podpisovanie elektronických správ využívaný kvalifikovaný, resp. zaručený elektronický podpis a postup pri vydávaní, rušení, ako aj samotný obsah certifikátu je pri analyzovaných krajinách – SR a ČR rovnaký.

ZOZNAM POUŽITÝCH ZDROJOV

ADAMCOVÁ, M. 2018. *Teória verejnej správy*. Košice: Univerzita Pavla Jozefa Šafárika, 2018. 136 s. ISBN 9788081525872.

ANDRAŠKO, Jozef. 2019. *Digitálna verejná správa a elektronická identifikácia*. Bratislava: Univerzita Komenského, 2019. 98 s. ISBN 978-80-7160-514-0.

BUDIŠ P. 2008. *Elektronický podpis a jeho aplikácie v praxi*. Praha: ANAG 2008. 157 s. ISBN 978-60-7263-465-1.

DOSEDĚL, T. 2004. *Počítačová bezpečnosť a ochrana dát*. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

GAŠPAR, M. 1993. *Moderná verejná správa*. Bratislava: Procom, 1993. 128 s. ISBN 80-85717-01-8.

GREGUŠOVÁ, D., HALÁSOVÁ, Z. 2018. *Zákon o e-Governmente – Komentár*. 1. vydanie. Bratislava: EUROKÓDEX, 2018. 328 s. ISBN 978-80-8155-080-5.

HAMALOVÁ, M. a kol. 2014. *Teória, riadenie a organizácia verejnej správy*. Bratislava: Wolters Kluwer, 2014. 454 s. ISBN 978-80-8168-140-0.

HARAUSOVÁ, H. 2013. *Komunikácia v organizácii*. Košice: Univerzita Pavla Šafárika, 2013. 120 s. ISBN 978-80-8152-019-8.

HEGER, V. 2012. *Komunikácie vo verejnej správe*. Praha: Grada Publishing, 2012. 256 s. ISBN 978-80-247-3779-9.

KLIMOVSKY, D. 2008. *Základy verejnej správy*. Bratislava: Wolters Kluwer, 2008. 270 s. ISBN 978-80-7097-713-2

KOCKS, K. Koll. 2020. *Öffentliche Verwaltung – Verwaltung in der Öffentlichkeit*. Wiesbaden: Springer Fachmedien, 2020. 248 s. ISBN 978-3-658-28008-6.

KOSORÍN, F. 2003. *Verejná správa*. Bratislava: EKONÓM, 2003. 163 s. ISBN 80-225-1696-1.

KOVÁČOVÁ, E. 2014. *Teória a prax verejnej správy v podmienkach Slovenskej republiky*. Banská Bystrica: UMB Belianum, 2014. 236 s. ISBN 978-80-557-0735-8.

KOVÁČOVÁ, E. 2020. *Vplyv decentralizácie na výkon a riadenie územnej samosprávy v SR*. Banská Bystrica: UMB Belianum, 2020. 222 s. ISBN 978-80-557-1766-1.

LIDINSKÝ, V. a kol. 2008. *eGovernment bezpečně*. Praha: Grada publishing, a. s., 2008. 160 s. ISBN 978-80-247-2462-1.

MACHYNIAK, J. 2020. *Verejná správa a verejná politika*. Trnava: Univerzita sv. Cyrila a Metoda, 2021. 78 s. ISBN 978-80-572-0103-8.

OCHRANA, F. a kol. 2015. *Veřejná správa*. Brno: Masarykova univerzita, 2015. 657 s.

PETERKA, J. 2011. *Báječný svět elektronického podpisu*. 1. vydanie. Praha: CZ.NIC, 2011. 430 s. ISBN 978-80-904248-3-8.

SOPÚCHOVÁ, S. 2021. *Informatizácia verejnej správy e-Government*. 1. vydanie. Bratislava: Univerzita Komenského, Právnická fakulta, 2021. 69 s. ISBN 978-80-7160-629-1.

ŠEBESTA, M. a kol. 2020. *eGovernment a jeho vplyv na podnikateľský sektor*. Bratislava: IA MPSVR SR, 2020. 80 s. ISBN 978-80-8273-000-8.

ŠPAČEK, D. 2012. *eGovernment: cíle, trendy a přístupy k jeho hodnocení*. 1. vydanie. Praha: C. H. Beck, 2012. 288 s. ISBN 978-80-7400-261-8.

VELŠIC, M. 2008. *E-Government na Slovensku*. Bratislava: Inštitút pre verejné otázky, 2008. 33 s. ISBN 970-80-89345-03-8.

BELÁŇOVÁ, Viera - GRELL, Michal - CHUDÁ, Daniela - ŠTEFANEC, Peter. Otvorený softvér vo verejnej správe SR. In *Dialógy o ekonomike a riadení : odbornoinformačný časopis pre členov Klubu ekonómov Ekonomickej univerzity a jej absolventov*. - Bratislava : Klub ekonómov Ekonomickej univerzity v Bratislave, 2006. ISSN 1335-4582, marec 2006, roč. 8, č. 24, s. 43-50.

NEUBAUEROVÁ, E., DUBROVINA, N. 2010. Verejná správa v Slovenskej republike - aktuálne problémy. IN: *Veřejná správa 2010: sborník příspěvků z vědecké konference s mezinárodní účastí: Seč u Chrudimi, 20. – 21. 9. 2010*. Pardubice: Univerzita Pardubice, Fakulta ekonomicko-správní, 2010. 156 – 163 s. ISBN 978-80-7395-334-8.

MADLEŇÁKOVÁ, L., MADLEŇÁK, R. 2012. Analýza využívania služieb e-Governmentu v SR. IN: *Pošta, Telekomunikácie a Elektronický obchod*. II/2012. 58 – 69 s. ISSN 1336-8281.

Aplikace e-Podatelna. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://epodatelna.justice.cz/ePodatelna/homepage>>.

Bankovní identita. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.businessinfo.cz/navody/bankovni-identita-ppbi/2/>>.

BankID. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.bankid.cz/>>.

BIZNÁR, M. 2018. Čo je to e-Government, utópia pre Slovensko? [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.techbox.sk/co-je-to-e-government-utopia-pre-slovensko/>>.

BOCAK, M. a kol. 2010. Texty elektronických médií: Stručný výkladový slovník. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<http://obornik.sk/images/Slovník.pdf>>.

Certifikát pre elektronický podpis. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://eidas.disig.sk/sk/certifikaty/certifikat-pre-elektronicky-podpis/>>.

Co je to e-Government? [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://sites.google.com/site/cojetoegov/vyhody-a-nevyhody-e-governmentu>>.

Co je bankovní identita a kde sa vám hodí. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/bankovni-identita>>.

Co je to Czech POINT? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://www.mvcr.cz/clanek/co-je-czech-point.aspx>>.

Čechom pomôže heslo do elektronického bankovníctva komunikovať so štátom a firmami. [online]. 2023. [cit. 2023-02-15]. Dostupné z: WWW: <<https://www.trend.sk/financie/cechom-pomoze-heslo-elektronickeho-bankovnictva-komunikovat-statom-aj-firmami>>.

Čo je hashovanie? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://sk.theastrologypage.com/hashing>>.

Čo je elektronický podpis a ako ho získať v roku 2022? [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://podnikam.sk/co-je-elektronicky-podpis-a-ako-ho-ziskat/>>.

Dátové schránky. [online]. 2023. [cit. 2023-01-27]. Dostupné z: WWW: <<https://info.mojedatovaschranka.cz/info/cs/>>.

E-Gov.sk – e-Government. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://portal.egov.sk/sk/content/egovernment>>.

E-Government. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/Sylaby/e-Government_power_point.pdf>.

Elektronická komunikace. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.sslch.cz/files/163/3-elektronicka-komunikace-u.pdf>>.

Elektronická značka. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://napoveda.slovaknet.sk/inpage/elektronicka-znacka-886/>>.

Národný bezpečnostný úrad, Elektronický podpis. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.nbu.gov.sk/index.html>>.

Návod na použitie portálu.. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.slovensko.sk/sk/navody/navod-na-pouzitie/>>.

O portáli. [online]. 2022. [cit. 2022-11-25]. Dostupné z WWW: <<https://www.slovensko.sk/sk/o-portali>>.

Prihlásenie cez portál slovensko.sk. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://prihlasenie.slovensko.sk>>.

Prihlásenie na ÚPVS. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <https://www.slovensko.sk/_img/CMS4/Navody/postup_prihlasenie_na_portal.pdf>.

Princípy eGov. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<http://info.egov.sk/node/90>>.

Projekt – Elektronické služby spoločných modulov ÚPVS a prístupových komponentov. 2012. [online]. 2022. [cit. 2022-11-26]. Dostupné z WWW: <<https://www.uvo.gov.sk/vyhľadavanie-dokumentov/document/3153117/content/1186766/download>>.

Projekt II – Elektronické služby spoločných modulov ÚPVS a prístupových komponentov II. 2015. [online]. [cit. 2022-11-26]. Dostupné z WWW: <<https://metais2.vicepremier.gov.sk/detail/Projekt/1919aafb-895a-4471-9bec-b72c834e62c4/cimaster?tab=basicForm>>.

Slovensko.sk. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.slovensko.sk/sk/titulna-stranka>>.

REMOVČÍKOVÁ, L. 2022. Koniec certifikátov pre e-podpis od 1.1.2023: koho sa to týka a čo robiť? [online]. 2023. [cit. 2023-01-29]. Dostupné z WWW: <<https://www.podnikajte.sk/zakonne-povinnosti-podnikatela/koniec-certifikatov-epodpis>>.

SALNER, A., MIŠINA, J. 2007. *Stav eGovernmentu na Slovensku, príčiny a riešenia: výskumná správa*. [online]. Bratislava: Inštitút pre dobre spravovanú spoločnosť, 2007. 27 s. [cit. 2022-11-26]. Dostupné z WWW: <https://www.governance.sk/wp-content/uploads/2016/10/eGov_sk.pdf>.

STANEK, M. 2004. *Základy kryptológie*. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://fmfi-uk.hq.sk/Informatika/Kryptologia/prednasky/krypto.pdf>>.

Symetrická a asymetrická kryptografia. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.itnetwork.sk/bezpecnost/symetricka-a-asymetricka-kryptografia>>.

Usmernenie k základným povinnostiam podľa zákona o e-Governmente. [online]. 2023. [cit. 2023-01-27]. Dostupné z WWW: <<https://www.mirri.gov.sk/wp-content/uploads/2018/10/Usmernenie-k-vykonu-verejnej-moci-elektronicky-od-1.11.2016.pdf>>.

Ústredný portál verejnej správy. [online]. [cit. 2022-11-25]. Dostupné z WWW: <<https://www.indprop.gov.sk/o-urade/elektronicke-sluzby/elektronicke-sluzby-vseobecne/ustredny-portal-verejnej-spravy-upvs>>.

Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe

Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy

Zákon č. 261/1995 Z. z. o informačných systémoch verejnej správy

Zákon č. 365/2000 Sb., o informačných systémoch verejnej správy v platnom znení

Zákon č. 300/2008 Sb., o elektronických úkonoch a autorizovanej konverzii dokumentov

Zákon č. 111/2009 Sb. o základných registroch

Zákon č. 486/2004 Sb., o elektronickom podpise a o zmene niektorých ďalších zákonov

Vyhláška č. 194/2009 Sb. o stanovení podrobností užívania a prevádzkovania informačného systému elektronických schránok

Vyhláška č. 438/2019 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente

ZOZNAM SKRATIEK

BankID – banková identita

ČR – Česká republika

EZ – elektronická značka

IKT – informačno-komunikačné technológie

KEP – kvalifikovaný elektronický podpis

NASES – Národná agentúra pre sieťové a elektronické služby

NBS – Národná banka Slovenska

NIA – Národný bod pre identifikáciu a autorizáciu

SR – Slovenská republika

ÚPVS – Ústredný portál verejnej správy

ZOZNAM OBRÁZKOV, TABULIEK A GRAFOV

Zoznam obrázkov

Obrázok 1 Významové dimenzie pojmu verejnej správy	13
Obrázok 2 Štruktúra verejnej správy v SR.....	15
Obrázok 3 Úvodná informačná stránka ÚPVS	20
Obrázok 4 Prihlásenie na portál ÚPVS.....	21
Obrázok 5 Výber spôsobu prihlásenia	22
Obrázok 6 Výhody a nevýhody e-Governmentu	33

Zoznam tabuliek

Tabuľka 1 Obsah certifikátu	48
-----------------------------------	----