

# **Datové schránky**

Barbora Nečasová

---

Bakalářská práce  
2016



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

## **ZADÁNÍ BAKALÁŘSKÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Barbora Nečasová**  
Osobní číslo: **A12635**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Informační technologie v administrativě**  
Forma studia: **prezenční**

Téma práce: **Datové schránky**  
Téma anglicky: **Data-boxes**

Zásady pro vypracování:

1. **Objasněte určení, architekturu a způsob použití datových schránek.**
2. **Analyzujte legislativu spojenou s datovými schránkami.**
3. **Specifikujte vazbu mezi datovými schránkami a elektronickou spisovou službou.**
4. **Na základě průzkumu identifikujte základní problémy datových schránek.**
5. **Specifikujte trendy rozvoje datových schránek.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SMEJKAL, Vladimír a Michal Altair VALÁŠEK.** Jak na datovou schránku: praktický manuál pro každého. Praha: Linde, 2012, 197 s. ISBN 978-80-86131-80-1.
2. **BUDIŠ, Petr a Iva HŘEBÍKOVÁ.** Datové schránky: fungování, doručování, bezpečnost, návody. 1. vyd. Olomouc: ANAG, 2010, 287 s. ISBN 978-80-7263-617-4.
3. **LAPÁČEK, Jiří.** Jak na datovou schránku a elektronickou komunikaci s úřady. Brno: Computer Pres, 2012. ISBN 978-80-251-3680-5.
4. **BUDIŠ, Petr.** Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority : legislativní rámec elektronického podpisu : praktické aplikace. 1. vyd. Olomouc: ANAG, 2008, 157 s. ISBN 978-80-7263-465-1.
5. **MATES, Pavel a Vladimír SMEJKAL.** E-government v České republice: právní a technologické aspekty. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012, 464 s. ISBN 978-80-87576-36-6.

Vedoucí bakalářské práce:

**doc. Ing. Luděk Lukáš, CSc.**

Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce:

**5. února 2016**

Termín odevzdání bakalářské práce:

**1. června 2016**

Ve Zlíně dne 5. února 2016



doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



Ing. Miroslav Matýsek, Ph.D.  
*ředitel ústavu*

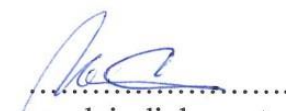
### Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen přípouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

### Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 31.5. 2016

  
.....  
podpis diplomanta

## **ABSTRAKT**

Cílem této bakalářské práce je analýza problematiky spojené s datovými schránkami. Teoretická část obsahuje vysvětlení pojmu datové schránky legislativu s nimi spojenou a vazbu mezi datovými schránkami a elektronickým systémem spisové služby. Hlavní část práce se věnuje problémům souvisejícím s datovými schránkami, které jsem mapovala pomocí dotazníkového šetření. Závěr práce se soustředí na budoucí vývoj datových schránek.

**Klíčová slova:** datové schránky, legislativa spojená s datovými schránkami, elektronický systém spisové služby, elektronický systém datových schránek, budoucnost datových schránek, dotazník

## **ABSTRACT**

The aim of this work is to analyze the problems associated with data boxes. Theorematic section explains the concept of data boxes legislation associated with them and the linkage between data boxes and electronic records management systems. The main part is devoted to the problems associated with data boxes, which I mapped using a questionnaire. Conclusion of the work will focus on the future development of data boxes.

**Keywords:** data boxes, legislation associated with data boxes, electronic records management, electronic data exchange system, the future of data boxes questionnaire

Tímto bych chtěla poděkovat vedoucímu bakalářské práce panu doc. Ing. Lud'ku Lukášovi, CSc, za čas, který mi věnoval a za poskytnutí rad během vypracovávání. Dále bych chtěla poděkovat rodině a přátelům za jejich podporu.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

# OBSAH

<b>ÚVOD.....</b>	<b>8</b>
<b>I TEORETICKÁ ČÁST.....</b>	<b>9</b>
<b>1 DATOVÉ SCHRÁNKY .....</b>	<b>10</b>
1.1 E-GOVERNMENT .....	10
1.2 CZECH POINT .....	11
1.3 DATOVÉ SCHRÁNKY .....	12
1.4 INFORMAČNÍ SYSTÉM DATOVÝCH SCHRÁNEK .....	14
1.5 ARCHITEKTURA DATOVÝCH SCHRÁNEK .....	15
Přístupové rozhraní.....	16
1.6 ZŘÍZENÍ DATOVÉ SCHRÁNKY .....	17
1.6.1 Datové schránky zřízené ze zákona .....	18
1.6.1.1 Datová schránka právnické osoby .....	18
1.6.1.2 Datová schránka orgánu veřejné moci.....	18
1.6.2 Datové schránky zřízené na žádost .....	18
1.6.2.1 Datové schránky fyzické osoby .....	19
1.6.2.2 Datová schránka podnikající fyzické osoby .....	19
1.7 REALIZACE PODÁNÍ ŽÁDOSTI O ZŘÍZENÍ DATOVÉ SCHRÁNKY .....	19
1.8 POUŽITÍ PŘÍSTUPOVÝCH ÚDAJŮ .....	21
1.8.1 Uživatelské jméno a heslo.....	21
1.8.2 Uživatelské jméno a heslo plus certifikát.....	22
1.8.3 Uživatelské jméno a heslo plus bezpečnostní kód .....	22
1.8.4 Uživatelské jméno a heslo plus SMS kód .....	24
1.9 ELEKTRONICKÝ PODPIS .....	24
1.10 ZNEPŘÍSTUPNĚNÍ DATOVÉ SCHRÁNKY .....	25
1.11 STRUČNÉ SHRNUÍ .....	26
<b>2 LEGISLATIVA .....</b>	<b>27</b>
2.1 ZÁKON Č. 300/2008 SB., O ELEKTRONICKÝCH ÚKONECH A AUTORIZOVANÉ KONVERZI DOKUMENTŮ .....	27
2.2 ZÁKON Č. 499/2004 SB., O ARCHIVNICTVÍ A SPISOVÉ SLUŽBĚ .....	28
2.3 ZÁKON Č. 227/2000 SB., O ELEKTRONICKÉM PODPISU .....	29
2.4 ZÁKON Č. 365/2000 SB., O INFORMAČNÍCH SYSTÉMECH VEŘEJNÉ SPRÁVY .....	30
2.5 STRUČNÉ SHRNUÍ .....	30
<b>3 VAZBA DATOVÝCH SCHRÁNEK A ELEKTRONICKÉHO SYSTÉMU SPISOVÉ SLUŽBY.....</b>	<b>31</b>
3.1 DEFINICE ELEKTRONICKÉHO SYSTÉMU SPISOVÉ SLUŽBY .....	31
3.1.1 Elektronická podatelna.....	31
3.1.2 Životní cyklus datové zprávy .....	32
3.1.2.1 Doručená datová zpráva.....	32
3.1.2.2 Odeslaná datová zpráva .....	33

3.2	STANDARD PRO KOMUNIKACI MEZI INFORMAČNÍM SYSTÉMEM DATOVÝCH SCHRÁNEK A SPISOVÝMI SLUŽBAMI .....	33
3.3	KONVERZE DOKUMENTŮ .....	35
3.3.1	Konverze z listinné do elektronické podoby .....	36
3.3.2	Konverze z elektronické do listinné podoby .....	37
3.3.3	Důvody znemožňující autorizovanou konverzi dokumentů .....	38
3.4	STRUČNÉ SHRnutí .....	39
<b>II</b>	<b>PRAKTICKÁ ČÁST .....</b>	<b>40</b>
<b>4</b>	<b>PROBLEMATIKA DATOVÝCH SCHRÁNEK.....</b>	<b>41</b>
4.1	CÍL VÝZKUMU .....	41
4.2	POUŽITÁ METODA VÝZKUMU.....	41
4.3	VYHODNOCENÍ VÝSLEDKŮ PRŮZKUMU .....	41
4.3.1	Shrnutí dotazníkového šetření.....	52
<b>5</b>	<b>SPECIFIKUJTE TRENDY ROZVOJE DATOVÝCH SCHRÁNEK.....</b>	<b>54</b>
5.1	SOUČASNÉ TRENDY .....	54
5.2	POHLED DO BUDOUCNA .....	54
	<b>ZÁVĚR .....</b>	<b>58</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>59</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>62</b>
	<b>SEZNAM OBRÁZKŮ .....</b>	<b>63</b>
	<b>SEZNAM TABULEK.....</b>	<b>CHYBA! ZÁLOŽKA NENÍ DEFINOVÁNA.</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>64</b>



## ÚVOD

Datové schránky jsou hlavním tématem bakalářské práce. Dnes jsou nedílnou součástí elektronické komunikace a e-governmentu - slouží především pro komunikaci s úřady. Jedná se tedy o náhradu klasických dopisů, které jsou na ústupu. Cílem práce je především zkoumat problémy spojené s datovými schránkami a návrh budoucnosti spojenou s datovými schránkami.

V první kapitole teoretické části budou rozebrány souvislosti s datovými schránkami. Tedy definice pojmu datová schránka, informační systém datových schránek, jejich architektura a další náležitosti.

Druhá kapitola teoretické části se bude zabývat legislativou spojenou s datovými schránkami. Tedy nejen zákonem, který zavedl používání datových schránek, ale také zákony které nepřímo souvisí s užíváním datových schránek.

Třetí a zároveň poslední kapitola teoretické části objasní pojem elektronický systém spisové služby a také vztah mezi Informačním systémem datových schránek a elektronickým systémem spisové služby.

Praktická část se bude soustředit zejména na problematiku spojenou s datovými schránkami, kterou budu zjišťovat pomocí dotazníkového šetření. Výsledky následně popíšu a pokusím se je zdůvodnit. Dotazník tedy pomůže specifikovat problémy z pohledu uživatelů datových schránek.

V druhé části budou specifikovány trendy datových schránek, jejich možný vývoj v budoucnu a popřípadě návrh na řešení problémů zjištěných v předchozí kapitole (dotazníkové šetření).

## **I. TEORETICKÁ ČÁST**

# 1 DATOVÉ SCHRÁNKY

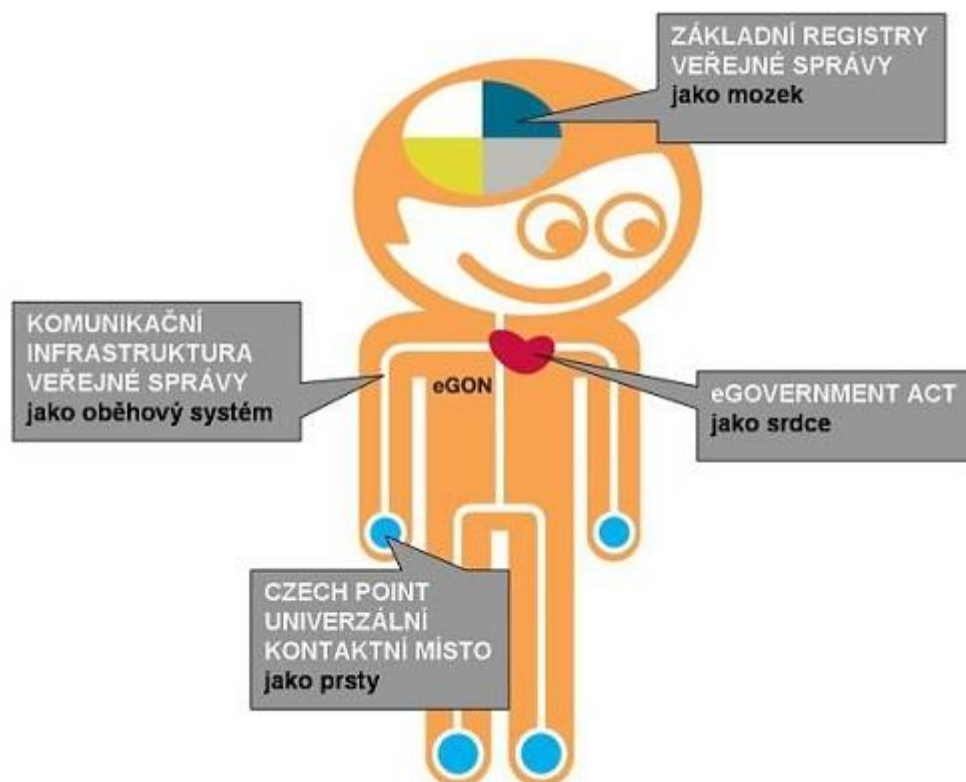
## 1.1 E-government

Výraz e-government (electronic government) se nepřekládá do češtiny, protože nikdy asi nebude úplně přesný. Proto se raději soustředím na jeho definici. E-government lze chápat jako možnost administrativní komunikace s institucemi státní a veřejné správy v elektronické podobě a všechny procesy, které s tím souvisejí (zejména tvorba příslušné legislativy a přechod úřadů na elektronickou verzi vedení agendy). Dal by se tedy popsat i jako elektronizace veřejné správy. Účelem e-governmentu je usnadnit komunikaci mezi veřejností (občany a podniky) s úřady, ale také zlepšit přístup k informacím pro občany a zvýšení efektivity veřejné správy (a tím ušetřit finance).

Výhodou e-governmentu je to, že lidé nemusí nikam chodit (pokud jejich osobní účast není nezbytná). Lze vše zařídit z domova pomocí počítače. E-government má uplatnění i při vybírání daní, výkonu spravedlnosti, sociálním zabezpečením a další. Komunikace probíhá většinou pomocí datových schránek, které jsou jednou z cest eGovernmentu. Zároveň s Czech POINTem jsou datové schránky nejviditelnějším projevem E-governmentu v České republice. Další oblastí e-governmentu může být eHealth (elektronické zdravotnictví) nebo eVolby (elektronické volby). [10], [11]

Výčet oblastí a činností, jež jsou součástí eGovernmentu v České republice:

- informační systém veřejné správy (dále jen ISVS),
- elektronická komunikace,
- ochrana osobních údajů,
- elektronický dopis, elektronická značka,
- elektronická správní řízení, elektronická podání, e-podatelný, e-volby,
- dlouhodobé uchovávání elektronických dokumentů,
- konverze dokumentů,
- registry veřejné správy,
- informační audit,
- bezpečnost a ochrana utajovaných informací,
- bezpečnost – komplexní zabezpečení informačního systému,
- eCommerce,
- elektronické veřejné zakázky. [11]



Obr. 1: Symbol eGovernmentu – panáček eGon (zdroj: [www.egovernment.unas.cz](http://www.egovernment.unas.cz))

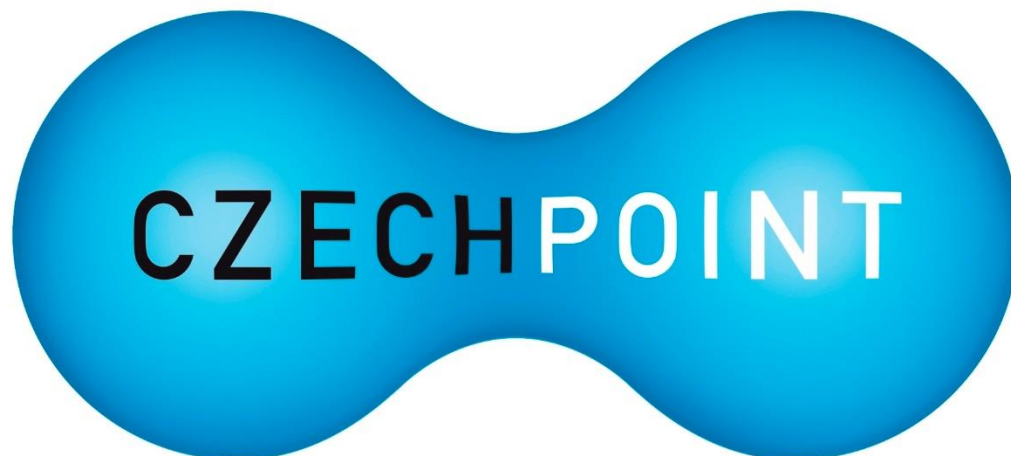
## 1.2 Czech POINT

Czech Point (Český podací ověřovací informační národní terminál) je síť pracovišť, který je označován jako kontaktní místa veřejné správy a provozuje jej Ministerstvo vnitra. Právní úprava Czech POINTu se nachází v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy. Kontaktními místy veřejné správy jsou notáři, matriční úřady, krajské úřady, obecní úřady, a další právnické osoby (např. provozovny České pošty). Czech POINT má za účel ulehčení komunikace se státem. Je také prostředníkem mezi občanem a Informačním systémem datových schránek (dále jen ISDS) a je zde možné např. zřídit datovou schránku, znepřístupnit datovou schránku nebo zneplatnit přístupové údaje. Žadatel musí vždy předložit doklad totožnosti, pokud zastupuje jinou osobu, musí předložit notářsky ověřenou plnou moc. Pokud jedná za právnickou osobu, musí předložit jakýkoliv úředně ověřený dokument, který určuje danou osobu jako jednatele či statutární orgán za danou právnickou osobu. Na pobočkách je možné získat výpisy a informace o údajích vedených v centrálních registrech (vydání ověřených výstupů z informačních systémů veřejné správy). [1], [22]

**Czech POINT poskytuje tyto služby:**

- autorizovanou konverzi dokumentů,

- centrální úložiště ověřovacích doložek,
- datové schránky,
- podání do registru účastníků provozu modulu autovraků ISOH (informační systém odpadového hospodářství),
- přijetí podání podle živnostenského zákona (§ 72),
- úschovna systému Czech POINT,
- vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů,
- výpis z bodového hodnocení řidiče,
- výpis z insolvenčního rejstříku,
- výpis z Katastru nemovitostí,
- výpis z Obchodního rejstříku,
- výpis z Rejstříku trestů,
- výpis z Rejstříku trestů právnické osoby,
- výpis z Živnostenského rejstříku,
- přístup k základním registrům. [1]



Obr. 2: Logo Czech POINTu (Zdroj: [www.khkpce.cz](http://www.khkpce.cz))

### 1.3 Datové schránky

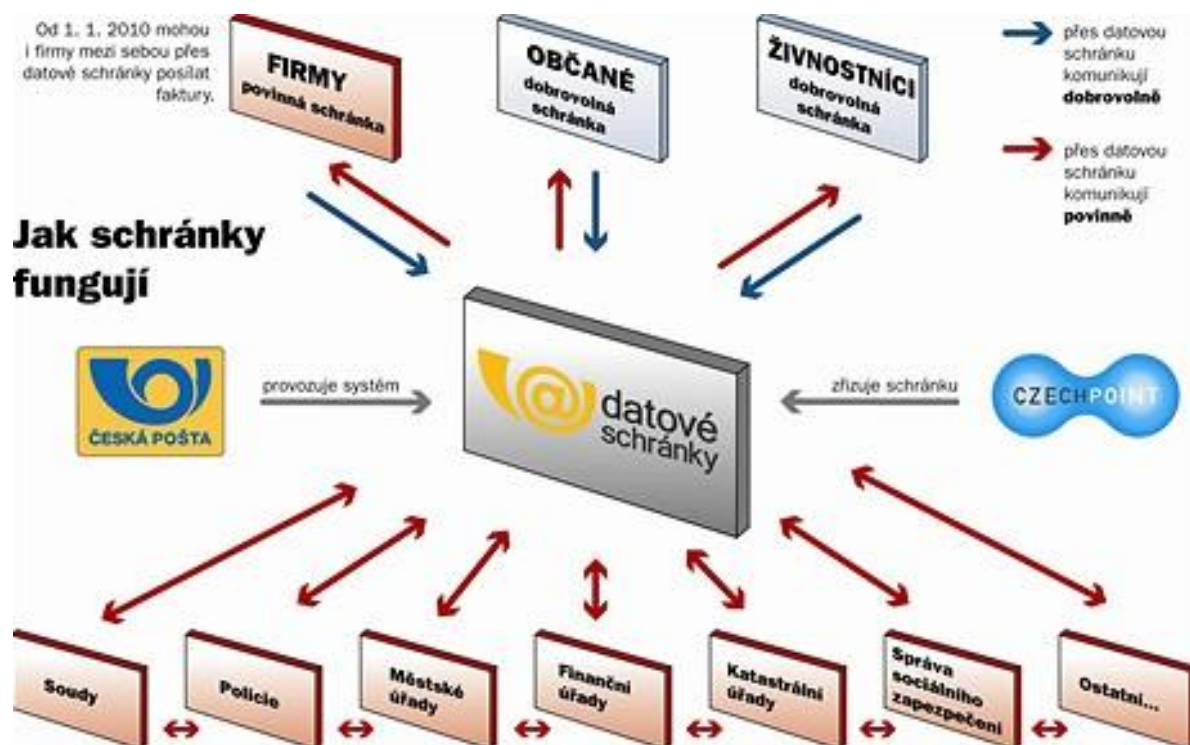
Datové schránky jsou dle zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, definovány jako prostředek pro zajištění elektronické komunikace v rámci e-Governmentu (přijímat a posílat elektronické dokumenty úřadům), který je elektronické úložiště sloužící k:

- Doručování elektronických zpráv orgánům veřejné moci,
- provádění úkonů vůči orgánům veřejné moci.
- dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. [1]

Tato služba však není obdobou e-mailové pošty, ani s ní není funkčně propojena (datové zprávy nelze posílat na e-mailovou adresu a ani opačně). Jedná se spíše o elektronickou obdobu klasické pošty v listinné podobě, tedy jakousi oficiální elektronickou komunikaci. E-mail není vhodný k doručování úředních dokumentů z několika důvodů. Hrozí zde nebezpečí odposlechu, modifikace, nedoručení a lze snadno zfalšovat jméno a adresu odesílatele. Z těchto důvodů byly zavedeny datové schránky jako důvěryhodný systém pro doručování elektronických zpráv. [3]

Mají za úkol efektivnější – tedy rychlejší, spolehlivější a levnější komunikaci s veřejnou správou. Uživatel se přihlašuje heslem uživatelským jménem – ID osoby, které slouží k identifikaci osoby, která zprávu odeslala (popřípadě přijala). Zřízení datové schránky je zdarma (zřizuje Česká pošta). Pouze subjekt, jenž má zřízenou datovou schránku může zasílat dokumenty, nebo zjišťovat, zda nějaký subjekt má zřízenou datovou schránku. Výjimku tvoří pouze možnost zjistit údaje o datové schránce veřejné moci. [1], [4]

Datová schránka však není určena k archivaci doručených dokumentů (datových zpráv), protože datová zpráva je ve schránce k dispozici pouze 90 dnů. Její velikost ale není nijak omezena. [1]



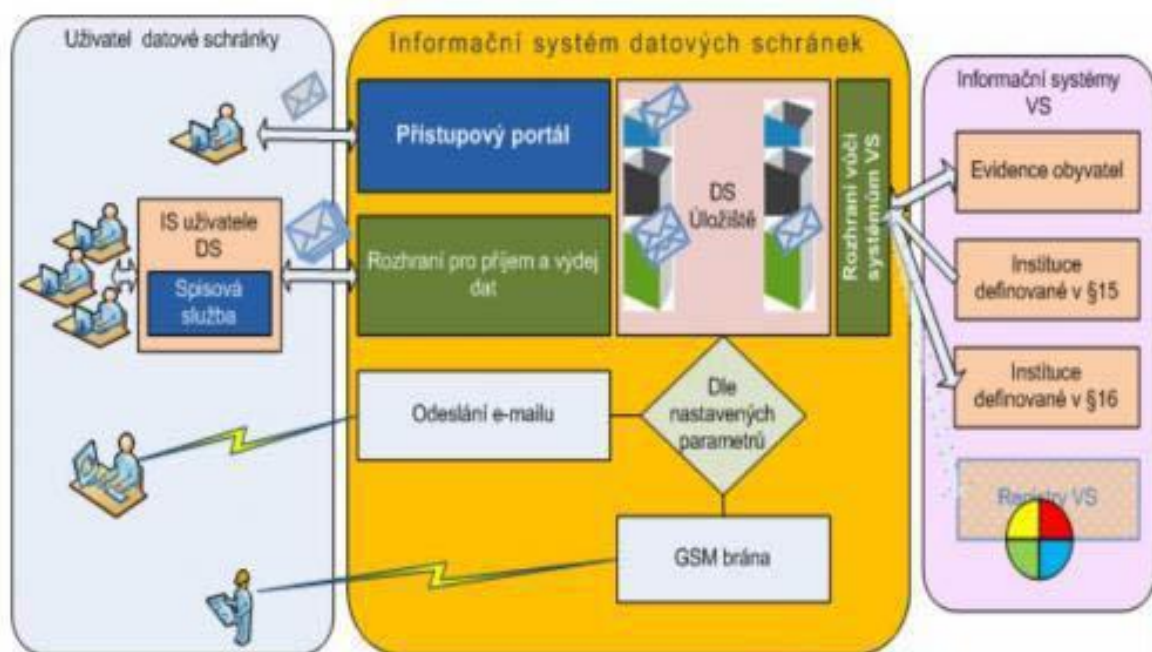
Obr. 3: Fungování datových schránek (zdroj: www.inflow.cz)

#### 1.4 Informační systém datových schránek

Provozovatelem ISDS je Česká Pošta, která provádí některé informační činnosti související s ISDS. Na ISDS se vztahuje zákon č. 365/2000 Sb., o informačních systémech veřejné správy. V souvislosti se správou ISDS Ministerstvo vnitra zajišťuje úkoly sloužící k zajištění důvěryhodnosti a neporušenost doručovaných datových zpráv. Ministerstvo vnitra zajišťuje informační servis o jednotlivých úkonech, a to:

- oznámení odesílatelům, že datové zprávy, které odeslali, byly dodány do datové schránky adresáta,
- ke každé datové zprávě odeslané z datové schránky je připojeno kvalifikované časové razítko,
- informování adresáta o dodání datové zprávy do jeho datové schránky na jím zvolenou e-mailovou adresu, nebo jiné technické zařízení, a to na náklady adresáta,
- oznamování odesílatelům, že datová zpráva, kterou odeslali, byla v pořádku doručena,
- oznámení odesílatelům, že datová schránka, do které odeslali datovou zprávu, neexistuje,

- oznámení odesílatelům, že datová schránka, do které odeslali datovou zprávu, je znepřístupněna a to i zpětně,
- oznámení odesílatelům, že datová schránka, do které odeslali datovou zprávu, je zrušena.



Obr. 4: Schéma informačního systému datových schránek (zdroj: [www.datove-schranky.eu](http://www.datove-schranky.eu))

V ISDS jsou tedy vedeny informace o datových schránkách, jejich uživateli a veškerá manipulace s jejich obsahem.

Správce a provozovatel ISDS zajišťuje příslušná opatření v oblasti bezpečnosti. Správce ani provozovatel nejsou oprávněni k přístupu do datových schránek jiných subjektů. Přístup k datové schránce je možný prostřednictvím webového rozhraní, které provozuje Ministerstvo vnitra České republiky. [1], [3]

## 1.5 Architektura datových schránek

ISDS je informační systém veřejné správy (dále jen ISVS), který zabezpečuje činnost související se zřízením, zpřístupněním a provozováním datové schránky, dále má na starost identifikaci osob oprávněných k přístupu do datové schránky. Datové schránky pracují jako systém, jehož hlavním úkolem je předávání datových zpráv od odesílatele k příjemci. Odesílací brána umožňuje konceptu zprávy do formátu ISDS, kde tento koncept může uživatel schválit a odeslat. [1], [21]



### Přístupové rozhraní

Uživatel se přihlašuje prostřednictvím přístupového rozhraní. Úkolem přístupového rozhraní je propojení jiných internetových aplikací s datovými schránkami tak, aby uživatel jiné aplikace mohl obsluhovat svou datovou schránku v celém rozsahu, aniž by se přihlásil přístupovými údaji k datové schránce. Přihlášení k datové schránce je prováděno jako propojení uživatelského účtu v internetové aplikaci s uživatelským účtem ISDS. ISDS využívá dva způsoby pro zajištění tohoto úkolu. První způsob, který je jednodušší a častější variantou, je využití internetového prohlížeče. Druhým způsobem je využití otevřeného rozhraní webových služeb. [20], [1]

U prvního způsobu je potřeba pouze počítač s operačním systémem, přístup k internetu a internetový prohlížeč. Přihlášení k ISDS prostřednictvím uživatelského jména a hesla probíhá přes https (HyperText Transfer Protocol Secure). HTTPS je bezpečnostní nadstavba protokolu http, který se používá u běžných webových aplikací. Přenášovaná data jsou šifrována, v našem případě uživatelské jméno a bezpečnostní heslo (nebo využití certifikátu). Tato základní varianta umožňuje příjem a vytváření datových zpráv (včetně přiřazení příloh a připojení adresáta), ale pouze v menším množství. [1]

Druhou variantou připojení využívají zejména orgány veřejné moci v rámci přístupu z interních informačních systémů nebo elektronického systému spisové služby. Dále tuto možnost využívají uživatelé, kteří mají datovou schránku napojenou na interní systém (DMS nebo ERP) a vytvářejí nebo přijímají velké množství datových zpráv. ISDS v tomto případě pouze přenáší data i příslušná metadata (data popisující souvislosti obsah a strukturu zprávy) od aplikace odesílatele k aplikaci příjemce. I při použití otevřeném rozhraní webových služeb se používá podobné zabezpečení jako u běžného webového klienta. Přihlášení je tedy také prostřednictvím uživatelského jména a bezpečnostního hesla (popřípadě s využitím elektronického prostředku třetí strany). Otevřené rozhraní webových služeb pro přístup ISDS umožňuje uživatelům využívat rozšířené funkce, například zasílání datových zpráv více příjemcům najednou. [1], [24]

ISDS umožňuje napojení aplikací třetích stran (například Agendové informační systémy orgánů veřejné moci, spisové služby, ERP systém nebo DMS systémy) prostřednictvím webových služeb.

*„Webové služby pro použití v externích programech:*

- vytvoření a odeslání nové zprávy,

- vytvoření a odeslání hromadné zprávy,
- stažení došlé zprávy,
- stažení došlé zprávy s podpisem značkou Ministerstva vnitra,
- stažení odeslané zprávy s podpisem Ministerstva vnitra,
- ověření uložené datové zprávy,
- prázdná operace pro navazování nebo udržování spojení,
- před podepsání zprávy, dodejky či doručenky,
- ověření neporušení datové zprávy,
- stažení obálky došlé zprávy,
- označení zprávy jako „Přečtená“,
- stažení informace o dodání a doručování zprávy,
- stažení informace o dodání a doručování zprávy, s podpisem značkou Ministerstva, vnitra,
- stažení seznamu došlých zpráv,
- stažení seznamu odeslaných zpráv,
- doručení poštovní datové zprávy,
- stažení seznamu zpráv, u kterých došlo ke změně stavu,
- zjištění identifikace odesílatele zprávy,
- smazání dlouhodobě uložené datové zprávy (trezorové).“ [21]

## 1.6 Zřízení datové schránky

Datové schránky zřizuje a spravuje Ministerstvo vnitra z titulu ústředního správního úřadu pro oblast informačních systémů veřejné správy (dle § 12 odst. 1 písm. o) zákona č.2/1969 Sb., zřízení ministerstev a jiných ústředních orgánů státní správy, ve znění pozdějších předpisů). Datové schránky jsou zřizovány dvojím způsobem a to buď ze zákona, nebo na žádost. Zákony uvádí rozdíly mezi jednotlivými typy datových schránek, které se odrážejí ve způsobu jejich zřízení, rolích oprávněných k přístupu do datové schránky, důvodů znepřístupnění a jejich zrušení. Každý subjekt má nárok na zřízení jedné datové schránky. Je však nutné zohlednit, že jednotlivec může mít několik právních postavení, z toho důsledku má právo na zřízení více typů datových schránek (odvíjejícího od jeho právního postavení). Například podnikající fyzické osobě může být zřízená jedna datová schránka jako podnikateli a druhá jako fyzické osobě.[1], [2]

### 1.6.1 Datové schránky zřízené ze zákona

Ze zákona se zřizují datové schránky orgánům veřejné moci, právnickým osobám, organizačním složkám podniků zahraničních právnických osob zapsaným v obchodním rejstříku, insolvenčním správcům, advokátům a daňovým poradcům. Orgánům veřejné moci zřídí ministerstvo bezodkladně po jejich vzniku. V případě notářů soudních exekutorů advokátů daňových poradců a insolvenčních správců poté, co obdrží informaci o jejich zapsání do zákonem stanovené evidence. [3]

#### 1.6.1.1 Datová schránka právnické osoby

Občanský zákoník za právnické osoby považuje sdružení fyzických nebo právnických osob, účelová sdružení majetku, jednotky uzemní samosprávy a jiné subjekty, o kterých to stanoví zákon. Těmto subjektům zřizuje ministerstvo datovou schránku právnické osoby bezplatně na žádost této osoby do tří pracovních dnů ode dne podání žádosti. Právnická osoba má nárok na zřízení jedné datové schránky právnické osoby. [2]

#### 1.6.1.2 Datová schránka orgánu veřejné moci

Datovou schránku orgánům veřejné moci zřizuje Ministerstvo vnitra bezplatně, a ihned po jeho vzniku. Orgán veřejné moci si může zažádat o zřízení další datové schránky (může využít elektronický formulář, který odešle ze své již zřízené datové schránky). Přístup do této schránky má vedoucí orgánu veřejné moci, tedy pověřená osoba, pro něž byla datová schránka zřízena. Do této datové schránky může mít dále přístup pověřená osoba, kterou je fyzická osoba pověřena Oprávněnou osobou (v rozsahu jí stanoveným). [6]

### 1.6.2 Datové schránky zřízené na žádost

Subjekty, kterým není datová schránka zřizována ze zákona, což jsou fyzické osoby, většina podnikajících fyzických osob a část právnických osob (např. občanská sdružení, církve), mohou o zřízení požádat. Také orgány veřejné moci mohou požádat o zřízení další datové schránky. Datovou schránku zřídí ministerstvo bezplatně do 3 pracovních dnů ode dne podání žádosti. Žádost se podává Ministerstvu vnitra to buď osobně (na podatelně Ministerstva vnitra nebo na kontaktních místech veřejné správy), poštou, elektronickou poštou na adresu elektronické podatelny Ministerstva vnitra, nebo prostřednictvím datové schránky (při žádosti zřízení další datové schránky orgánu veřejné moci). [2], [3]

### ***1.6.2.1 Datová schránky fyzické osoby***

Tato datová schránka se zřizuje výhradně na žádost fyzické osoby, pro níž má být zřízena. Každá fyzická osoba má nárok na jednu datovou schránku fyzické osoby. Pokud ovšem nevystupuje ve více rolích (např. občan, podnikatel, osoba vykonávající advokacii nebo veřejnou moc), pak může mít zřízeno více datových schránek. Podmínky ke zřízení datových schránek nejsou limitovány občanstvím nebo místem pobytu. [2], [3]

### ***1.6.2.2 Datová schránka podnikající fyzické osoby***

Tato datová schránka se zřizuje všem podnikatelům, kteří provádí soustavnou činnost samostatně, vlastním jménem a na vlastní odpovědnost za účelem dosažení zisku, při čemž jím může být:

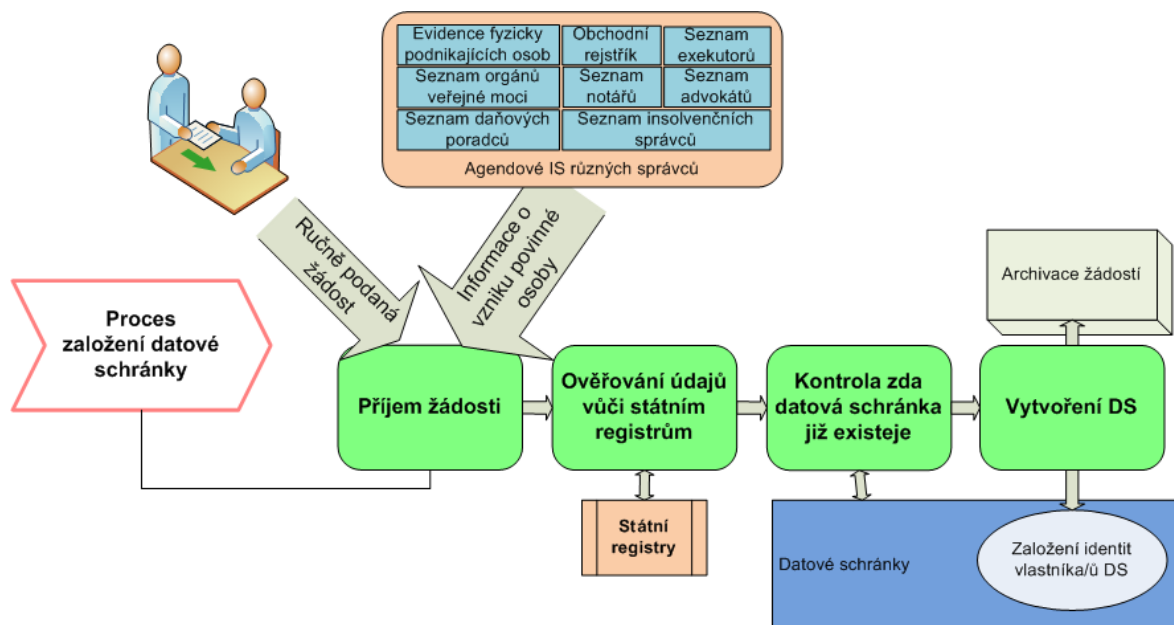
- osoba zapsaná v obchodním rejstříku,
- osoba, která podniká na základě živnostenského oprávnění,
- osoba, která podniká na základě jiného než živnostenského podle zvláštních předpisů,
- osoba, která provozuje zemědělskou výrobu a je zapsána do evidence podle zvláštního předpisu. [2], [3]

Fyzická osoba může mít zřízenou pouze jednu datovou schránku fyzické osoby a podnikající fyzická osoba může mít zřízenou pouze jednu datovou schránku podnikající fyzické osoby. [3]

## **1.7 Realizace podání žádosti o zřízení datové schránky**

O zřízení datové schránky mohou požádat ty subjekty, kterým není datová schránka zřizována ze zákona. Žádost podává osoba, pro kterou bude datová schránka zřízena. Podání žádosti lze:

- Osobně na Czech POINTu,
- písemně v listinné podobě,
- elektronickou poštou [7]



Obr. 5: Proces založení datové schránky (zdroj: www.slideshare.net)

**Forma a obsah žádosti:**

Zřízení datové schránky fyzické osoby:

- Jméno, popřípadě jména, příjmení, a jejich případné změny
- Rodné příjmení
- Den, měsíc, rok narození
- Místo a okres narození
- Státní občanství

Zřízení datové schránky podnikající fyzické osoby:

- Jméno, popřípadě jména, příjmení, a jejich případné změny
- Rodné příjmení
- Den, měsíc, rok narození
- Místo a okres narození
- Státní občanství
- Identifikační číslo osoby (bylo-li přiděleno)
- Místo podnikání

Zřízení datové schránky právnické osoby:

- Název nebo obchodní firma
- Identifikační číslo osoby (bylo-li přiděleno)
- Adresa sídla
- Jméno, příjmení, datum narození a adresa pobytu osoby, která jedná ve jménu právnické osoby

- d) Stát registrace nebo evidence právnické osoby

Zřízení další datové schránky orgánu veřejné moci:

- a) Název orgánu veřejné moci a název vnitřní organizační jednotky orgánu veřejné moci
- b) Identifikační číslo ekonomického subjektu, bylo-li přiděleno
- c) Adresa sídla
- d) Jméno, příjmení, datum narození a adresa pobytu osoby, již mají být přiděleny přístupové údaje.

Dále musí žádost obsahovat elektronický podpis nebo úředně ověřený podpis – ten se nevyžaduje v případě, kdy je žádost podepsaná před zaměstnancem Ministerstva vnitra nebo zaměstnancem kontaktního místa veřejné zprávy. [1]

## 1.8 Použití přístupových údajů

Přístupové údaje jsou zasílány na adresu Oprávněné osoby nebo administrátora, kterou zadala Oprávněná osoba při zadávání žádosti o zřízení účtu Pověřené osoby nebo Administrátora. Přístupové údaje jsou pro každého unikátní. Ke zpřístupnění datové schránky buď po prvním přihlášení, nebo 15. den po doručení přístupových údajů. Tímto okamžikem je datová schránka zpřístupněna jak pro uživatele, který datovou schránku vlastní, tak pro ty, kteří do ní chtějí zasílat datové zprávy. [8], [3]

Do webového rozhraní ISDS se jako uživatel lze přihlásit těmito metodami:

- uživatelské jméno a heslo,
- uživatelské jméno a heslo plus certifikát,
- uživatelské jméno a heslo plus bezpečnostní kód,
- uživatelské jméno a heslo plus SMS kód. [3]

### 1.8.1 Uživatelské jméno a heslo

Nejjednodušším způsobem přihlášení je přihlášení uživatelským jménem a heslem, který je pro všechny uživatele výchozí. **Uživatelské jméno** je náhodně vygenerovaným řetězcem písmen a číslic a má délku 6 až 12 znaků a nezáleží, zda při jeho zadávání použijete velká či malá písmena. Uživatelské jméno je možné změnit, procesem zneplatnění a vydání nových přihlašovacích údajů. Uživatelské jméno lze měnit pouze za jiný automaticky vygenerovaný kód. **Heslo** obsahuje 8 až 32 znaků, přičemž záleží na velkých a malých písmenech. Heslo je zasláno společně s uživatelským jménem při zřízení, ale při prvním přihlášení je nutno ho

změnit. Pokud subjekt vlastní více datových schránek, jsou na sobě nezávislé a každá má své přístupové údaje. [3]

Infolinka 270 005 200

Czech POINT

Portál veřejné správy

@ datové schránky

Moje datová schránka

Přihlášení jménem a heslem

Přihlášení certifikátem

Přihlášení pomocí SMS

Přihlášení bezpečnostním kódem

Uživatelské jméno

Heslo

Otevřít grafickou klávesnici

Přehrát kód

Vytvořit nový kód

Opište kód z obrázku

Přihlásit se

81320

Vyplňte své uživatelské jméno a heslo, opište kód z obrázku a přihlaste se. Pokud jste se ještě nikdy nepřihlašovali do své datové schránky, použijte přihlašovací údaje, které Vám byly vygenerovány systémem a doručeny v obálce se žlutým pruhem nebo prostřednictvím akivačního portálu.

[Jste zde poprvé?](#)

[Nemůžete se přihlásit?](#)

[Nápověda](#)

[Informační web datových schránek](#)

Obr. 6: Přihlášení pomocí jména a hesla (zdroj: [www.mojedatovaschranka.cz](http://www.mojedatovaschranka.cz))

### 1.8.2 Uživatelské jméno a heslo plus certifikát

Do datové schránky je možné se přihlašovat také pomocí elektronických prostředků, které obsahují autentizační certifikát, což umožňuje větší bezpečnost. Jedná se o dodatečnou autentizační metodu, která doplňuje přihlášení pomocí hesla. Pokud je tato metoda povolena, pro přihlášení je nutné zadat uživatelské jméno, heslo a zároveň mít přihlašovací certifikát (bez kterého se není možné přihlásit). Ten bývá vydáván akreditovaným poskytovatelem certifikačních služeb. [3]

### 1.8.3 Uživatelské jméno a heslo plus bezpečnostní kód

Další možností zabezpečení je ochrana jednorázovým heslem, kterému se říká bezpečnostní kód. Jeho použití je pouze doplňkem pro uživatelské jméno a heslo. Tento kód lze použít

pouze k jedinému přihlášení, potom je bezcenné. Jednorázová hesla se generují speciálním nástrojem. Ten může být jak hardwarový tak softwarový. **Hardwarový token** je malý (vypadá jako přívěšek na klíče) a má na sobě numerický displej a tlačítko, po jehož zmáčknutí se na displeji objeví číselné heslo. **Softwarový token** je speciální aplikace, která běží na chytrém telefonu s operačním systémem a pracuje stejně jako hardwarový token. Tyto aplikace jsou snadno dostupné a většinou bezplatné. [3]



Obr. 7: Hardwarový token (zdroj: [www.webobjects2.cdw.com](http://www.webobjects2.cdw.com))





Obr. 8: Softwarový token (zdroj: www.recarta.co.uk)

#### 1.8.4 Uživatelské jméno a heslo plus SMS kód

Poslední možností dodatečné ochrany je použití hesla zasláného na mobilní telefon krátké textové zprávy. Jde opět o jednorázové heslo, které je zasláno po síti operátora. Přihlášení není závislé na konkrétním přístroji nebo SIM kartě, ale pouze na telefonním čísle. V době přihlášení je nutné, aby v době přihlášení byl mobilní telefon v dosahu sítě. Za každou poslanou SMS (a tedy za každé přihlášení) se platí prostřednictvím svého operátora. [3]

Infolinka 270 005 200

Czech POINT

Portál veřejné správy

@ datové schránky

Moje datová schránka

Přihlášení jménem a heslem

Přihlášení certifikátem

Přihlášení pomocí SMS

Přihlášení bezpečnostním kódem

Uživatelské jméno

Heslo

SMS kód

Přihlásit se

Otevřít grafickou klávesnici

Zaslat SMS s kódem

**i**

Vyplňte své uživatelské jméno a heslo a stiskněte tlačítko pro zaslání SMS. Na mobilní telefon Vám obratem doručíme kód, který opište do zbývajících polí a přihlaste se. Bezplatnou alternativou k tomuto způsobu přihlašování je přihlášení bezpečnostním kódem.

[Jste zde poprvé?](#)

[Nemůžete se přihlásit?](#)

[Nápověda](#)

[Informační web datových schránek](#)

Obr. 9: Přihlášení pomocí SMS kódu (zdroj: www.mojedatovaschranka.cz)

### 1.9 Elektronický podpis

Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené, nebo jsou spjaté s datovou zprávou. Slouží jako jednoznačné ověření identity podepsané osoby. U běžného podpisu to umožňuje unikátnost písma, ale u elektronického podpisu to zajišťuje kryptografie. Umožňuje nám tedy bezpečnější elektronickou komunikaci. Není možné se zříci odpovědnosti za odeslání, popř. doručení dokumentu. Elektronický podpis umožňuje kvalitní zajištění důvěryhodnosti přenášených dat. Elektronický podpis je v současnosti založen na kombinaci kryptografických metod a hashovacích funkcí.

Bezpečnost elektronického podpisu je závislá na mnoha faktorech. Mezi nejvýznamnější patří například: délka šifrovacích klíčů pro asymetrickou kryptografii, typy algoritmů, kvalita nosiče a mnoho dalších. Pro ověření tohoto podpisu se používá tzv. certifikát (elektronický dokument), který by mohl být považován za obdobu průkazu totožnosti v elektronickém světě. [1], [2]

**Certifikáty** - obsahují obvykle veřejný klíč, jméno a další údaje, které slouží k identifikaci subjektu, kterému byl certifikát vydán. Dále běžně používané certifikáty obsahují datum počátku platnosti, datum ukončení platnosti, sériové číslo a další informace. Vydavatelem těchto certifikátů může být kdokoliv, kdo má k dispozici příslušnou technologii, většinou to ale bývají specializovaní poskytovatelé certifikačních služeb. [5]

### 1.10 Znepřístupnění datové schránky

Datová schránka nezaniká jejím znepřístupněním. Stále tedy existuje, pouze je zablokována a nelze do ní zasílat ani z ní odesílat datové zprávy. Znepřístupněním DS se rozumí takové opatření, jehož výsledkem je nemožnost doručování do datové schránky adresáta. To znamená, že dojde k vyřazení datové schránky ze systému. O znepřístupnění datové schránky lze požádat, pokud nebyla zřízena ze zákona (to znamená fyzické osoby a podnikající fyzické osoby). Takové žádosti, je Ministerstvo povinno vyhovět nejpozději do tří pracovních dnů od podání žádosti. Tuto žádost nemusí poslat pouze osoba, které byla datová schránka přímo vydána, ale také administrátor datové schránky.

Ministerstvo datovou zprávu znepřístupní (i zpětně) ke dni:

- Úmrtí osoby, pro niž byla DS zřízena
- Uvedenému v rozhodnutí soudu o prohlášení za mrtvého jako den úmrtí této osoby
- Nabytí právní moci rozhodnutí o zbavení nebo omezení způsobilosti této osoby k právním úkonům
- Kdy byla tato osoba omezena na osobní svobodě z důvodu vzetí do vazby, výkonu trestu odnětí svobody, výkonu zabezpečovací detence, ochranného léčení nebo ochrany zdraví lidu [2], [9]

Datovou schránku právnické osoby a datovou schránku orgánu veřejné nelze znepřístupnit na žádost. Tyto schránky lze znepřístupnit pouze dnem zrušení těchto subjektů, a tuto akci provádí Ministerstvo vnitra. [1]

Opětovné zpřístupnění datové schránky je možné na žádost fyzické nebo právnické osoby a to tak, že Ministerstvo vnitra je povinno žádosti vyhovět a to do tří dnů ode dne podání žádosti. [9]

### **1.11 Stručné shrnutí**

Datové schránky byly vytvořeny pro zjednodušení komunikace s úřady zprostředkováním pomocí internetu a webového rozhraní datových schránek. Jejich prostřednictvím je komunikace bezpečnější, rychlejší a spolehlivější než přes e-mail. Datové schránky jsou neodmyslitelnou částí e-governmentu a spravuje je ISDS, který vlastní Ministerstvo vnitra (provozovatelem je však držitel poštovní licence). ISDS má na starost všechny údaje o datových schránkách a úkony spojené s jejich provozem. Datové schránky se týkají zejména právnických osob a orgánů veřejné moci, pro které je zřízení datové schránky ze zákona povinné. Fyzické osoby a podnikající fyzické osoby si můžou datovou schránku zřídit dobrovolně. Následující kapitola bakalářské práce se bude zabývat legislativou, která s datovými schránkami souvisí.

## 2 LEGISLATIVA

Legislativu spojenou s datovými schránkami má na starosti Ministerstvo vnitra České republiky. Zákon, zabývající se datovými schránkami, který byl přijat dne 17. července 2008 a účinnosti nabyl dne 1. července 2009, je **zákon č. 300/2008 Sb.**, o elektronických úkonech a autorizované konverzi dokumentů ve znění pozdějších předpisů. Dále existují zákony, které jsou úzce spjaty s datovými schránkami a mezi ně patří **zákon č. 227/2000 Sb.**, o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, **zákon č. 499/2004 Sb.**, o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, **zákon č. 500/2004 Sb.**, správní řád, ve znění pozdějších předpisů, **zákon č. 99/1963 Sb.**, občanský soudní řád, ve znění pozdějších předpisů a **zákon č. 365/200 Sb.**, o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. V této kapitole se budu zabývat těmito vybranými zákony, které jsou z mého pohledu nejvýznamnější, co se týče datových schránek.

### 2.1 Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

Tento zákon má za úkol specifikovat způsoby elektronické komunikace v oblasti orgánů veřejné moci a také odstranit právní i organizační problémy v této oblasti, které by bránili jejímu rozvoji. Tento zákon se zabývá činnostmi, které vykonávají orgány veřejné moci prostřednictvím datových schránek a jejich komunikaci s fyzickými osobami, podnikajícími fyzickými osobami a právnickými osobami. Před platností tohoto zákona nebylo povinné, aby měly právnické osoby zřízenou datovou schránku. Největší dopad má tedy na právnické osoby a orgány veřejné moci, kteří prostřednictvím datových schránek spolu musí komunikovat od 1. července 2009.

#### Předmět úpravy (§1):

- „elektronické úkony státních orgánů, orgánů územních samosprávných celků, státních fondů, zdravotních pojišťoven, Českého rozhlasu, České televize, samosprávných komor zřízených zákonem, notářů a soudních exekutorů (dále jen „orgán veřejné moci“) vůči fyzickým osobám a právnickým osobám, elektronické úkony fyzických osob a právnických osob vůči orgánům veřejné moci a elektronické úkony mezi orgány veřejné moci navzájem prostřednictvím datových schránek,

- *dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob prostřednictvím datových schránek,*
- *informační systém datových schránek,*
- *autorizovanou konverzi dokumentů*
- *Tento zákon se nevztahuje na /dokumenty, které obsahují utajované informace. “[12]*

Tento zákon dále definuje, pojem datová schránka, a jak ji správně používat (zrušení, zneplatnění), a datová zpráva (dokument doručovaný prostřednictvím datové schránky). Také vysvětluje, co se rozumí konverzí dokumentů, k čemu slouží a jak probíhá. Konverze dokumentů se týká i **vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek**, která obsahuje technické náležitosti při autorizované konverzi dokumentů (ze dne 17. června 2009).

#### **Předmět úpravy (§ 1)**

- a) technické náležitosti provádění autorizované konverze dokumentů
- b) technické náležitosti dokumentu, který provedením konverze vznikl
- c) technické náležitosti dokumentu, jehož převedením výstup při konverzi vznikl
- d) vzor osvědčení o vykonání zkoušky zaměstnance provádějícího konverzi na žádost.

## **2.2 Zákon č. 499/2004 Sb., o archivnictví a spisové službě**

Tento zákon stanovuje právní podmínky pro vedení spisové služby v elektronické podobě. Vznikl díky modernizaci (elektronizaci) veřejné správy. Soustředí se na spisovou službu v analogové i elektronické podobě s pomocí elektronických systémů spisové služby, bez které by se datové schránky neobešly. Zákon se soustředí jak na skupinu, která vykonává spisovou službu v plném rozsahu, i na ty kteří ji vykonávají v rozsahu omezeném. Nabyt platnosti dne 23. září 2004, a říká, které dokumenty jsou vhodné k jejich uložení. Dále stanovuje jak je evidovat, ochraňovat a jak o ně pečovat, aby bylo možné jejich pozdější zpřístupnění a použití (informační, vědecké, kulturní a správní). Dokumentem se zde rozumí každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace (digitální nebo analogová), která byla vytvořena, nebo doručena původcem. Může se tedy jednat i o přijatou datovou zprávu.

#### **Předmět úpravy (§ 1)**

„a) výběr a evidenci archiválií,

- b) ochranu archiválií,*
- c) práva a povinnosti vlastníků archiválií,*
- d) práva a povinnosti držitelů a správců archiválií (dále jen "držitel archiválie"),*
- e) využívání archiválií,*
- f) zpracování osobních údajů pro účely archivnictví,*
- g) soustavu archivů,*
- h) práva a povinnosti zřizovatelů archivů,*
- i) spisovou službu,*
- j) působnost Ministerstva vnitra (dále jen "ministerstvo") a dalších správních úřadů na úseku archivnictví a výkonu spisové služby,*
- k) správní delikty. " [17]*

### **2.3 Zákon č. 227/2000 Sb., o elektronickém podpisu**

Cílem zákona je usnadnění právních úkonů při použití digitálního podpisu jako ekvivalent k vlastnoručnímu podpisu. Zajišťuje uživatelům stejné možnosti, jako těm, co používají dokumenty v analogové podobě. Tento zákon tedy posouvá digitální dokument na stejnou úroveň jako je dokument v listinné podobě. I když každá datová schránka má své ID což do jisté míry nahrazuje klasický podpis, často datová schránka patří pod firmu, kde ji spravuje více lidí a při odeslání dokumentu nemusí být jednoznačné, kdo zprávu odeslal. Proto je zákon o elektronickém podpisu významnou součástí datových schránek. Upravuje používání elektronického podpisu, elektronické značky a poskytování certifikačních služeb. Také umožňuje zjistit, pokud dojde k porušení zprávy a to od okamžiku, kdy byla podepsána nebo označena, toto porušení bude možno zjistit. Tento zákon také určuje, že pokud je dokument podepsaný zaručeným elektronickým podpisem, vlastník podpisu se nemůže vzdát odpovědnosti za vznik tohoto dokumentu. Tento zákon nabyl platnosti dne 26. července 2000. [18]

#### **Účel zákona (§ 1)**

*„Tento zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.“ [18]*

## 2.4 zákon č. 365/2000 Sb., o informačních systémech veřejné správy

Zákon určuje práva a povinnosti, které souvisejí s užíváním, provozem a vytvářením informačních systémů veřejné správy. ISVS jsou informační systémy, sloužící pro výkon veřejné správy. Do informačního systému veřejné správy spadá také ISDS. Provozovatel a správce informačního systému datových schránek (ministerstva, jiné správní úřady a územní samosprávné celky) se tedy musí také řídit tímto zákonem. Tento zákon také upravuje podmínky dodávání datových zpráv orgánům veřejné moci prostřednictvím portálu veřejné správy. Tímto zákonem se rozumí tedy správa informačních činností a informačních systémů. Dále je zde popsáno, jak zacházet s informací, tedy jejich poskytováním, shromažďováním, získáváním, šířením, atd. Důležitou součástí tohoto zákona je také stanovení postavení Ministerstva vnitra, které pracuje s informacemi, které jsou klíčovými pro rozvoj a vytváření ISVS. Ministerstvo zpracovává návrhy dokumentů, připravuje a koordinuje záměry pro budování a přetváření ISVS. Tento zákon nabyl platnosti dne 23. října 2000.

### Předmět úpravy (§ 1)

*„Tento zákon stanoví práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.“ [19]*

## 2.5 Stručné shrnutí

Zmíněné zákony jsou důležité v oblasti komunikace prostřednictvím datových schránek a je potřeba se jimi řídit. Tyto zákony upravuje Ministerstvo vnitra. Zákon č. 300/2008 sb., o elektronických úkonech a autorizované konverzi dokumentů, přímo popisuje používání datových schránek. Před jeho přijetím byly právnické osoby a orgány veřejné moci odkázáni pouze na osobní kontakt, nebo kontakt přes e-mail (v případě, že vlastnili zaručení elektronický podpis nebo značku). Proto si myslím, že přijetím tohoto zákona nastala jakási revoluce v elektronické komunikaci. Ostatní zákony specifikují oblasti související s datovými schránkami jako je ISDS, elektronický podpis a archivnictví dokumentů. Myslím si, že tyto zákony je také potřebné znát pro správné používání datové schránky. Další kapitola objasní správné zacházení s dokumenty a jejich souvislost s datovými schránkami.

### 3 VAZBA DATOVÝCH SCHRÁNEK A ELEKTRONICKÉHO SYSTÉMU SPISOVÉ SLUŽBY

#### 3.1 Definice elektronického systému spisové služby

Pojem spisová služba představuje soubor činností, které vedou ke správě dokumentů a to jak v listinné, tak i v elektronické podobě a není možné jejich smíšení. Systém spisové služby bych popsala i jako oběh písemností od přijetí spisu (dokumentu), přes jeho zpracování a odeslání až po jeho uložení – probíhá tedy po celou dobu jeho životního cyklu. Slouží k evidenci a zakládání písemností, které umožní snazší vyhledávání dokumentů, které byly založeny již dříve. Touto oblastí se musí alespoň v minimální míře zabývat každá firma.

Já se zde soustředím na spisovou službu v elektronické podobě. Elektronický systém spisové služby se tedy zabývá dokumenty, ať už se jedná o datovou zprávu, nebo datový soubor. V dnešní době nabízí spousta poskytovatelů elektronických spisových služeb propojení se systémem datových schránek. [13]

Elektronický oběh písemností znamená, že spis obíhá v organizaci v digitální podobě. U elektronického oběhu se jako podklad (vzor) používá oběh dokumentu v listinné podobě. Životní cyklus elektronického dokumentu začíná **vznikem elektronického dokumentu**. Ten vzniká napsáním, naskenováním nebo přímým vstupem z externího systému. Následuje **zařazení dokumentu** do systému pro správu dokumentů. V tomto kroku musí být přiřazeny atributy k dokumentům, které slouží k jejich identifikaci. Dalším úkonem je **zpracování dokumentu**. Zpracování dokumentu zajišťuje doručení příslušné osobě, jejich odeslání nebo schválení do dalších procesů. Zřídka kdy zpracování dokument končí uložením do datového úložiště. Nakonec přichází na řadu **archivace dokumentu**, která znamená pouze označení vybraných dokumentů jako archivovaných nebo přesun dokumentu do jiné složky. [15]

##### 3.1.1 Elektronická podatelna

Elektronická podatelna, nebo také e-podatelna je určena k přijímání a odesílání elektronické pošty z, nebo do úřadu. Doručená i odeslaná datová zpráva musí obsahovat elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále „uznávaný e-podpis“), nebo kvalifikovaný systémový certifikát a elektronická značka založená na tomto certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále „uznávaná e-značka“). E-podatelna umožňuje připojení prostřednictvím internetu na poštovní server e-podatelny, kde je možné si stáhnout, uložit a evidovat



doručenou elektronickou poštou. Je tedy nutné, aby e-podatelná disponovala odpovídajícím technickým a programovým vybavením. Nakládání s elektronickou poštou musí být definováno ve spisovém a skartačním řádu, který upravuje postupy pro práci s elektronickými dokumenty. Tento řád by měl popisovat, které písemnosti jsou písemnostmi úřadu a které nikoliv. Je tedy zřejmé, že soukromá pošta, reklamní sdělení nebo komunikace mezi zaměstnanci nebudou patřit mezi písemnosti určené úřadu. Dále tento řád dává elektronické poště stejnou důležitost jako poště v listinné podobě, a mělo by se s ní zacházet se stejnou obezřetností. Je možné, aby úřad zřídil více e-podatelen, při čemž na každou z nich budou chodit zprávy předem určeného obsahu. Odesílatel však není povinen odeslat datovou zprávu na e-podatelnu určenou pro příjem zpráv určitého obsahu. Jakmile zpráva dojde do e-podatelny s libovolným předem určeným obsahem, považuje se za doručenou. Proto dle mého názoru není pro úřady výhodné mít více e-podatelen. [14], [1]

### **3.1.2 Životní cyklus datové zprávy**

V této podkapitole se budu zabývat životním cyklem datové zprávy. Chtěla bych zdůraznit, že je rozdíl mezi životním cyklem datové zprávy a elektronického dokumentu. Tok elektronického dokumentu se zabývá postupem elektronického dokumentu obecně, který se může, ale nemusí být datovou zprávou. Datová zpráva je již vytvořeným elektronickým dokumentem, který má svůj účel jako elektronická pošta. Elektronický dokument se tedy stává datovou zprávou v případě, je-li zaslán prostřednictvím datové schránky popřípadě elektronické podatelny.

#### **3.1.2.1 Doručená datová zpráva**

Před tím, než e-podatelná přijme nějaký dokument, je nutné ověřit, zda zpráva neobsahuje vir. V takovém případě by se zpráva považovala za nedoručenou. Nakažené zprávy by měly být uloženy například do antivirových trezorů, aby bylo možné se k nim případně vrátit při vyskytnutí nějakého problému.

Je nutné, aby byl zaznamenán přesný čas doručení s přesností na sekundy (může se lišit od času, kdy byla zpráva poprvé otevřena). V okamžiku kdy je zpráva ověřena a doručena e-podatelně je oficiálně přijata a je možné s ní dále nakládat.

Datová zpráva se ukládá společně s e-podpisem nebo e-značkou. Úložiště datových zpráv musí být bezpečné, tedy aby se předcházelo ztrátě a neoprávněnému pozměnění dokumentů a přístup do tohoto úložiště by měli mít určení pracovníci.

Evidence může být v elektronické i v listinné podobě, ale je výhodné, aby byl v elektronické podobě. Následně je zpráva opatřena identifikátorem e-podatelný (obdoba podacího razítka), který má za úkol evidovat informace o dané zprávě pro další řízení. Identifikátor by měl zejména obsahovat výsledek ověření e-podpisu, popřípadě časového razítka a přesný čas doručení.

Pokud je možné zjistit z doručené zprávy elektronickou adresu odesílatele, e-podatelná musí potvrdit doručení datové zprávy zasláním zprávy o doručení. Tato zpráva by měla obsahovat datum a čas doručení zprávy, charakteristiku doručené zprávy. Dále by toto potvrzení mělo být opatřeno e-podpisem nebo e-značkou.

Následně e-podatelná musí zjistit a zaznamenat náležitosti doručených zpráv, především vlastnosti e-podpisu. Dále zjišťuje, jestli datová zpráva odpovídá technickým parametrům stanoveným úřadem, zda je připojen uznávaný e-podpis nebo uznávaná e-značka, a jestli jejich certifikát nebyl zneplatněn.

Pokud proběhl výše uvedený postup, e-podatelná datovou zprávu příslušným útvarům úřadu k vyřízení. [14]

#### **3.1.2.2 Odeslaná datová zpráva**

Každá datová zpráva, která je odeslána z úřadu, se ukládá současně do úložiště v e-podatelně ve tvaru, ve kterém byla odeslána. Pokud je ke zprávě připojen uznávaný e-podpis a jeho kvalifikovaný certifikát nebo uznávaná e-značka a její kvalifikovaný e-certifikát, ukládají se společně se zprávou. Datovou zprávu může svým e-podpisem podepsat pouze zaměstnanec, který je k tomu oprávněn. Dále prochází datová zpráva před odesláním kontrolou, zda neobsahuje škodlivý kód. Nakonec musí být zaznamenán přesný čas odeslání s přesností na sekundy. [14]

### **3.2 Standard pro komunikaci mezi Informačním systémem datových schránek a spisovými službami**

Za účelem stanovit jednotný standard komunikace mezi spisovými službami a datovými schránkami, připravilo Ministerstvo vnitra ČR ve spolupráci s vybranými dodavateli spisových služeb dokument „Návrh funkcí WS pro komunikaci mezi ISDS a SS“. V tomto dokumentu jsou rozděleny funkce do šesti skupin.

#### **Podání zprávy**

Pokud chce subjekt poslat zprávu jinému subjektu, který vlastní datovou schránku, musí být nejprve zjištěna existence aktivní datové schránky druhého subjektu.

Pokud se data předávají od spisové služby do ISDS (žádost), zpráva musí obsahovat:

- popisné objekty a jejich vlastnosti dokumentu nebo spisu (identifikace, název, popis, evidenční údaje, datum a čas vytvoření, klasifikační údaje, poznámka, zmocnění),
- logické uspořádání (pořadí, datum a čas vytvoření, popis vazby),
- související subjekty (vztah k dokumentu, informace od subjektu, obchodní název, IČ, jméno a příjmení, typ, oslovení, titul před a za, funkce – útvar, adresy).

Pokud se data předávají od ISDS do spisové služby (odpověď) obálka zprávy musí obsahovat:

- podací číslo zprávy,
- identifikátor datové schránky odesílatele,
- identifikátor datové schránky adresáta,
- typ zprávy,
- časové razítko (doručeno, vyzvednuto, smazáno),
- hash (převod vstupních dat do malého čísla - kódování),
- zmocnění.

Pokud chce subjekt seznam nevyzvednutých zpráv (dosud nestažené), ISDS mu zobrazí obálky těchto zpráv. V případě, že chce subjekt číst celý obsah došlé zprávy, určí totožnost podle seznamu zjištěného předchozí funkcí (seznam nevyzvednutých zpráv). Tato funkce však nesmí měnit stav zprávy na „vyzvednuto“. Pokud však subjekt požaduje nastavení zprávy na „vyzvednuto“, musí být potvrzeno úspěšného vyzvednutí zprávy spisovou službou.

### **Doručenky**

Doručenky jsou charakterizovány jako dotaz na stav zprávy, tedy zda byla přijata druhým subjektem. Doručeny jsou doručovány do datové schránky jako standardní zprávy, s označením v poli, typ zprávy v obálce zprávy. Ze spisové služby do ISDS bude odeslán identifikátor zprávy. Odpověď od ISDS přichází stejná obálka jako při podání jen doplněná o další

časová razítka. Dodejka bude odeslána v okamžiku, kdy se druhý subjekt přihlásí do ISDS, nebo po uplynutí deseti dnů od doručení.

### **Dotaz na existenci datové schránky**

Jedná se tedy o vyhledávání datové schránky. V případě, že chce spisová služba provést odeslání zprávy prostřednictvím datové schránky, musí ověřit číslo datové schránky adresáta. Tato funkce zajišťuje:

- zjištění čísla datové schránky subjektu,
- ověření aktivní DS a vazebných údajů,
- zjištění, komu patří DS.

Žádost od spisové služby by měla obsahovat identifikaci datové schránky a identifikaci subjektu. Odpověď od ISDS by měla obsahovat seznam možných aktivních datových schránek odpovídající požadavku včetně charakteristiky ve stejném rozsahu jako u žádosti (identifikaci datové schránky a identifikaci subjektu).

### **Ověření zprávy**

Žádost musí obsahovat identifikátor zprávy a celé tělo zprávy jako při podání. V odpovědi by měl být „hash“ nebo celá obálka zprávy, informace že zpráva existuje, nebo informace, že hash neodpovídá uloženému.

### **Autentizační funkce**

Autentizační funkce jsou přihlášení (otevření komunikace), pomocí ověřovacích údajů, a odhlášení (ukončení komunikace).

### **Doplňkové a provozní funkce**

Mezi doplňkové provozní funkce mohou patřit dotazy na obsah celých front (odeslané a doručené zprávy) a funkce pro získání historie (provozní údaje, doručování, odesílání, smazání atd.). [23]

## **3.3 Konverze dokumentů**

Konverze dokumentů se dá popsat jako převedení dokumentu z digitální do listinné podoby nebo naopak. Dále se konverze dokumentů dělí na autorizovanou a neautorizovanou. Liší se od sebe tím, že autorizovaná konverze je navíc ověřená shodou těchto dokumentů a má při-

pojené ověřovací doložky. K tomu, aby se dokument mohl považovat za oficiální a tím pádem mohl být použit jako datová zpráva pro komunikaci s úřady, je potřeba, aby prošel autorizovanou konverzí. Z toho důvodu se v této kapitole budu zabývat autorizovanou konverzí dokumentů. [1],[2]

Dokument, který vznikl po jeho konverzi, má stejné právní účinky jako originální dokument. Zavedení autorizované konverze dokumentů umožňuje širší využívání elektronické komunikace a také napomáhá zrovnoprávnění digitální komunikace s úřady. Konverze však nepotvrzuje správnost a pravdivost dokumentů. Dále se autorizovaná konverze dokumentů dělí na prováděné „z moci úřední“ a „na žádost“. Autorizovanou konverzi dokumentů z moci úřední mohou provádět orgány veřejné moci pro výkon své působnosti (§23 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů). Autorizovanou konverzi na žádost provádějí především kontaktní místa veřejné správy (například notáři, krajské úřady, matriční úřady, obecní úřady, úřady městských částí). [1], [2]

### 3.3.1 Konverze z listinné do elektronické podoby

Listinný dokument, který má být konvertován, zákazník přinese příslušný úřad nebo orgán a zvolí formu výstupu. Je možné si vybrat mezi CD/DVD nebo zasláním do úložiště konvertovaných dokumentů, kde si jej musí nejpozději do tří dnů vyzvednout. Konverze do elektronického dokumentu se provádí pomocí snímacího zařízení (skeneru). Minimální parametry skeneru jsou stanoveny tak, aby byla autorizovaná konverze dostatečně kvalitní. Vstup v listinné podobě, nesmí být ve stavu, ve kterém by mohl poškodit skener. [1]

Při konverzi do elektronického dokumentu subjekt provádějící konverzi opatří výstup svou uznávanou e-značkou, nebo uznávaným e-podpisem a zajistí, aby byl výstup opatřen kvalifikovaným časovým razítkem. [2]

#### **Ověřovací doložka z listinné do elektronické podoby obsahuje následující údaje:**

- název subjektu, který konverzi provedl,
- pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí (úložiště ověřovacích doložek),
- údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,
- údaj o tom, z kolika listů se skládá vstup,

- údaj o tom, zda vstup obsahu vodoznak, reliéfní tisk nebo embossing, suchou pečeť nebo reliéfní ražbu, opticky variabilní prvek nebo jiný zajišťovací prvek,
- datum vyhotovení ověřovací doložky,
- jméno, případně jména, a příjmení osoby, která konverzi provedla. [16]

### 3.3.2 Konverze z elektronické do listinné podoby

Elektronický dokument, který má být konvertován, je možné přenést na CD/DVD nosič, nebo jej lze zaslat z datové schránky do elektronického uložení pro autorizované konverze dokumentů. V tomto případě je třeba, aby s sebou zákazník při vyzvednutí konvertovaného výstupu, přinesl potvrzení o vložení dokumentu do datového uložení. Při tomto druhu autorizované konverze je potřeba tiskárny splňující technické náležitosti, jako je například rozlišení tisku nejméně 300 dpi, barevný tisk, velikost formátu nejméně A4. Počítačový software, sloužící k identifikaci a odstraňování virů a jiných škodlivých kódů, provádí kontrolu, zda vstupní dokument je v pořádku. Soubor by měl být ve formátu PDF a může obsahovat text i obrázek. [1], [2]

Jakmile subjekt, provádějící konverzi, obdrží dokument, který má být konvertován, ověří platnost kvalifikovaného časového razítka (je-li jím vstup opatřen), platnost e-podpisu nebo platnost uznávané elektronické značky a ověření, zda kvalifikovaný certifikát, na němž je založen e-podpis, nebo kvalifikovaný systémový certifikát, na němž je založena e-značka, nebyly zneplatněny před okamžikem uvedeným v kvalifikovaném časovém razítku. [2]

**Ověřovací doložka z elektronické do listinné podoby obsahuje následující údaje:**

- název subjektu, který konverzi provedl,
- pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí (úložiště ověřovacích doložek),
- údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,
- údaj o tom, z kolika listů se skládá vstup,
- datum vyhotovení ověřovací doložky,
- údaj o tom, zda byl vstup podepsán platným uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou, číslo kvalifikovaného certifikátu, na němž je uznávaný elektronický podpis založen, nebo číslo kvalifikovaného systémového certifikátu, na němž je uznávaná elektronická značka založena, a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydal,

- datum a čas uvedené v kvalifikovaném časovém razítku, číslo kvalifikovaného časového razítka a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal, byl-li vstup kvalifikovaným časovým razítkem opatřen,
- otisk úředního razítka, jméno, případně jména, příjmení a podpis osoby, která konverzi provedla. [16]

### 3.3.3 Důvody znemožňující autorizovanou konverzi dokumentů

Konverzi dokumentů není možné provádět podle §24 odst. 5 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů převážně u dokumentů v listinné podobě, které jsou jedinečné, a není možné je nahradit konverzí. Jedná se zejména o:

- občanské průkazy,
- řidičské průkazy,
- cestovní pasy,
- zbrojní průkazy,
- vojenské knížky,
- rybářské lístky,
- průkaz o povolení pobytu cizince,
- lovecký lístek nebo jin průkazy,
- losy,
- sázenky,
- šeky,
- vkladní knížky,
- směnky a jiné cenné papíry,
- rysy a technické kresby.

Dále autorizovanou konverzi není možné provést v případě, že dokument v listinné podobě plastickým textem nebo otiskem plastického razítka. Je to proto, že text nebo otisk razítka, který dosahuje trojrozměrných hodnot, není možné převést do digitální podoby a listina by tedy ztratila svou autentičnost.

Jedním z důvodů, proč také nelze provádět autorizovanou konverzi je, že dokument nesplňuje technické podmínky.

Další podmínkou pro provádění autorizovaných konverzí (na žádost) je, že vstupující dokument v elektronické podobě musí mít obsažen uznávaný e-podpis nebo uznávanou e-značkou autora dokumentu.

Jedná-li se o dokument, který je obsažen v datové zprávě, například audio nebo video záznam, také není možné konvertovat. [2]

### **3.4 Stručné shrnutí**

Zprávy přijaté na datovou schránku se většinou ukládají v digitální podobě. Spisová služba je dnes ve většině případů již elektronická, jelikož její evidence a archivace je jednodušší jak u listinné spisové služby. Spisová služba se dá popsat i jako životní cyklus spisu. Zde byl spis chápán jako přijatá nebo odeslaná datová zpráva. S tím souvisí i autorizovaná konverze, kterou je nutno provádět v případech, když je potřeba převést elektronický dokument na listinný nebo naopak. Autorizovaná konverze má jisté náležitosti, které je nutné dodržet, aby byl dokument právoplatný. V další kapitole budou rozebrány nedostatky datových schránek, jejich případné odstranění a budoucnost datových schránek.



## **II. PRAKTICKÁ ČÁST**

## **4 PROBLEMATIKA DATOVÝCH SCHRÁNEK**

### **4.1 Cíl výzkumu**

Praktická část bakalářské práce obsahuje i dotazníkové šetření a je zaměřen zejména na podnikající fyzické osoby a právnické osoby, které mají od roku 2009 ze zákona povinnost mít zřízenou datovou schránku pro právnické osoby. Je tedy zřejmé, že ne všem může takhle forma komunikace s úřady vyhovovat. Úkolem dotazníku bylo především zjistit spokojenost uživatelů datových schránek v poměru s klasickou poštou, a jaké jsou podle nich největší problémy datových schránek. Dále se tento dotazník zkoumal, na jaké uživatelské úrovni jsou uživatelé seznámeni s možnostmi a prostředím datových schránek a do jaké míry je využívají.

### **4.2 Použitá metoda výzkumu**

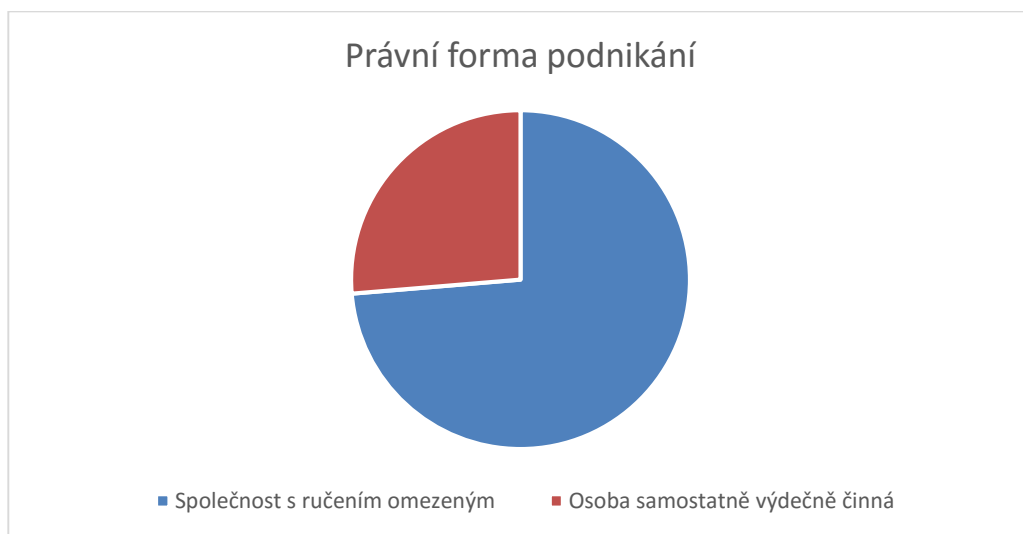
Dotazník jsem vytvořila na webových stránkách, které jsou přímo určeny pro vytváření průzkumů - [www.vyplnto.cz](http://www.vyplnto.cz). Je zde na výběr široká škála formulace otázek a také jednoduché uživatelské rozhraní. Respondenty jsem si vybrala z [www.firmy.abc.cz](http://www.firmy.abc.cz), kde jsou firmy z celé České republiky a oslovovala je prostřednictvím emailu. Celkem jsem oslovila přibližně 100 respondentů a z toho mi odpovědělo 38. Dotazník obsahoval celkem 15 otázek.

### **4.3 Vyhodnocení výsledků průzkumu**

#### **1. Otázka**

První otázka se týkala právní formy podnikání. Zjišťovala jsem, jestli jsou respondenti společnost s ručením omezeným nebo osoba samostatně výdělečně činná. Respondenti jsou tedy

z větší části (73,68%) společnost s ručením omezeným. Osoby samostatně výdělečně činné jsou v zastoupení 26,32%.



Obr. 10: Právní forma podnikání (zdroj: vlastní)

## 2. Otázka

Další otázka byla směřována na komunikaci prostřednictvím datových schránek, a jestli jsou s ní respondenti spokojeni. Většina uživatelů (76,32%) je s užíváním datových schránek spokojena. Nespokojena je 23,68%.



Obr. 11: Spokojenost s komunikací přes datové schránky (zdroj: vlastní)

Více spokojení s datovými schránkami jsou respondenti, kteří označili, že jsou společnost s ručením omezeným. 82,29% z nich označilo, že jsou spokojeni. Osoby samostatně výdělečně činné jsou spíše nespokojeny (60%).

Dle mého názoru jsou osoby samostatně výdělečně činné spíše nespokojeny, protože musí datovou schránku spravovat sami. Respondenti ze společností s ručením omezeným mohou pověřit více osob, které se starají o datovou schránku. Tím pádem pro ně není správa datové schránky tak obtížná.

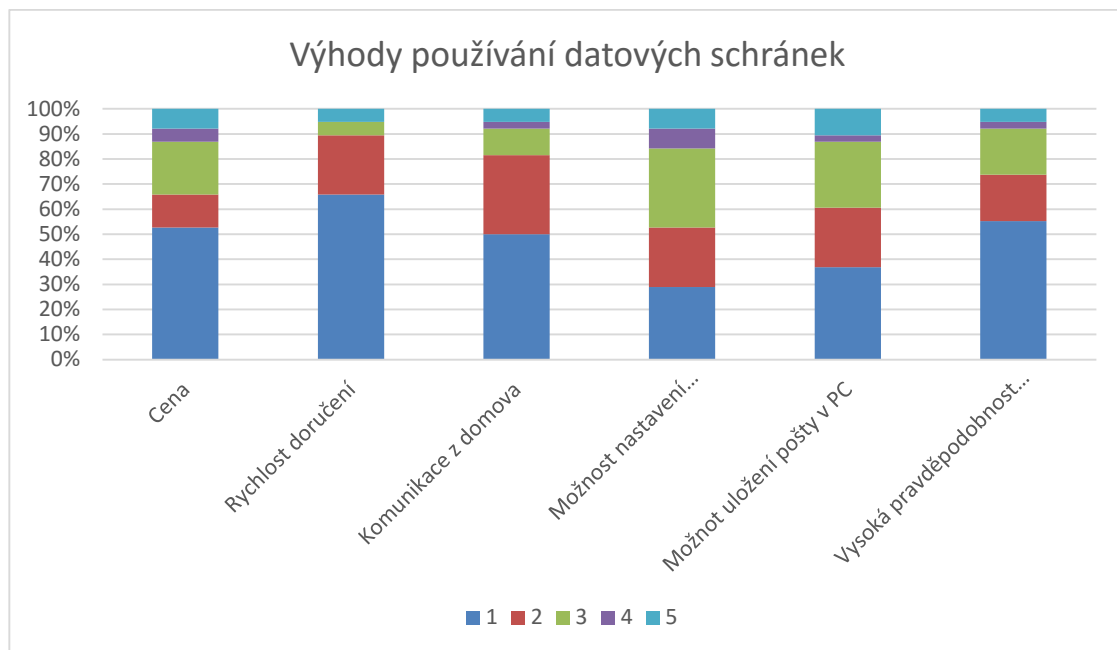
### 3. Otázka

Další otázka byla otevřená a respondenti se v ní měli vyjádřit, jaké problémy vnímají u datových schránek. **Patnáct** respondentů odpovědělo, že žádný problém nevnímají, nebo si ho neuvědomují. Zbytek odpovědí se lišil. Nejčastější popisovaný problém je automatické mazání zpráv po třech měsících. Na tento problém upozornilo celkem **šest** respondentů. **Čtyři** respondenti si stěžovali na uživatelské rozhraní a jeho složitost (zdlouhavé odesílání dokumentů, složité přihlašování, a změna hesla). Dalším zmíněným problémem je nutnost ověření pravosti dokumentu a konverze dokumentu do papírové podoby, který zmínili celkem **dva** respondenti. Neosobní jednání zmínili také **dva** respondenti. Další **dva** respondenti zmínili problém s komunikací s Finančním úřadem - problém s daňovým přiznáním (po vyplnění daňového přiznání přes datovou schránku nutnost jít na Finanční úřad a nelze přijmout zprávu od Finančního úřadu v případě chybného daňového přiznání). Ostatní odpovědi byly zmíněny pouze jednou. Patří mezi ně nedostačující bezpečnost, fikce doručení (když se uživatel nepřihlásí do datové schránky do deseti dnů, je zpráva považována za doručenou), problém s přístupovým heslem (automatická změna hesla), zpoplatněné upozorňovací emaily a SMS zprávy na došlé datové zprávy, problémy s rychlostí a přihlášením, při výběrových řízeních nejde přes datovou schránku podat právoplatnou nabídku a že přes jejich prostřednictvím nekomunikují všichni státní úředníci.

### 4. Otázka

U čtvrté otázky měli za úkol respondenti zhodnotit výhody používání datových schránek na škále od jedné do pěti (při čemž: jedna – nejvíce podstatná výhoda; pět – nejméně podstatná výhoda). Měli hodnotit tyto aspekty: Cena; Rychlost doručení; Komunikace z domova; Možnost nastavení datových stránek tak, aby se mohli do ní zasílat “Poštovní datové zprávy”, např. z bank nebo pojišťovny; Možnost uložení doručené pošty v PC; Vysoká pravděpodobnost doručení zprávy. S nejlepším průměrem 1,553 vyšla Rychlost doručení. Jako

druhá nejlepší výhoda s průměrem 1,816 byla zhodnocena Komunikace z domova. S třetím nejlepším průměrem 1,842 byla vyhodnocena Vysoká pravděpodobnost doručení zprávy. Následovala Cena s průměrem 2,026, Možnost nastavení datových stránek tak, aby se mohli do ní zasílat „Poštovní datové zprávy“ byla vyhodnocena s průměrem 2,421. Jako nejméně podstatné respondentům přišla Možnost uložení doručené pošty v PC s průměrem 2,263.



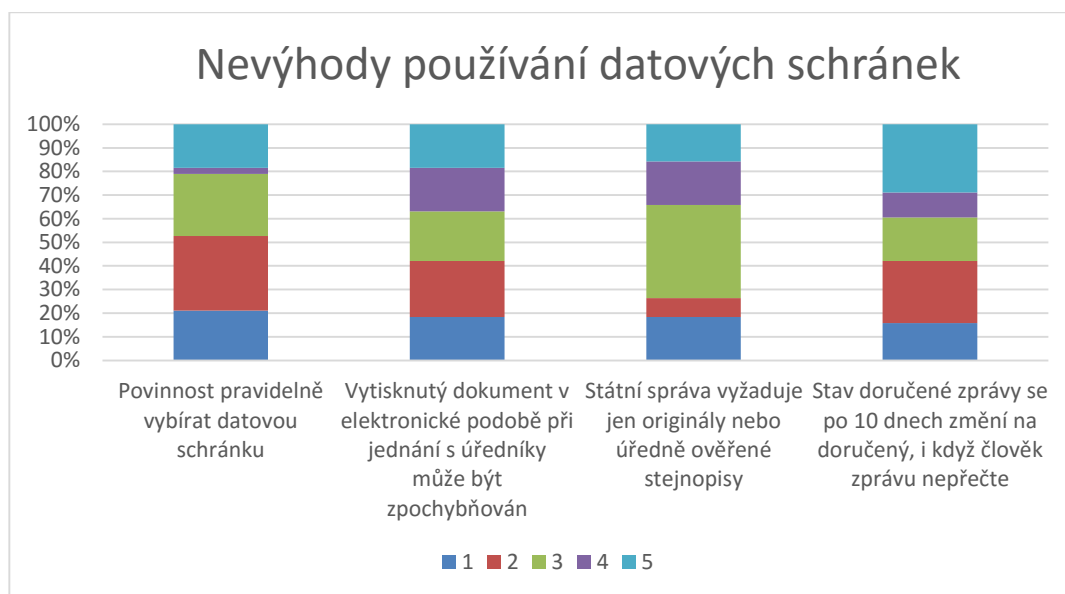
Obr. 12: Výhody používání datových schránek (zdroj: vlastní)

Nejlépe hodnocená odpověď – „Rychlost doručení“ byla zvolena dle mého názoru proto, že v dnešní uspěchané době lidé nemají čas na to, aby chodili po úřadech. Z toho důvodu byla druhý nejlépe hodnocený klad „Komunikace z domova“. Naopak nejméně důležitý klad – „Možnost nastavení datových schránek tak, aby se mohli do ní zasílat „Poštovní datové zprávy“, např. z bank nebo pojišťovny“, byl vyhodnocen proto, že většina uživatelů tuto službu nevyužívá a z bank a pojišťoven si nechávají zasílat zprávy na e-mail.

## 5. Otázka

Pátá otázka byla zkonstruovaná stejně jako čtvrtá otázka s tím rozdílem, že dotazovaní zde hodnotili nevýhody používání datových schránek pěti (při čemž: jedna – nejvíce podstatná nevýhoda; pět – nejméně podstatná nevýhoda). Měli hodnotit tyto aspekty: Povinnost pravidelně vybírat datovou schránku; Vytisknutý dokument v elektronické podobě při jednání s úředníky může být zpochybňován; Státní správa vyžaduje jen originály nebo úředně ověřené stejnopisy; Stav doručené zprávy se po 10 dnech změnil na doručený, i když člověk zprávu

nepřečte. Jako největší nevýhodu s průměrem 2,658 respondenti zhodnotili Povinnost pravidelně vybírat datovou schránku. Druhá největší nevýhoda s průměrem 2,947 byla vyhodnocena možnost - Vytisknutý dokument v elektronické podobě při jednání s úředníky může být zpochybňován. Možnost Státní správa vyžaduje jen originály nebo úředně ověřené stejnopisy, byla vyhodnocena s průměrem 3,053. Jako nejméně podstatná nevýhoda vyšel s průměrem 3,105 - Stav doručené zprávy se po 10 dnech změní na doručený, i když člověk zprávu nepřečte.

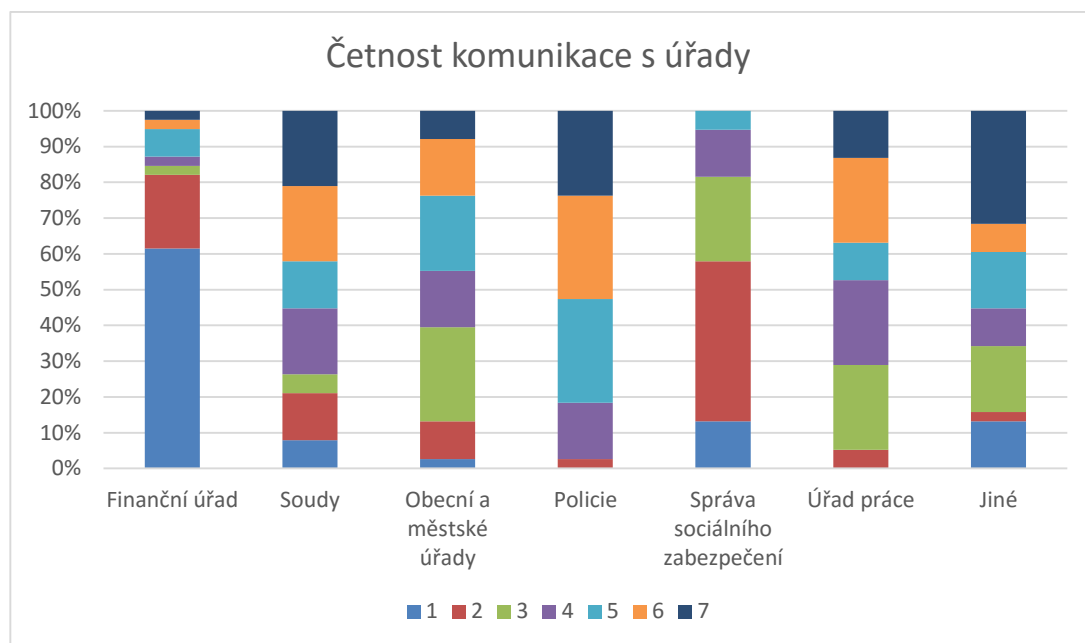


Obr. 13: Nevýhody používání datových schránek (zdroj: vlastní)

Jako největší nevýhoda „Povinnost pravidelně vybírat datovou schránku“ byla dle mého názoru vyhodnocena z toho důvodu, že uživatelé jsou nuceni se pravidelně přihlašovat do datové schránky, protože zprávy se po deseti dnech po doručení automaticky změní na přečtené. V případě, že uživatelům chodí upozornění na telefon nebo e-mail, není nutné, aby se pravidelně přihlašovali (stačí, když se přihlásí vždy, když přijde upozornění).

## 6. Otázka

Další otázka měla za úkol zjistit, se kterými státními orgány respondenti komunikují nejčastěji. Možnosti měli seřadit od nejčastější po nejméně častou možnost. Nejčastější komunikace probíhá s Finančním úřadem, poté se Správou sociálního zabezpečení. Jako třetí nejčastější možnost byly zvoleny Obecní a městské úřady. Pátá, šestá a sedmá nejčastější možnost měly stejné hodnoty a byly zvoleny Soudy a Úřady práce a jiné. Nejméně často respondenti komunikují s policií.

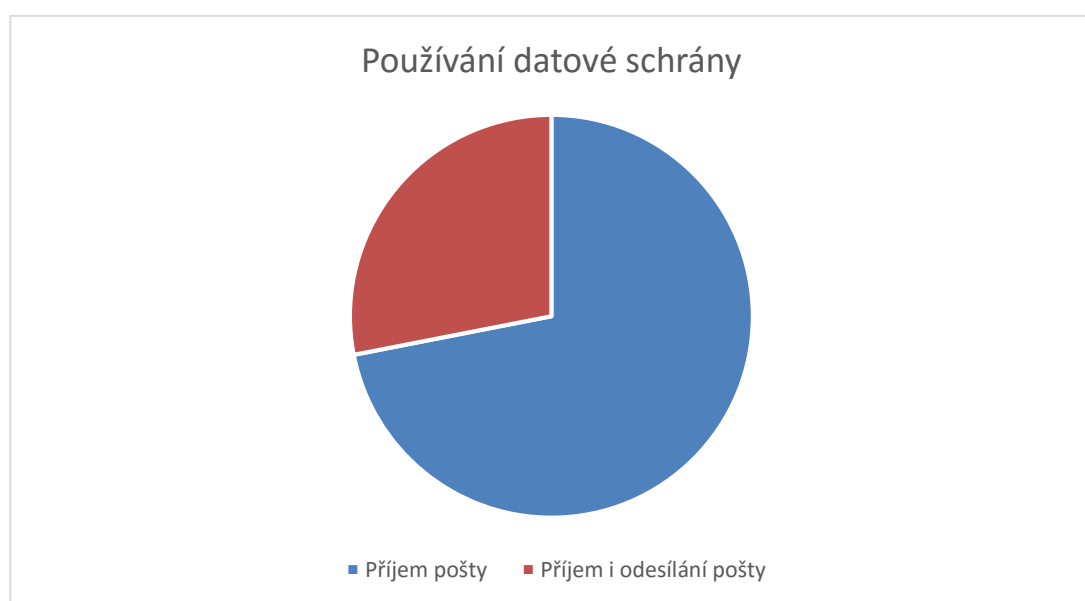


Obr. 14: Četnost komunikace s úřady (zdroj: vlastní)

Dle mého názoru uživatelé nejčastěji komunikují s Finančním úřadem proto, že vlastníci datových schránek musí podávat daňové přiznání prostřednictvím datových schránek.

## 7. Otázka

V sedmé otázce jsem zjišťovala, k jakým úkonům respondenti používají datové schránky. Tedy jestli pouze k příjmu pošty, nebo i k jejímu odesílání. Většina (78,95%) respondentů odpověděla, že datové schránky používají k příjmu i odesílání pošty. Zbytek (21,05%) pouze k příjmu pošty.

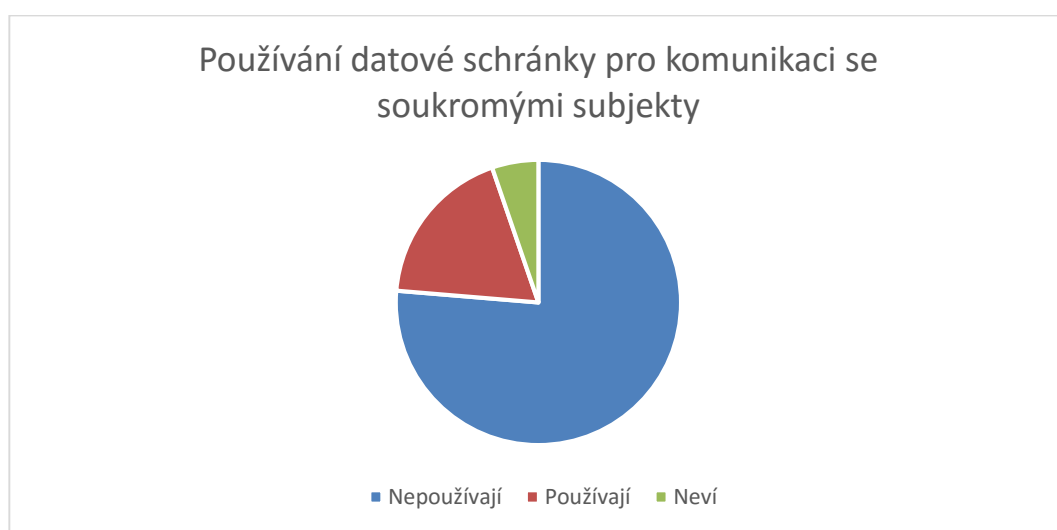


Obr. 15: Používání datové schránky (zdroj: vlastní)

Většina uživatelů používá datové schránky aktivně – tedy k příjmu i odesílání pošty. Pouze jedna čtvrtina používá datové schránky pasivně.

### 8. Otázka

U osmé otázky jsem se dotazovala, zda respondenti používají datové schránky pro komunikaci se soukromými subjekty (fyzické, podnikající fyzické a právnické osoby). Většina (76,32%) odpověděla, že se soukromými osobami přes datové schránky nekomunikuje. 18,42% dotazovaných odpovědělo, že komunikuje i se soukromými subjekty. Dále 5,26% respondentů odpovědělo, že neví, jestli komunikují i se soukromými subjekty.



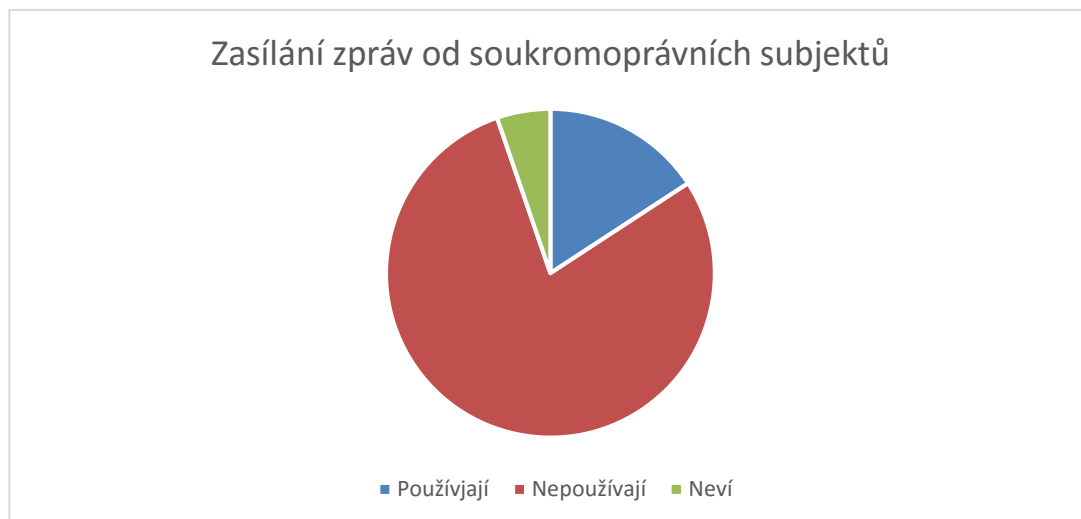
Obr. 16: Používání datové schránky pro komunikaci se soukromými subjekty (zdroj: vlastní)

Tři čtvrtě z dotazovaných nepoužívá datovou schránku k soukromým účelům. Myslím si, že je to pro uživatele zbytečně formální a složitá cesta komunikace. K těmto účelům je pro ně hodnější e-mail (nebo jiná forma komunikace).

### 9. Otázka

U deváté otázky byli respondenti dotazováni, zda si nechávají zasílat zprávy i od soukromoprávních subjektů? (banky pojišťovny, dodavatelé energií). 78,95% odpovědělo, že si nenechávají a 15,79% odpovědělo, že si nechávají zasílat zprávy od soukromoprávních subjektů. Zbytek (5,26%) odpověděl, že neví.



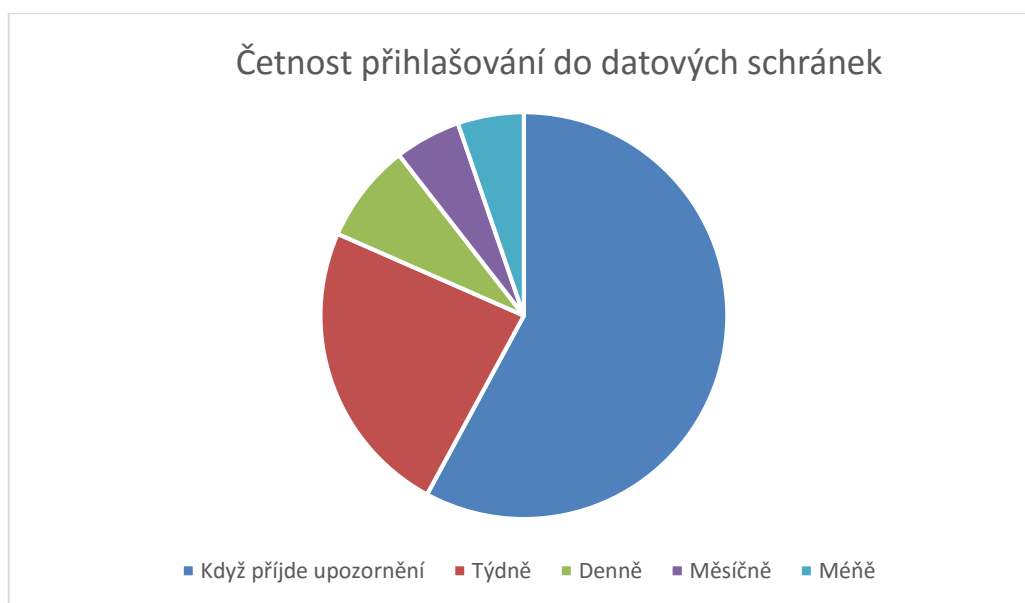


Obr. 17: Zasílání zpráv od soukromoprávních subjektů (zdroj: vlastní)

Důvodem, proč většina respondentů nepoužívá datové schránky pro komunikaci se soukromými subjekty je, že si veškeré zprávy nechávají zasílat na e-mail, který navštěvují častěji. Datové schránky tedy používají výhradně pro komunikaci s úřady.

### 10. Otázka

Další otázka se soustředila na to, jak často se respondenti přihlašují do datové schránky. 57,89% dotazovaných odpovědělo, že se přihlašují, když jim přijde upozornění na mobil nebo email. Druhá nejčastější odpověď s 23,68% bylo týdenní přihlašování. Denně se do datových schránek přihlašuje 7,89% respondentů. 5,26% nasbíraly odpovědi s měsíční a méně než měsíční četností přihlášení.

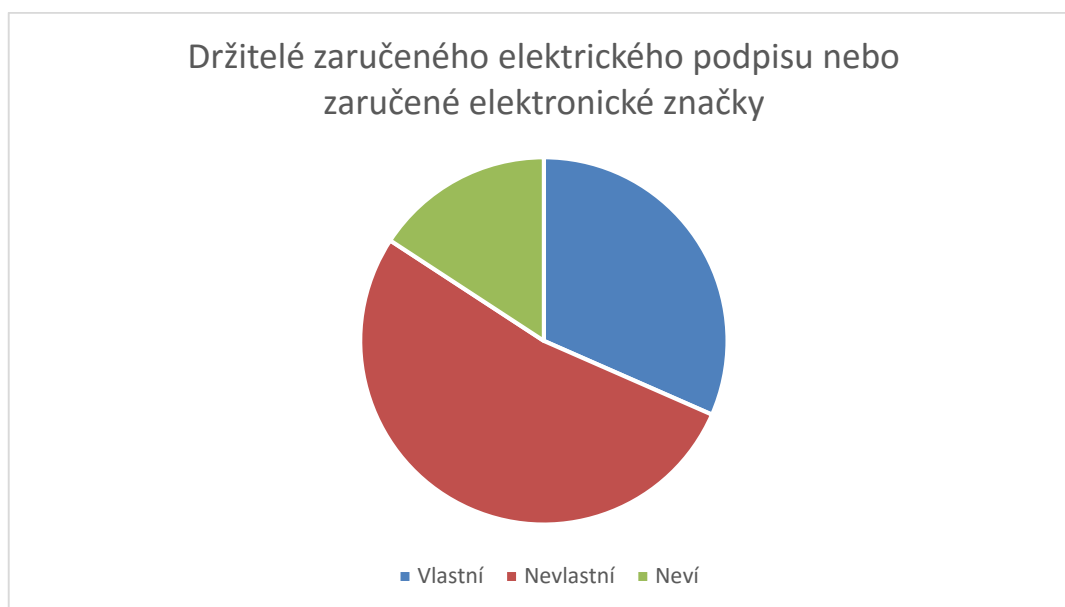


Obr. 18: Četnost přihlašování do datových schránek (zdroj: vlastní)

Více jak polovina respondentů uvedlo, že si nechává zasílat upozornění na e-mail nebo mobilní telefon. Myslím si, že je to proto, že uživatelé nemusí myslet na to, aby vybírali datovou schránku, ale zkrátka je na to upozorní SMS nebo e-mail. Dle mého názoru upozornění přes SMS je efektivnější, je však zpoplatněno.

### 11. Otázka

Jedenáctá otázka měla za úkol zjistit, zda respondenti vlastní zaručený elektronický podpis nebo zaručenou elektronickou značku. 52,63% tedy více jako polovina dotazujících ne vlastní zaručený elektronický podpis ani zaručeno elektronickou značku. 31,58% respondentů jsou vlastníky zaručeného elektronického podpisu nebo značky. 15,79% odpovědělo, že neví, zda vlastní zaručený elektronický podpis nebo zaručeno elektronickou značku.

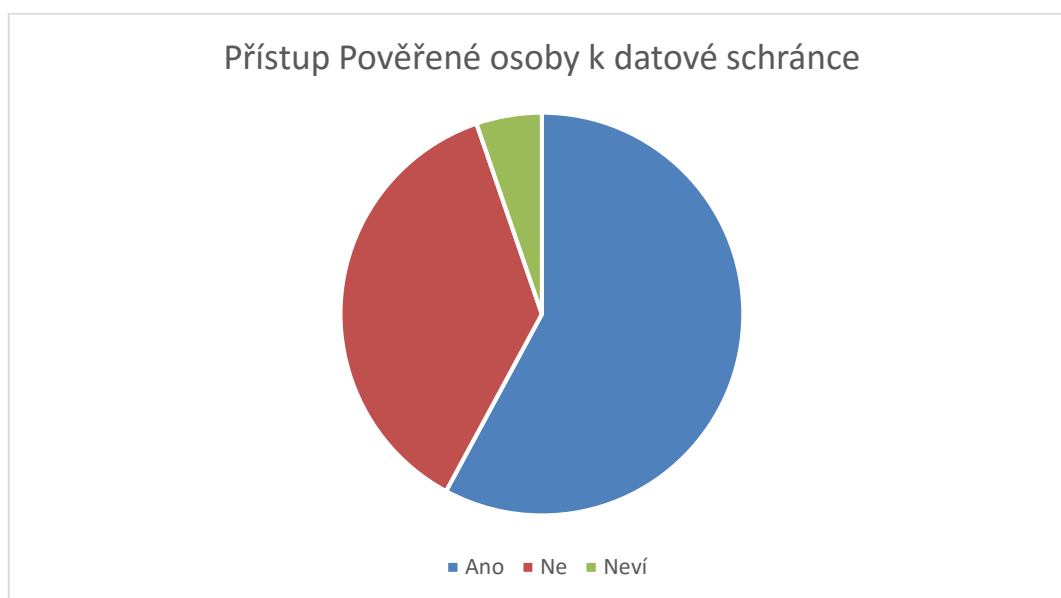


Obr. 19: Držitelé zaručeného elektrického podpisu nebo zaručené elektronické značky (zdroj: vlastní)

Mezi respondenty nebyla žádná osoba samostatně výdělečně činná, která by vlastnila zaručený elektronický podpis nebo značku. Respondenti, kteří označili, že jsou vlastníci zaručeného elektronického podpisu nebo značky, byli pouze ze společností s ručením omezeným. Dle mého názoru je důvodem to, že ke komunikaci prostřednictvím datových schránek není potřeba vlastnit zaručený elektronický podpis nebo značku. Pouze pokud jedná uživatel za sebe prostřednictvím firemní datové schránky, ke které má přístup více osob, je potřeba se identifikovat. Do datové schránky osoby samostatně výdělečně činné má většinou přístup jedna osoba, proto není nutné, aby vlastnili elektronický podpis nebo značku.

## 12. Otázka

Dvanáctá otázka zjišťovala, zda má k datové schránce přístup i Pověřená osoba. U více jak poloviny (57,89%) respondentů odpovědělo, že k jejich datové schránce má přístup Pověřená osoba. Dále 36,84% z dotazovaných odpovědělo, že nemají Pověřenou osobu a 5,26% odpovědělo, že neví.



Obr. 20: Přístup Pověřené osoby k datové schránce (zdroj: vlastní)

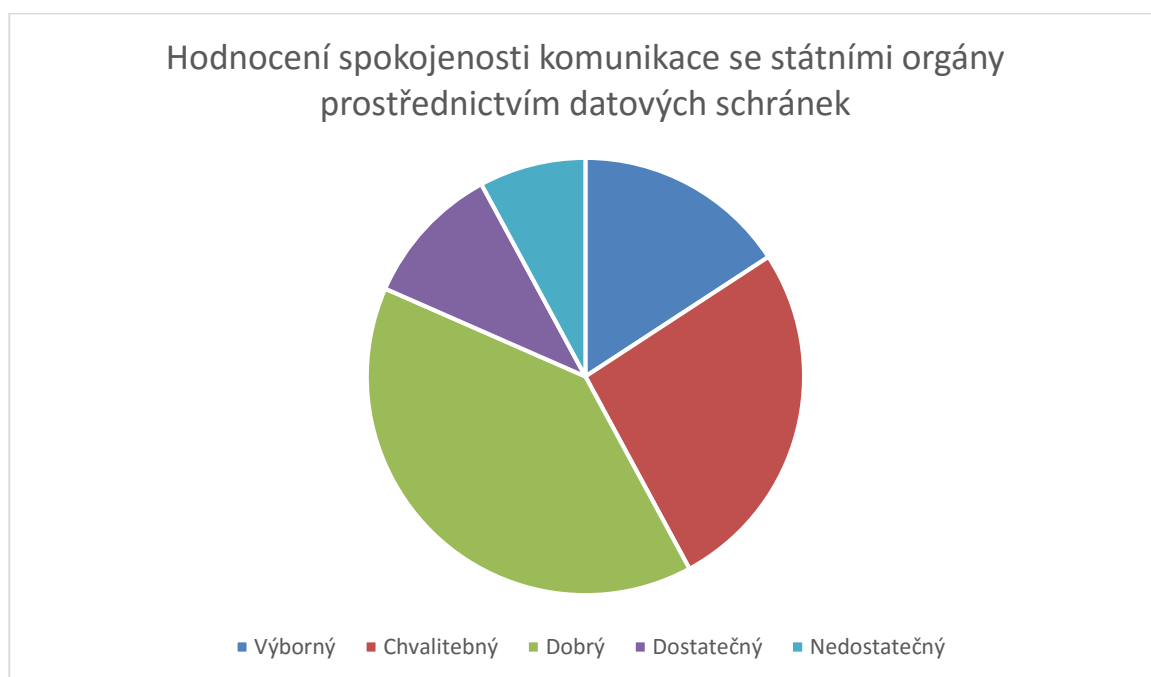
Přístup Pověřené osoby používají výhradně společnosti s ručením omezeným. Dle mého názoru je to dáno tím, že podnikání osoby samostatně výdělečně činné stojí na jedné osobě, která zároveň vlastní datovou schránku. Kdyžto u společnosti s ručením omezeným může mít několik řídících osob (jednatelů).

## 13. Otázka

Třináctá otázka byla otevřená a respondent musel napsat odpověď vlastními slovy. Měli se vyjádřit k tomu, jaké změny by si v budoucnu přáli, aby nastaly u datových schránek. **Dvacet** respondentů odpovědělo, že by nic neměnilo. Dále **Čtyři** respondenti uvedli, že by jim vyhovovalo, kdyby nebyly datové schránky ze zákona povinné (právnícké osoby). **Tři** z dotazovaných by uvítali, kdyby byl dokument zaslaný přes datovou schránku plnohodnotný bez dalšího ověřování. Další tři z dotazovaných reagovali na problém s ukládáním přijatých zpráv (bezplatná služba ukládání pošty, nebo prodloužení úložné doby na šest měsíců). **Dva** respondenti zmínili, modernizaci a zjednodušení prostředí datových schránek. Ostatní odpovědi byly zmíněny pouze jednou. Mezi ně patří „možnost připojit krátkou průvodní zprávu“, „neměnit přístupová hesla“, „všechny upozornění na email“ a „zrušit fikci doručení“.

#### 14. Otázka

Čtrnáctá otázka zjišťovala, jak jsou respondenti spokojeni s komunikací se státními orgány prostřednictvím datových schránek. Dotazovaný se musel rozhodnout mezi odpověďmi „výborný“, „chvalitebný“, „dobrý“, „dostatečný“ a „nedostatečný“. Nejvíce (39,47%) respondentů hlasovalo, že je komunikace se státními orgány „dobrá“. Druhá nejčastější zvolená odpověď s 26,32% bylo „chvalitebný“. 15,79% si myslí, že komunikace je na výborné úrovni. 10,53% odpovědělo, že komunikace je „dostatečná“ a 7,89% odpovědělo, že je nedostatečná.

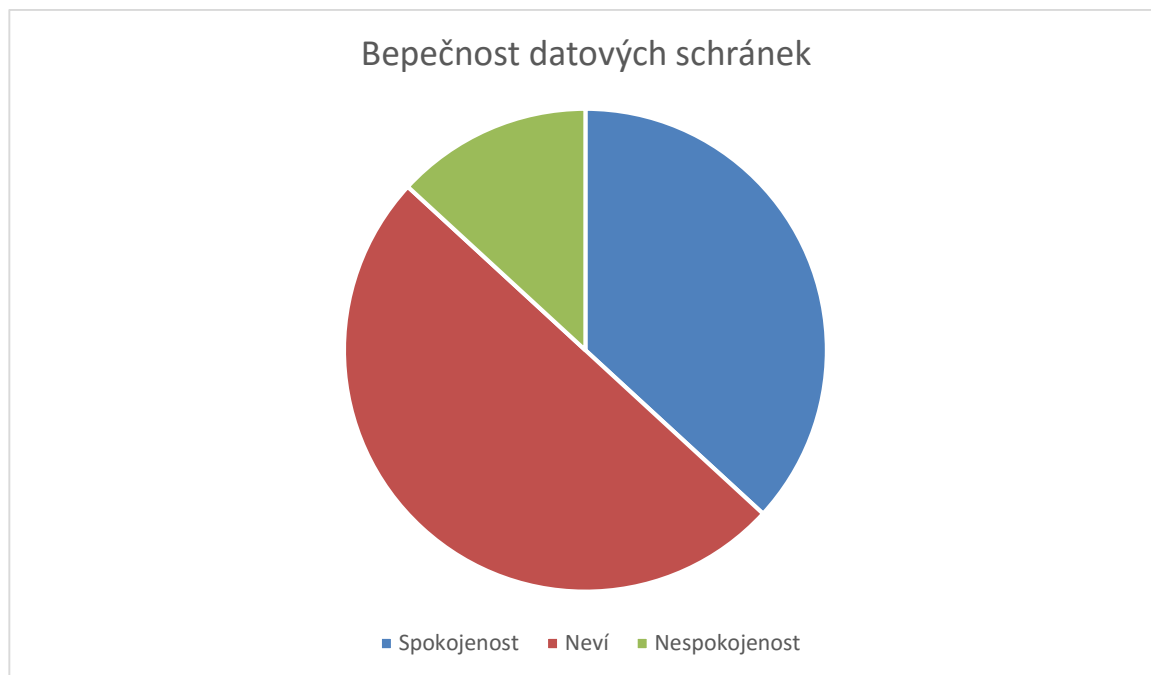


Obr. 21: Hodnocení spokojenosti komunikace se státními orgány prostřednictvím datových schránek (zdroj: vlastní)

Průměrná („dobrá“) spokojenost je dána tím, že některé úřady nekomunikují prostřednictvím datových schránek přesto, že by měli (viz. 3. otázka). Dále jak bylo řečeno u šesté otázky, většinou komunikace probíhá s Finančním úřadem, takže si myslím, že hodně uživatelů vidí problém hlavně tam (daňové přiznání, atd.).

#### 15. Otázka

Patnáctá a taky poslední otázka byla zaměřena na bezpečnost datových schránek. 50% respondentů uvedlo, že neví na jaké úrovni je bezpečnost u datových schránek. Dále 36,84% si myslí, že je bezpečnost dostatečná a 13,16% si myslí, že dostatečná není.



Obr. 22: Bepečnost datových schránek (zdroj: vlastní)

Řekla bych, že spokojenost se zabezpečením je průměrná. Jak bylo řečeno u třetí a třinácté otázky, někteří respondenti vidí problém s přihlášením, což myslím, že je největší problém s bezpečností.

#### 4.3.1 Shrnutí dotazníkového šetření

Odpovědi týkajících se datových schránek byly více méně kladné. Více jak tři čtvrtina respondentů je spokojená s používáním datových schránek. I přes jejich spokojenost si myslí, že je stále co zlepšovat. Nejvíce jim vadí automatické mazání přijatých zpráv po třech měsících, složitost pracovního prostředí datových schránek. Dále jako největší nevýhoda byla vyhodnocena „Povinnost pravidelně vybírat datovou schránku“, což v podstatě také souvisí s automatickým mazáním zpráv. Naopak jako největší kladná vlastnost vyšla rychlost doručení. S bezpečností u datových schránek je spokojeno pouze 36,8%, což je čtrnáct respondentů. Respondenti uvedli, že nejčastěji komunikují s Finančním úřadem. Celková komunikace s úřady jim však přijde pouze dostačující (průměrné hodnocení 3,87). U dotazu, co by dotazovaní změnili na datových schránkách, sedmnáct respondentů odpovědělo, že jim vyhovuje, vyhovuje aktuální stav datových schránek. Čtyři z dotazovaných však odpovědělo nejsou spokojeni s datovými schránkami, a že je používají pouze z nutnosti.

Dále jsem v tomto průzkumu zjistila, že většina respondentů používá pouze základní funkce datových schránek. Pro komunikaci se soukromými subjekty používá datovou schránku

pouze 18,4%. což je sedm respondentů. Od soukromoprávních subjektů, mezi které patří banky, pojišťovny a dodavatelé energií, si nechává zasílat pouze 6 respondentů. Upozornění na email nebo SMS při příchodu nové zprávy si nechává zasílat více jak polovina (dvacet dva respondentů). Zbytek se přihlašuje denně (tři respondenti), týdně (devět respondentů) a méně. Více jak polovina (20) respondentů nevlastní zaručený elektronický podpis ani zaručenou elektronickou značku. Většina dotazovaných (30) však používá datové schránky jak k příjmu, tak i k odesílání pošty. Více jak polovina (22) uvedla, že má k datové schránce přístup více uživatelů (Pověřené osoby).

**Nejčastěji zmiňované klady:**

- rychlost doručení,
- komunikace z domova,
- spolehlivost v doručování zpráv.

**Nejčastěji zmiňované nedostatky:**

- povinnost pravidelně vybírat datovou schránku,
- bez autorizované konverze není dokument plnoprávný,
- fikce doručení,
- nedostatečná komunikace s úřady,
- složitá správa datových schránek,
- bezpečnost datových schránek,
- tříměsíční doba archivace přijaté zprávy.

## 5 SPECIFIKUJTE TRENDY ROZVOJE DATOVÝCH SCHRÁNEK

### 5.1 Současné trendy

Datové schránky nejsou ve světě komunikace žádným nováčkem vzhledem k tomu, jak v dnešní době jde rozvoj informačních a komunikačních technologií rychle kupředu. Dnes je možné téměř vše zařídit z domova prostřednictvím internetu. Proto ani komunikace s úřady nezůstala pozadu a v roce 2008 eGovernment zavedl datové schránky, které jsou určeny především pro komunikaci mezi orgán veřejné moci a právníckými osobami. Má jít tedy o jakési zjednodušení komunikace mezi těmito subjekty. Postupně se komunikace přes datové schránky více rozšiřuje. Stále jsou schvalovány novelizace zákonů, které souvisejí s komunikací prostřednictvím datových schránek.

Česká pošta zavedla tzv. hybridní datovou zprávu (poštu). Je tedy možné už posílat přes datovou schránku dokumenty osobám, které nejsou vlastníky datových schránek. To by znamenalo, že vlastníci datových schránek by už vůbec nepoužívaly klasickou poštu.

Ministerstvo vnitra chce postupně všechny dokumenty zelektronizovat, což má za následek, že zavedlo podání daňového přiznání a ostatních důležitých tiskopisů prostřednictvím datové schránky. Pro držitele datové schránky je to povinné, jinak budou povinni zaplatit pokutu (2000 – 50000 Kč).

I přes většinovou spokojenost s datovými schránkami, je stále co vylepšovat. Dle mého názoru je možné, že v budoucnu bude postupně omezena listinná komunikace a nahrazena elektronickými dokumenty i u fyzických osob. Tomuto se však věnuje následující podkapitola.

### 5.2 Pohled do budoucna

Dle mého názoru můžeme v budoucnu očekávat následující změny:

- archivace doručených zpráv (alespoň na 6 měsíců), nebo bezplatná služba ukládání zpráv,
- design a ovladatelnost pracovního prostředí datových schránek,
- rovnoprávnost dokumentů zasílaných přes datové schránky (bez konverze),
- web optimalizovaný pro mobilní zařízení,
- omezení listinné komunikace,
- zlepšení autentizace,

- povinné zřizování datové schránky pro fyzické osoby.

### **Prodloužení archivace doručených zpráv, nebo bezplatná služba ukládání zpráv**

Jeden z nejčastěji zmiňovaných problémů v dotazníkovém šetření bylo, že se přijaté zprávy smažou po třech měsících. Uživatelé musí archivovat data vlastními silami, nebo používat aplikaci Datový trezor, která je ale zpoplatněna. Proto si myslím, že by uživatelé uvítali, kdyby se doba archivace zprávy prodloužila alespoň na šest měsíců. Další variantou řešení tohoto problému by byla služba, která by poskytovala bezplatné ukládání zpráv. Takle aplikace by mohla být i externího původu – tedy že by program vyvinula třetí strana. Dle informací, které mi poskytl Ing. Ondřej Menoušek – vedoucí oddělení informačních systémů, se nic takového neplánuje.

### **Design a ovladatelnost pracovního prostředí datových schránek**

Jak bylo zmíněno v dotazníku – některým respondentům se zdá, že správa datové schránky je poněkud složitá. Design je jedním z hlavních faktorů při používání webových stránek (nejen u datových schránek) a je důležité, aby byl srozumitelný pro všechny uživatele. Tento problém by mohl vyřešit zjednodušený a přehlednější design pracovního prostředí datových schránek.

### **Rovnoprávnost dokumentů zasílaných přes datové schránky (bez autorizované konverze)**

Aby byl přijatý dokument plnohodnotný, je potřeba provést autorizovanou konverzi, což se může někomu zdát zdlouhavé. Proto si myslím, že by bylo dobré vymyslet nějaký způsob, jak lze elektronický dokument konvertovat „z pohodlí domova“. Tento krok je však stále v nedohlednu, jelikož by nebylo možné zaručit, že před konverzí nebyl dokument upraven.

### **Web optimalizovaný pro mobilní zařízení**

V době chytrých telefonů a tabletů je možné, že s největší pravděpodobností, že za pár let bude možný přístup k datovým schránkám i přes mobilní rozhraní. V tomto případě by se uživatelé mohli připojit k datové schránce opravdu kdykoli a odkudkoliv. Pokud se tak stane, jeden z největších problémů by byla autentizace. Většina uživatelů mobilních zařízení se k internetu připojuje prostřednictvím veřejných Wi-Fi sítí, které nejsou zrovna bezpečné. Další otázkou by byl design pracovního prostředí datových schránek. Bylo by nutné, aby byl jednoduchý a přehledný, jelikož práce přes mobilní telefon neumožňuje takové možnosti jako práce přes počítač či notebook.



Dle mého názoru by mobilní rozhraní sloužilo především k přijímání zpráv. Psaní na mobilu nebo tabletu je složité, pomalé a snadno se udělá chyba, proto si myslím, že k psaní formálních zpráv není vhodné.

### **Omezení listinné komunikace**

Dle mého názoru je pravděpodobné, že v budoucnu se do jisté míry přestane používat komunikace v listinné podobě. Nahradí ji elektronická komunikace a to i u fyzických osob. Dnes se už nepoužívají ani klasické osobní dopisy, které byly nahrazeny komunikací přes e-mailly a sociální sítě. Proto je logické, že tento progres nastane i u komunikace s úřady. Fyzická osoba výhradně přijímá dopisy od úřadů a odesílá jen zřídka - bývá upřednostňován osobní kontakt (nejen fyzické osoby – viz. dotazníkové šetření). Z toho důvodu si myslím, že v některých případech by osobní forma komunikace měla být ponechána. Tahle vize je však stále v nedohlednu.

### **Zlepšení autentizace**

V dotazníku byla zmíněna nedostatečná bezpečnost datových schránek, se kterou může souviset právě identifikace (přihlášení) uživatele. Ing. Ondřej Menoušek mi poskytl informaci, že je v budoucnu plánovaná autentizace prostřednictvím elektronického občanského průkazu. V současné době však elektronický občanský průkaz není ze zákona povinné vlastnit, proto si myslím, že málo občanů tuto variantu využije.

Další variantou identifikace by mohla být biometrická autentizace, tedy autentizace pomocí biologických charakteristik člověka. Tahle možnost by však vyžadovala speciální hardware (snímací zařízení), který by snímal určitou část těla (popřípadě hlas). V dnešní době už se vyrábí notebooky, které disponují čtečkou otisku prstů. Proto si myslím, že v budoucnu budou všechny počítače a notebooky vlastnit nějaký biometrický systém. Z tohoto důvodu je tahle varianta dosažitelnější, než by se na první pohled mohlo zdát.

### **Povinné zřizování datové schránky pro fyzické osoby**

Jak bylo zmíněno výše, Ministerstvo vnitra postupně elektronizuje všechny dokumenty u právnických osob a orgánů veřejné moci. Proto si myslím, že tenhle trend bude zaveden i mezi fyzické osoby. Všechny dopisy od úřadů už by se vyřizovaly pouze přes datovou schránku.

Datová schránka by mohla být zřízena už při narození dítěte, o kterou by se staral do jeho plnoletosti (popř. do jeho patnácti let) jeho zákonný zástupce. Další variantou by mohlo být

zřízení datové schránky po dovršení určitého věku (patnáct nebo osmnáct let). Do této doby by zprávy určené nezletilé osobě chodily jejímu zákonnému zástupci. Osobně si myslím, že nejvýhodnějším řešením by bylo zřízení datové schránky po dovršení patnáctého roku, tedy zároveň s občanským průkazem (elektronický občanský průkaz) by se zřídila i datová schránka.

Držitelé datové schránky už dnes mají výhodu například v tom, že můžou prostřednictvím datové schránky požádat o zaslání informativního osobního listu důchodového pojištění. Tuto možnost však občané bez datové schránky nemají, což by se dalo považovat za první krůček k tomuto velkému kroku.

## ZÁVĚR

První kapitola teoretické části se zabývala především pojmy, které souvisejí s datovými schránkami, jejich obecným popisem a správou datových schránek. V další části byly zmíněny zákony z mého pohledu důležité, které se týkají datových schránek a jaký vliv na ně mají. Třetí kapitola se soustředila na elektronický systém spisové služby a jeho spojení s datovými schránkami. Tahle kapitola tedy popisovala zacházení s elektronickými spisy. Byl zde objasněn životní cyklus přijaté a odeslané datové zprávy od jeho vzniku až po jeho archivaci a jak konvertovat elektronický dokument na listinný a naopak. Nastínila jsem zde také vztah mezi Informačním systémem datových schránek a spisovými službami.

Hlavním úkolem bakalářské práce byla praktická část, kde bylo za úkol určit pomocí dotazníkového šetření hlavní problémy týkající se datových schránek. Patnáct otázek, na které respondenti odpovídali, byly formulovány tak, abych zjistila, co jim nejvíce vadí na datových schránkách, ale i do jaké míry je využívají. Výzkum ukázal, že i přes většinovou spokojenost, jsou nedostatky, které by bylo možné eliminovat.

V další kapitole praktické části jsem měla za úkol specifikovat trendy v oblasti datových schránek. Také jsem navrhla řešení některých problémů, které byly zjištěny pomocí dotazníku a dají se nějakým způsobem ovlivnit. Dále byly navrženy další změny, které by z mého pohledu prospěly datovým schránkám a vzhledem k vývoji IT techniky by byly logické.

## SEZNAM POUŽITÉ LITERATURY

- [1] BUDIŠ, Petr a Iva HŘEBÍKOVÁ. Datové schránky: fungování, doručování, bezpečnost, návody. 1. vyd. Olomouc: ANAG, 2010, 287 s. ISBN 978-80-7263-617-4.
- [2] MATES, Pavel a Vladimír SMEJKAL. E-government v České republice: právní a technologické aspekty. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012, 464 s. ISBN 978-80-87576-36-6.
- [3] LAPÁČEK, Jiří. Jak na datovou schránku a elektronickou komunikaci s úřady. Brno: Computer Pres, 2012. ISBN 978-80-251-3680-5.
- [4] Datové schránky [online]. 2014 [cit. 2015-02-06]. Dostupné z: <http://www.datove-schranky.eu/>
- [5] BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi: certifikáty a certifikační autority: legislativní rámec elektronického podpisu: praktické aplikace. 1. vyd. Olomouc: ANAG, 2008, 157 s. ISBN 978-80-7263-465-1.
- [6] Datové schránky: Orgán veřejné moci [online]. 2015 [cit. 2015-12-01]. Dostupné z: <https://www.datoveschranky.info/organ-verejne-moci/organ-verejne-moci>
- [7] Datové schránky: Zřízení datové schránky na žádost [online]. 2015 [cit. 2015-12-01]. Dostupné z: <https://www.datoveschranky.info/zakladni-informace/zrizeni-datove-schranky-na-zadost>
- [8] Datové schránky: Doručování přístupových údajů [online]. [cit. 2015-12-03]. Dostupné z: <https://www.datoveschranky.info/zakladni-informace/dorucovani-pristupovych-udaju>
- [9] Datové schránky: Znepřístupnění datové schránky [online]. [cit. 2015-12-03]. Dostupné z: <http://www.datoveschranky.eu/info-o-datovych-schrankach/pravni-teorie-a-zajimavosti/znepristupneni-datove-schranky>
- [10] LIDINSKÝ, Vít. EGovernment bezpečně. 1. vyd. Praha: Grada, 2008, 145 s. ISBN 978-80-247-2462-1.
- [11] Adaptic: E-government. Adaptic: E-government [online]. [cit. 2016-02-04]. Dostupné z: <http://www.adaptic.cz/znalosti/slovnicek/e-government/>
- [12] Zákony pro lidi: Předpis č. 300/2008 Sb. Zákony pro lidi: Předpis č. 300/2008 Sb. [online]. [cit. 2016-02-04]. Dostupné z: <http://www.zakonyprolidi.cz/cs/2008-300#p2>

- [13] ŠTOURAČOVÁ, Jiřina. Úvod do archivnictví. Brno: Vydavatelství MU, 1999. 139 s. ISBN 80-210-2216-7.
- [14] BITTNER, Ivan. Spisová a archivní služba ve státní správě, samosprávě a v podnikatelské sféře. 3., aktualiz. a přeprac. vyd. Praha: Linde, 2005. ISBN 8072015494.
- [15] Životní cyklus dokumentu: Přehled řešení jednotlivých fází života dokumentu. System online: S přehledem ve světě informačních technologií [online]. 2003 [cit. 2016-04-02]. Dostupné z: <http://www.systemonline.cz/clanky/zivotni-cyklus-dokumentu.htm>
- [16] Czech point. Ministerstvo vnitra České republiky: eGovernment[online]. [cit. 2016-04-04]. Dostupné z: <http://www.czechpoint.cz/web/?q=node/470>
- [17] Předpis č. 499/2004 Sb. Zákon o archivnictví a spisové službě a o změně některých zákonů. Zákony pro lidi.cz [online]. [cit. 2016-04-27]. Dostupné z: <http://www.zakonyprolidi.cz/cs/2004-499>
- [18] Předpis č. 227/2000 Sb. Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Zákony pro lidi.cz [online]. [cit. 2016-04-28]. Dostupné z: <http://www.zakonyprolidi.cz/cs/2000-227>
- [19] Předpis č. 365/2000 Sb. Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. Zákony pro lidi.cz [online]. [cit. 2016-04-28]. Dostupné z: <http://www.zakonyprolidi.cz/cs/2000-365#p3>
- [20] Přístupové rozhraní. Datové schránky [online]. [cit. 2016-05-04]. Dostupné z: <https://www.datoveschranky.info/technicke-pozadavky/pristupove-rozhrani>
- [21] ING. TESAŘ, Pavel, ING. MENOŠEK, Ondřej (ed.). Provozní řád Informačního systému datových schránek. In: Datové schránky [online]. [cit. 2016-05-04]. Dostupné z: <https://www.datoveschranky.info/-/provozni-rad-is-8>
- [22] Datové schránky. Ministerstvo vnitra České republiky: Czech POINT [online]. [cit. 2016-05-12]. Dostupné z: <http://www.czechpoint.cz/web/?q=node/389>
- [23] Jednotný standard pro komunikaci mezi spisovými službami (SS) a Informačním systémem datových schránek (ISDS). Ministerstvo vnitra České republiky [online]. Zlín [cit. 2016-05-26]. Dostupné z: <http://www.mvcr.cz/sluzba/docDetail.aspx?docid=21344798&docType=ART&chnum=2>

[24] SMEJKAL, Vladimír a Michal Altair VALÁŠEK. Jak na datovou schránku: praktický manuál pro každého. Praha: Linde, 2012, 197 s. ISBN 978-80-86131-80-1.

## SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISDS    Informační systém datových schránek

ISVS    Informační systém veřejné zprávy

## SEZNAM OBRÁZKŮ

Obr. 1: Symbol eGovernmentu – panáček eGon (zdroj: <a href="http://www.egovernment.unas.cz">www.egovernment.unas.cz</a> ) .....	11
Obr. 2: Logo Czech POINTu (Zdroj: <a href="http://www.khkpce.cz">www.khkpce.cz</a> ) .....	12
Obr. 3: Fungování datových schránek (zdroj: <a href="http://www.inflow.cz">www.inflow.cz</a> ) .....	14
Obr. 4: Schéma informačního systému datových schránek (zdroj: <a href="http://www.datoveschranky.eu">www.datoveschranky.eu</a> ) .....	15
Obr. 5: Proces založení datové schránky (zdroj: <a href="http://www.slideshare.net">www.slideshare.net</a> ) .....	20
Obr. 6: Přihlášení pomocí jména a hesla (zdroj: <a href="http://www.mojedatovaschranka.cz">www.mojedatovaschranka.cz</a> ) .....	22
Obr. 7: Hardwarový token (zdroj: <a href="http://www.webobjects2.cdw.com">www.webobjects2.cdw.com</a> ) .....	23
Obr. 8: Softwarový token (zdroj: <a href="http://www.recarta.co.uk">www.recarta.co.uk</a> ) .....	24
Obr. 9: Přihlášení pomocí SMS kódu (zdroj: <a href="http://www.mojedatovaschranka.cz">www.mojedatovaschranka.cz</a> ) .....	24
Obr. 10: Právní forma podnikání (zdroj: vlastní) .....	42
Obr. 11: Spokojenost s komunikací přes datové schránky (zdroj: vlastní) .....	42
Obr. 12: Výhody používání datových schránek (zdroj: vlastní) .....	44
Obr. 13: Nevýhody používání datových schránek (zdroj: vlastní) .....	45
Obr. 14: Četnost komunikace s úřady (zdroj: vlastní) .....	46
Obr. 15: Používání datové schránky (zdroj: vlastní) .....	46
Obr. 16: Používání datové schránky pro komunikaci se soukromými subjekty (zdroj: vlastní) .....	47
Obr. 17: Zasílání zpráv od soukromoprávních subjektů (zdroj: vlastní) .....	48
Obr. 18: Četnost přihlašování do datových schránek (zdroj: vlastní) .....	48
Obr. 19: Držitelé zaručeného elektrického podpisu nebo zaručené elektronické značky (zdroj: vlastní) .....	49
Obr. 20: Přístup Pověřené osoby k datové schránce (zdroj: vlastní) .....	50
Obr. 21: Hodnocení spokojenosti komunikace se státními orgány prostřednictvím datových schránek (zdroj: vlastní) .....	51
Obr. 22: Bezpečnost datových schránek (zdroj: vlastní) .....	52



## SEZNAM PŘÍLOH

### **P I: Dotazníkové šetření**

CD obsahující dotazníkové šetření