

# **Analýza systému datových schránek**

Bc. Petr Píchal

---

Diplomová práce  
2012



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2011/2012

## ZADÁNÍ DIPLOMOVÉ PRÁCE (PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Petr PÍCHAL**  
Osobní číslo: **A10391**  
Studijní program: **N 3902 Inženýrská informatika**  
Studijní obor: **Informační technologie**

Téma práce: **Analýza systému datových schránek**

Zásady pro vypracování:

1. Seznamte se se systémem datových schránek.
2. Uvedte současné scénáře nasazení datových schránek.
3. Vypracujte metodu zpětného inženýrství use case model a popis uživatelských scénářů.
4. Analyzujte nedostatky současných scénářů.
5. Vypracujte upravený model případu užití.
6. Proveďte vyhodnocení přínosu upraveného řešení.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Datové schránky** [online]. 2010 [cit. 2012-02-03]. Dostupné z: <http://www.datoveschranky.eu/> Česká republika. Zákon o elektronických úkonech a autorizované konverzi dokumentu. In: c. 300/2008 Sb. 2008.
2. **Businessinfo: Datové schránky** [online]. 1997-2011 [cit. 2012-02-03]. Dostupné z: <http://www.businessinfo.cz/cz/rubrika/datove-schranky/1001772/>
3. **Portál datových schránek** [online]. 2011 [cit. 2012-02-03]. Dostupné z: <https://www.czebox.cz/PortalDS/> Ministerstvo vnitra České republiky: **Datové schránky** [online]. 2010 [cit. 2012-02-03]. Dostupné z: <http://www.mvcr.cz/datove-schranky.aspx>
4. **CzechPoint: Datové schránky** [online]. 2010 [cit. 2012-02-03]. Dostupné z: <http://www.czechpoint.cz/web/index.php?q=node/389>
5. **Datové schránky** [online]. 2011 [cit. 2012-02-03]. Dostupné z: <http://www.datoveschranky.info/>
6. **BUDIŠ, Petr, HŘEBÍKOVÁ Iva. Datové schránky: fungování, doručování, bezpečnost, návody.** 1. vyd. Olomouc: ANAG, 2010, 287 s. ISBN 80-726-3617-0.
7. **SMEJKAL, Vladimír. Datové schránky v právním řádu ČR: zákon c. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu, s komentářem.** 1. vyd. Praha: ABF, 2009, 176 s. ISBN 978-808-6284-781.

Vedoucí diplomové práce:

**Ing. Radek Šilhavý, Ph.D.**

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

**24. února 2012**

Termín odevzdání diplomové práce:

**21. května 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.  
*děkan*



doc. Mgr. Roman Jašek, Ph.D.  
*ředitel ústavu*

## **ABSTRAKT**

Práce, která se Vám dostala do rukou, se zaměřuje na současný stav a vývoj e-Governmentu v České republice. Její největší část analyzuje současný stav projektu datových schránek a nastiňuje možnosti rozvoje informačního systému pro tuto problematiku v následující etapě vývoje. Datové schránky byly uvedeny do provozu začátkem července 2009 jako unikátní projekt Ministerstva vnitra České republiky. Tento nástroj slouží k elektronickému doručování a konverzi dokumentů v oblasti veřejné správy.

Následující práce se zabývá zejména informačním systémem datových schránek (ISDS). V teoretické části je nastíněno pozadí elektronické komunikace ve veřejné správě. Praktická část se pak zabývá samotným informačním systémem, jeho analýzou pomocí metody zpětného inženýrství a návrhy na zlepšení.

Klíčová slova:

e-Government, datová schránka, konverze dokumentů, elektronický podpis, ISDS

## **ABSTRACT**

Work, which you are holding, focuses on the current state and development of e-Government in the Czech Republic. The largest part analyzes the current status of the data deposit boxes project and outlines the opportunities for information system development in the next stage of expansion. Data deposit boxes were put into operation in early July 2009 as an unique project of the Ministry of Interior of the Czech Republic. This tool is used for electronic document conversion and delivery in public administration. The following work is primarily dealing with data deposit boxes information system (ISDS). The theoretical part outlines the background of electronic communications in public administration. The practical part deals with the information system itself, its analysis using reverse engineering method and suggestions for improvement.

Keywords:

e-Government, data deposit box, document conversion, electronic signature, ISDS

## **Poděkování**

Chtěl bych poděkovat Ing. Radku Šilhavému, Ph.D. za laskavý souhlas s vedením této diplomové práce, vstřícný přístup, cenné rady a odborné vedení mé diplomové práce. Dále děkuji Mgr. Lence Hoškové za velmi cenné konzultace a také bych rád poděkoval celé své rodině, bez které by toto vše nebylo možné.

### **Prohlašuji, že**

1. 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;
2. 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;
3. 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;
4. 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;
5. 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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
6. 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;
7. 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,**

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

Ve Zlíně

.....  
podpis diplomanta

# OBSAH

<b>ÚVOD</b> .....	<b>9</b>
<b>I. TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 E-GOVERNMENT</b> .....	<b>11</b>
1.1 VYMEZENÍ POJMU.....	11
1.2 E-GOVERNMENT A JEHO VÝVOJ V ČR .....	12
1.3 SOUČASNOST V ČR .....	12
<b>2 DATOVÉ SCHRÁNKY</b> .....	<b>14</b>
2.1 CO JE TO DATOVÁ SCHRÁNKA.....	14
2.2 ÚČEL DATOVÝCH SCHRÁNEK.....	14
2.3 TYPY DATOVÝCH SCHRÁNEK.....	17
2.4 ZŘÍZENÍ A ZRUŠENÍ DATOVÉ SCHRÁNKY .....	19
2.4.1 Zřízení .....	19
2.4.2 Zpřístupnění .....	20
2.4.3 Znepřístupnění a zrušení .....	20
2.5 PŘÍSTUP DO DATOVÝCH SCHRÁNEK.....	21
2.6 AUTORIZOVANÁ KONVERZE .....	23
2.6.1 Definice, význam a druhy .....	23
2.6.2 Postup.....	26
2.6.3 Pojem ověřovací doložka a její význam.....	28
2.7 ELEKTRONICKÝ PODPIS, CERTIFIKÁTY A ELEKTRONICKÉ RAZÍTKO .....	31
<b>3 INFORMAČNÍ SYSTÉM DATOVÝCH SCHRÁNEK</b> .....	<b>33</b>
3.1 LEGISLATIVA A PROVOZOVATEL .....	33
3.2 OBSAH ISDS .....	33
3.3 NEVEŘEJNÉ ÚDAJE V ISDS.....	35
<b>II. PRAKTICKÁ ČÁST</b> .....	<b>36</b>
<b>4 SOUČASNÉ ŘEŠENÍ</b> .....	<b>37</b>
4.1 AKTÉŘI.....	37
4.2 PŘÍPADY UŽITÍ (USE CASE) .....	38
4.2.1 Přihlášení k ISDS .....	38
4.2.2 Nastavení datové schránky.....	40
4.2.3 Práce s datovou zprávou.....	44
4.2.4 Práce s adresářem .....	50
<b>5 NEDOSTATKY SOUČASNÉHO ŘEŠENÍ</b> .....	<b>53</b>
<b>6 NÁVRHY NA VYLEPŠENÍ PRO SYSTÉM ISDS</b> .....	<b>56</b>
<b>7 NAVRHOVANÉ ŘEŠENÍ</b> .....	<b>57</b>
7.1 POŽADAVKY.....	57
7.1.1 Nefunkční požadavky.....	57
7.1.2 Funkční požadavky .....	58
7.2 PŘÍPADY UŽITÍ (USE CASE) .....	59
7.2.1 Nastavení datové schránky.....	59
7.2.2 Práce s datovou zprávou.....	60

7.2.3 Práce s adresářem .....	61
7.3 VYHODNOCENÍ .....	62
<b>ZÁVĚR .....</b>	<b>63</b>
<b>CONCLUSION .....</b>	<b>64</b>
<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>65</b>
<b>SEZNAM POUŽITÝCH CITACÍ.....</b>	<b>66</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>	<b>67</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>68</b>
<b>SEZNAM TABULEK.....</b>	<b>69</b>
<b>SEZNAM PŘÍLOH.....</b>	<b>70</b>

## ÚVOD

Nástup informačních technologií do stále nových oblastí v dnešní době už asi zaskočí jen málokoho, tím méně pokud se jedná o správu informací. Přesto mnozí lidé označují schválení zákona č. 300/2008 Sb., jako největší změnu ve státní správě od dob Marie Terezie. 1. července 2009 nabyl zákon o elektronických úkonech a autorizované konverzi dokumentů platnosti a rozběhl se projekt známý jako „datové schránky“, který měl za úkol zjednodušit a zlevnit komunikaci v oblasti veřejné správy. Během prvních čtyř měsíců probíhalo tzv. náběhové období, během kterého se majitelé zákonem zřízených datových schránek mohli se systémem seznámit, nicméně stále nemuseli schránku povinně aktivovat. Toto období skončilo k 1. listopadu 2009 a tehdy také došlo k automatické aktivaci všech zákonem zřízených datových schránek. Od tohoto data jsou také všichni majitelé těchto schránek zákonem povinováni k jejich používání.

Tento projekt je naprostým unikátem, který nemá ve světě obdoby. Datové schránky dnes slouží jako nástroj komunikace orgánům veřejné moci, právníkům osobám a podnikajícím fyzickým osobám a zároveň přinášejí možnost efektivní autorizované konverze dokumentů pro uvedené subjekty.

V následující práci se seznámíme se současným stavem a vývojem e-Governmentu v České republice. Analyzujeme projekt datových schránek a podíváme se na možnosti dalšího rozvoje. V první části nastíníme pozadí elektronické komunikace ve veřejné správě. Vymežíme pojmy jako e-Government, autorizovaná konverze či elektronický podpis. Seznámíme se se systémem datových schránek a uvedeme současné scénáře nasazení.

V praktické části provedeme studii informačního systému datových schránek metodou zpětného inženýrství. Vypracujeme analýzu současného systému a podíváme se jak na jeho fungování, tak na scénáře nasazení. Pokusíme se odhalit nedostatky stávajícího řešení a na základě těchto poznatků vypracujeme nový model informačního systému s cílem dojít k vylepšenému řešení.

## TEORETICKÁ ČÁST

## 8. E-GOVERNMENT

E-Government, v překladu doslova elektronické vládnutí, je jedním z nástrojů budování informační společnosti. Umožňuje komunikaci s institucemi státní a veřejné správy v elektronické podobě a elektronizaci veškerých procesů, které s tím souvisejí.

### 1. Vymezení pojmu

K vymezení e-Governmentu můžeme uvést několik definicí. Podle dokumentu Evropské unie „Evropská informační společnost 2010“ e-Government znamená efektivní a výkonné veřejné služby a informační a komunikační technologie umožňující občanům plně se podílet na životě společensky a kulturně tvůrčích komunit včetně demokratického procesu.

Stručnější definici uvádí organizace OECD, ta vymezuje e-Government jako použití elektronických komunikací, zejména pak internetu, jako nástroje pro dosažení lepší správy.

V České republice definuje e-Governmentu Ministerstvo vnitra ČR: „e-Government představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům.“ (1)

Za klíčovou část e-Governmentu považujeme elektronickou komunikaci, e-Government pak můžeme rozdělit na:

1. Government-to Citizen (G2C) – komunikace úřadu s občanem
2. Government-to-Business (G2B) – komunikace úřadu s podnikateli a obchodními společnostmi
3. Government-to- Government (G2G) – komunikace mezi úřady navzájem

Hlavním cílem e-Governmentu je především usnadnění komunikace veřejnosti s úřady, vytvoření jejích jednoznačných a předvídatelných postupů a zajištění požadovanou míru dosažitelnosti informací o podmínkách této komunikace v příslušných agendách.

## 1. E-Government a jeho vývoj v ČR

Před 13 lety, v roce 1999, byla v České republice uvedena první ucelená koncepce v oblasti budování informační společnosti. Strategie se zaměřila na tři oblasti:

1. Informatizace veřejné správy (jež byla prioritou)
2. Informační gramotnost
3. Elektronický obchod

Následně byla rozpracována na jednotlivé specifické úkoly uvedené v dokumentu „Akční plán realizace státní informační politiky do roku 2003“.

20. září 2006 významně přispělo k legislativním změnám v oblasti elektronizace státní správy usnesení vlády ČR č. 1085 o souboru opatření pro urychlení rozvoje e-Governmentu v České republice. O dva roky později, 19. srpna 2008 byl vyhlášen ve sbírce zákonů zákonem č.300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů. Společně se zákonem č.300/2008 Sb. byl přijat také doprovodný zákon č.301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů.

## 1. Současnost v ČR

V České republice nabyt účinnosti Zákon o elektronických úkonech a autorizované konverzi dokumentů, který byl vyhlášen ve Sbírce zákonů 19. 8. 2008 jako **Zákon č.300/2008 Sb.**, někdy též nazývaný Zákon o e-Governmentu nebo e-Government Act.

Cílem zákona je vytvoření optimálních podmínek pro elektrickou komunikaci mezi úřady a občany i mezi úřady navzájem. Umožňuje též vedení elektronických spisů ve správních řízeních.

V současnosti je za e-Government v České republice odpovědným resortem Ministerstvo vnitra ČR. To e-Government představuje pomocí symbolu/postavičky EGONa. Prezentuje jej jako symbol elektronizace veřejné správy – moderního, přátelského a efektivního řádu.

EGON je v přeneseném významu jako živý organismus. Fungování jeho jednotlivých částí se navzájem podmiňuje a vše souvisí se vším. Existenci a životní funkce EGONa zajišťuje mozek, srdce, oběhová soustava a prsty.



Obrázek 1: *EGON* (zdroj [www.mvcr.cz](http://www.mvcr.cz))

Mozkem míníme **Základní registry veřejné správy** – bezpečné a aktuální databáze dat pojednávajících o občanech i o státních a nestátních subjektech. Těžištěm jsou základní čtyři registry. Registr obyvatel, Registr práv a povinností, Registr osob a Registr územní identifikace, adres a nemovitostí.

Dalším a klíčovým orgánem je srdce, tedy **Zákon o elektronických úkonech a autorizované konverzi č. 300/2008 Sb.**

**Komunikační infrastruktura veřejné správy**, představující oběhovou soustavu, se zabývá citlivým tématem a to bezpečností přenosu dat. Zjednodušeně řečeno, představuje sjednocení různých datových linek subjektů veřejné správy do jedné datové sítě.

**Czech POINT** – Český Podací Ověřovací Informační Národní Terminál, který je na EGO-Nu představován prsty, umožňuje získat na jednom místě všechny informace o údajích vedených v centrálním registru prostřednictvím vydávání ověřených výstupů z informačního systému veřejné správy. Czech POINT upravuje zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

## 4. DATOVÉ SCHRÁNKY

### 1. Co je to datová schránka

Informačním systémem veřejné správy jsou datové schránky, které zásadně mění způsob doručování úředních dokumentů a to právě díky informačním technologiím. Pomocí datových schránek je možné zasílat dokumenty v elektronické podobě orgánům veřejné moci a také je takto od nich přijímat.

Datová schránka slouží pro komunikaci v oblasti veřejné správy. Jejím prostřednictvím lze činit podání kterémukoliv úřadu. Úřady prostřednictvím datové schránky doručují své písemnosti příslušným adresátům (fyzickým nebo právnickým osobám), stejně jako komunikují s jinými orgány veřejné správy. Veškerým úkonům, které jsou prostřednictvím elektronické datové schránky, resp. přepážky činěny, je přiznána ekvivalence k úkonům činěným písemně. (2)

Cílem projektu informačního systému je zefektivnit veřejnou správu. Učinit ji rychlejší, levnější a spolehlivější.

### 2. Účel datových schránek

Datová schránka je elektronické úložiště určené k provádění elektronických úkonů vůči orgánům veřejné moci, doručování orgány veřejné moci, jejich vzájemné komunikaci a dodávání dokumentů fyzických osob, podnikajících fyzických a právnických osob mezi těmito osobami.

#### **Provádění elektronických úkonů vůči orgánům veřejné moci**

Provádění elektronických úkonů vůči orgánům veřejné moci prostřednictvím datových schránek upravuje zákon č.300/2008 Sb. Podle §18 zákona může fyzická osoba, podnikající fyzická osoba a právnická osoba provádět úkon vůči orgánu veřejné moci, má-li zpřístupněnou svou datovou schránku a umožňuje-li to povaha tohoto úkonu, prostřednictvím datové schránky. Úkon provedený prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více uvedených osob.

Podání prostřednictvím datových schránek učiněné právnickou nebo fyzickou osobou, nemusí být nutně opatřeno uznávaným elektronickým podpisem, a to pokud podání učiní osoba oprávněná/pověřená k přístupu do datové schránky a pověřená k danému úkonu. Výjimkou je, pokud jiný právní či vnitřní předpis určuje k podpisu dvě či více osob oprávněných k jednání. V tomto případě by museli být všechny podpisy na tomto dokumentu opatřeny zaručeným elektronickým podpisem.

Podání prostřednictvím datové schránky lze činit pouze jménem jejího držitele. Úkon takto učiněný prostřednictvím cizí datové schránky nemá zákonem přiznané právní účinky. Nelze jej však nutně považovat za neúčinné. Příkladem je odeslání z cizí datové schránky opatřené zaručeným elektronickým podpisem subjektu činícího tento úkon. Pak lze i tento úkon považovat za bezzávadný.

Důležitou otázkou týkající se okamžiku doručení dokumentu do datové schránky se zabýval poradní sbor ministerstva vnitra. Podání fyzické osoby, podnikající fyzické osoby nebo právnické osoby vůči správnímu orgánu (orgánu veřejné moci) prostřednictvím datové schránky je učiněno okamžikem dodání do datové schránky orgánu veřejné moci. (3)

Výše popsané pravidlo, podpořené také soudní judikaturou (Rozhodnutí ústavního soudu, sp. zn. I. ÚS 750/06 ze dne 6. června 2007), se neuplatňuje při doručování dokumentů orgánů veřejné moci, popsané v dalších odstavcích.

### **Dokumenty orgánů veřejné moci a jejich doručování**

Dokumenty orgánů veřejné moci, které jsou doručovány přes datovou schránku a úkony prováděné vůči orgánům veřejné moci prováděné přes datovou schránku mají formu datové zprávy. Tyto úkony pak musí být opatřeny uznávaným elektronickým podpisem úřední osoby.

Zákon o e-Governmentu vymezuje, kdy není možné doručování prostřednictvím datových schránek. V první řadě je to případ, doručuje-li se veřejnou vyhláškou (např. řízení při velkém počtu účastníků), druhým případem je doručování na místě (, které je spjato s provedením konkrétního úkonu), v neposlední řadě doručení prostřednictvím datových schránek není možné, pokud to neumožňuje povaha dokumentu (např. jedná-li se o utajované informace nebo formu, kterou nelze odeslat přes datové schránky). Logickým důvo-

dem pro nemožnost doručení prostřednictvím datových schránek je, že adresát nemá datovou schránku zpřístupněnou.

Závěrečné rozhodnutí, zda povaha dokumentu umožňuje odeslání přes datovou schránku, učiní vždy orgán veřejné moci, který dokument odesílá.

Důležitým a poněkud problematickým je téma určení doby doručení adresátovy. Podle zákona č.300/2008 Sb., je dokument, který byl dodán do datové schránky, je doručen okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému dokumentu. (4)

V případě přístupu/přihlášení do datové schránky je dokument považován za doručený tímto okamžikem vstupu. Nedojde-li k přihlášení do 10 dnů, považujeme dokument za doručený posledním dnem této lhůty.

Dokladem o doručení dokumentu do datové schránky je oznámení odeslané Ministerstvem vnitra ČR (podle §20 odst. 1 písm. e) zákona) opatřené uznávanou elektronickou značkou.

### **Komunikace mezi orgány veřejné moci**

Orgány veřejné moci mají od 1. července 2009 mezi sebou navzájem komunikovat pouze prostřednictvím datových schránek. Komunikaci písemnou korespondencí by měly využívat jen tehdy, pokud to vyžaduje povaha věci zasílaného dokumentu.

Jak jsem uvedl v předchozí kapitole, za okamžik doručení datové zprávy orgánu veřejné moci považujeme okamžik jejího dodání.

### **Dodávání dokumentů fyzických osob, podnikajících fyzických a právnických osob mezi těmito osobami**

Možnost komunikace pomocí datových zpráv mezi fyzickými osobami, podnikajícími osobami a právnickými osobami navzájem upravila až novelizace Zákona o e-Governmentu č.190/2009 Sb. Tato komunikace mezi soukromými subjekty se částečně odlišuje oproti komunikaci s orgány veřejné moci.

## 1. Zpoplatnění

Plátcem je subjekt, z jehož datové schránky byla zpráva odeslána a příjemcem platby je provozovatel systému (Česká pošta, s.p.). Níže uvádím aktuální ceny bez DPH.

<b>Ceník poplatků</b>	
Odeslání Poštovní datové zprávy (Cena / 1 PDZ)	11,68 Kč
Odeslání Odpovědní datové zprávy	11,68 Kč
Odeslání Dotované datové zprávy	11,68 Kč
<b>Měsíční poplatek za využívání služby</b>	
Počet zpráv odeslaných v měsíci	Cena / měsíc
1 - 10	50 Kč
11 - 50	35 Kč
nad 50	20 Kč

Tabulka 1: *Ceník poplatků*

## 2. Okamžik doručení dokumentu

V případě komunikace „privátní“ se za okamžik doručení považuje okamžik, kdy adresát potvrdí odesílateli prostřednictvím datové schránky jeho převzetí. Toto potvrzení neodesílá Ministerstvo vnitra ČR ale sám adresát. Nečiní se tak automaticky po přihlášení do datové schránky, ale jde o úkon svobodné vůle adresáta.

## 3. Elektronický podpis

Dokument odeslaný prostřednictvím datové schránky musí být elektronicky podepsán, pokud se jedná o komunikaci „privátní“.

## 1. Typy datových schránek

Zákon č. 300/2008 Sb. rozlišuje čtyři typy datových schránek a to podle subjektu, jímž jsou zřizovány.

1. Datové schránky fyzických osob
2. Datové schránky podnikajících fyzických osob
3. Datové schránky právnických osob
4. Datové schránky orgánů veřejné moci

**Datové schránky fyzických osob:** Na žádost fyzické osoby zřídí ministerstvo bezplatně datovou schránku do tří dnů od podání žádosti. Každá fyzická osoba má nárok na zřízení jedné datové schránky a žádost musí splňovat náležitosti dané zákonem (zákon č. 300/2008 Sb. §3, odst. 3). Fyzická osoba žádající o zřízení není limitována svým státním občanstvím nebo místem trvalého pobytu apod.

**Datové schránky podnikajících fyzických osob** zřizuje ministerstvo na žádost. Každá podnikající fyzická osoba má nárok na jednu datovou schránku, vyjma advokátů, daňových poradců a insolvenčních plátců. Podle §4 zákona 300/2008 Sb. se pro advokacii, daňové poradenství a insolvenční správcovství zřizuje samostatná datová schránka podnikající fyzické osoby. Za určitých okolností může mít podnikající fyzická osoba až tři datové schránky, např. advokát+podnikatel+občan nepodnikající. Od 1. 7. 2012 je zřízení datové schránky pro tuto specifickou skupinu povinné. Pokud si ji takto podnikající fyzické osoby nezřídí sami, udělá to za ně Ministerstvo vnitra.

**Datovou schránku právnické osoby** zřídí ministerstvo bezplatně právnické osobě zřízené zákonem, právnické osobě zapsané v obchodním rejstříku a organizační složce podniku zahraniční právnické osoby zapsané v obchodním rejstříku, a to v případě právnické osoby zřízené zákonem bezodkladně po jejím vzniku, v případě právnické osoby zapsané v obchodním rejstříku a organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku bezodkladně poté, co obdrží informaci o jejím zapsání do obchodního rejstříku. (5)

Dobrovolně, na základě žádosti zřídí ministerstvo datovou schránku ostatním právnickým osobám. Každá právnická osoba má nárok na jednu datovou schránku.

**Datové schránky orgánů veřejné moci** zřizuje ministerstvo stejně jako u právnických osob bezodkladně po jejím vzniku. Za orgán veřejné moci považujeme samosprávné komory zřízené zákonem (např. Česká lékařská komora nebo Česká advokátní komora), státní fondy (např. Státní fond dopravní infrastruktury, Státní fond rozvoje bydlení...), zdravotní pojišťovny (v současnosti 8 pojišťoven) a notáři a soudní exekutoři (na základně výkonu veřejné moci).

## 1. Zřízení a zrušení datové schránky

### 1. Zřízení

Jak vyplývá z předchozích kapitol, rozlišujeme dva způsoby zřízení datové schránky, na žádost nebo ze zákona.

Ze zákona se zřizují datové schránky pro:

1. orgány veřejné moci
2. právnické osoby zřízeným zákonem
3. právnické osoby zapsané v obchodním rejstříku
4. organizační složky podniků zahraničních právnických osob zapsaných v obchodním rejstříku
5. insolvenční správce
6. advokáty
7. daňové poradce

Podle zákona č. 300/2008 Sb. zřizuje výše uvedeným datovou schránku Ministerstvo Vnitřní záležitostí ČR již od 28. 9. 2009. Výjimkou jsou advokáti a daňoví poradci, kterým je zřizována datová schránka prozatím na žádost. Od 1. 7. tohoto roku, tomu však bude jinak a používání schránek budou mít i tito povinné. Ministerstvo zřizuje datovou schránku bezodkladně po obdržení informace o vzniku/zápisu do zákonem stanovené evidence (např. obchodní rejstřík).

Fyzické osoby, většina podnikajících fyzických osob a část právnických osob (tedy skupina, které není zřizována datová schránka podle zákona automaticky) má možnost požádat o zřízení. Tato žádost musí obsahovat údaje požadované zákonem a je doručována Ministerstvu vnitra. Vzorový formulář pro tuto žádost ministerstvo vypracovalo a je ke stažení např. zde <http://www.datoveschranky.info/cz/metodicke-postupy/postupy-pri-zrizovani-datove-schranky-a-zadost-id34700/>, avšak jeho použití pouze doporučuje, neukládá jej za povinné.

Žádost lze podat několika způsoby. Osobně a to na podatelnu Ministerstva vnitra nebo na Czech POINTu, poštou, elektronickou poštou či ve zvláštním případě zřízení další datové schránky prostřednictvím datové schránky (další schránka orgánu veřejné moci).

Splňuje-li žádost všechny zákonem stanovené požadavky, zřídí ji ministerstvo do 3 dnů ode dne podání žádosti. V této lhůtě mají být žadateli také zaslány přístupové údaje.

## 1. Zpřístupnění

Rozhodujícím, nikoli však jediným způsobem zpřístupnění do datové schránky je první přihlášení uživatele. To se odvíjí od okamžiku doručení přístupových údajů.

Pokud se oprávněná osoba do datové schránky sama nepřihlásí po obdržení těchto údajů, počínaje dnem doručení přístupových hesel počítáme patnácti denní lhůtu, po jejímž uplynutí je schránka sama automaticky zpřístupněna a od této chvíle do ní mohou být zasílány datové zprávy.

## 2. Znepřístupnění a zrušení

Zákon o e-Governmentu vymezuje také znepřístupnění do datové schránky (§11). Pamatujte na nečekané události v životě osoby, proto ministerstvo znepřístupní datovou schránku fyzické osoby (případně i zpětně) ke dni úmrtí osoby, pro kterou byla datová schránka zřízena nebo ke dni uvedenému rozhodnutí soudu o prohlášení za mrtvého (jako den úmrtí této osoby). Datová schránka je znepřístupněna také osobě, která byla zbavena nebo jí byla omezena způsobilost k právním úkonům nebo pokud byla daná osoba omezena na osobní svobodě. Důvodem k omezení na osobní svobodě pak míníme vzetí do vazby, výkon trestu odnětí svobody, výkon zabezpečovací detence, ochranného léčení nebo ochrany zdraví lidu.

Pokud je právnická osoba vymazána ze zákonem stanovené evidence, provede Ministerstvo znepřístupnění její datové schránky ke dni jejího výmazu.

Stejný je také postup, pokud dojde ke zrušení orgánu veřejné moci nebo zákonem zřízené právnické osoby. Jde-li o notáře a soudní exekutory, znepřístupní ministerstvo jejich datovou schránku ke dni zániku funkce.

Datovou schránku, která byla zřízena na žádost, lze také znepřístupnit na žádost. V tomto případě je pak schránka znepřístupněna nejpozději třetím pracovním dnem následujícím po podání žádosti. Touto žádostí dává oprávněná osoba najevo, že si nepřeje zasílat datové zprávy ze strany orgánů veřejné moci. Zpřístupnění je opět obnoveno po zaslání žádosti. Pokud ministerstvo obdrží žádost o znepřístupnění dvakrát za poslední rok, lze ji zpřístupnit nejdříve uplynutím jednoho roku od jejího posledního znepřístupnění.

**Zrušení datové schránky** je stejně jako její zřízení v kompetenci Ministerstva vnitra ČR. O zrušení pojednává zákon č. 300/2008 Sb. v §13. Obecně lze říci, že ke zrušení dochází

po uplynutí doby 3 let. U fyzických osob je to tři roky od jejího úmrtí, případně od rozhodnutí soudu o prohlášení za mrtvého. Právníkům osobám je lhůta tří let započata dnem jejího výmazu z evidence a orgánům veřejné moci ode dne jeho zrušení.

## 2. Přístup do datových schránek

Prvotní přístup do datové schránky mají tzv. **primární osoby**, pro něž je datová schránka zřízena. Tyto osoby pak mohou zplnomocnit tzv. pověřenou osobu či administrátora. Role těchto oprávněných osob blíže popíšeme v dalších odstavcích.

Typ datové schránky	Kdo má přístup do datové schránky?
<b>datová schránka</b> fyzické osoby	<ul style="list-style-type: none"> <li>. fyzická osoba, pro niž je schránka zřízena</li> <li>. administrátor</li> <li>. pověřená osoba</li> </ul>
<b>datová schránka</b> podnikající fyzické osoby	<ul style="list-style-type: none"> <li>. podnikající fyzická osoba, pro niž je DS zřízena</li> <li>. administrátor</li> <li>. pověřená osoba</li> </ul>
<b>datová schránka</b> právnické osoby	<ul style="list-style-type: none"> <li>. statutární orgán právnické osoby/člen statutárního orgánu právnické osoby nebo vedoucí organizační složky</li> <li>. administrátor</li> <li>. pověřená osoba</li> </ul>
<b>datová schránka</b> orgánu veřejné moci	<ul style="list-style-type: none"> <li>1. vedoucí orgánu veřejné moci</li> <li>. administrátor</li> <li>. pověřená osoba</li> </ul>

Tabulka 2: *Přístupy*

Pro vedoucí orgány veřejné moci a statutární orgány velkých právnických osob může správa datových schránek znamenat časově náročnou ryze administrativní činnost. Proto byla vytvořena funkce **administrátora**, kterým je ustanovena fyzická osoba k tomu určená. Role administrátora slouží hlavně k pověřování dalších odpovědných osob a stanovení jejich

rozsahu oprávnění. Administrátor také může sám ministerstvo žádat o zneprístupnění a zpřístupnění datové schránky. Prvotně není funkce administrátora určena k přístupu do datové schránky a čtení a odesílání zpráv. Tyto úkony může činit pouze tehdy, pokud by byl osoba pověřená. Teoreticky může administrátor do role pověřené osoby pověřit sám sebe.

Další osobou, která může mít přístup do datových schránek je tzv. **pověřená osoba**. Jedna datová schránka může mít libovolný počet takto pověřených osob. Lze jim přidělovat tato práva:

1. čtení zpráv
2. čtení zpráv určených do vlastních rukou
3. vytvářet a odesílat datové zprávy
4. prohlížet seznam dodaných zpráv i doručenek

Nejsnadnější cestou pro jmenování ověřené osoby či administrátora je využití webovém portálu datových schránek, kde je uložen ke stažení příslušný formulář.

Oprávněné osoby se do datové schránky přihlašují za pomoci přístupových údajů. Těmi jsou **uživatelské jméno** a **bezpečnostní heslo**, které obdrží od Ministerstva vnitra ČR. Uživatelské jméno je řetězec nejméně 6 a nejvíce 12 znaky. Vzniká automatickým generováním. Heslo musí tvořit nejméně 8 a nejvýše 32 znaků, které tvoří kombinace písmen, číslic a speciálních znaků uvedených v příloze vyhlášky č. 194/2009 Sb., (viz tabulka č. 3) a musí být odlišné od přihlašovacího jména. Z bezpečnostních důvodů je systém nastaven tak, aby po prvním přihlášení odpovědná osoba toto heslo změnila. Změnu hesla lze provést kdykoli. V současnosti je systém nastavený tak, že platnost hesla je 90 dní.

I. Písmena a číslice Přípustný znak	ASCII kód přípustného znaku	Přípustný znak	ASCII kód přípustného znaku	Přípustný znak	ASCII kód přípustného znaku
0	48	L	76	g	103
1	49	M	77	h	104
2	50	N	78	i	105
3	51	O	79	j	106
4	52	P	80	k	107
5	53	Q	81	l	108
6	54	R	82	m	109
7	55	S	83	n	110
8	56	T	84	o	111
9	57	U	85	p	112
A	65	V	86	q	113
B	66	W	87	r	114
C	67	X	88	s	115
D	68	Y	89	t	116
E	69	Z	90	u	117
F	70	a	97	v	118
G	71	b	98	w	119
H	72	c	99	x	120
I	73	d	100	y	121
J	74	e	101	z	122
K	75	f	102		
II. Speciální znaky Přípustný znak	ASCII kód přípustného znaku	Přípustný znak	ASCII kód přípustného znaku	Přípustný znak	ASCII kód přípustného znaku
!	33	+	43	[	91
#	35	,	44	]	93
\$	36	-	45	_	95
%	37	.	46	{	123
&	38	:	58		124
(	40	=	61	}	125
)	41	?	63	~	126

Tabulka 3: Přípustné znaky pro tvorbu uživatelského jména a bezpečnostního hesla

## 1. Autorizovaná konverze

### 1. Definice, význam a druhy

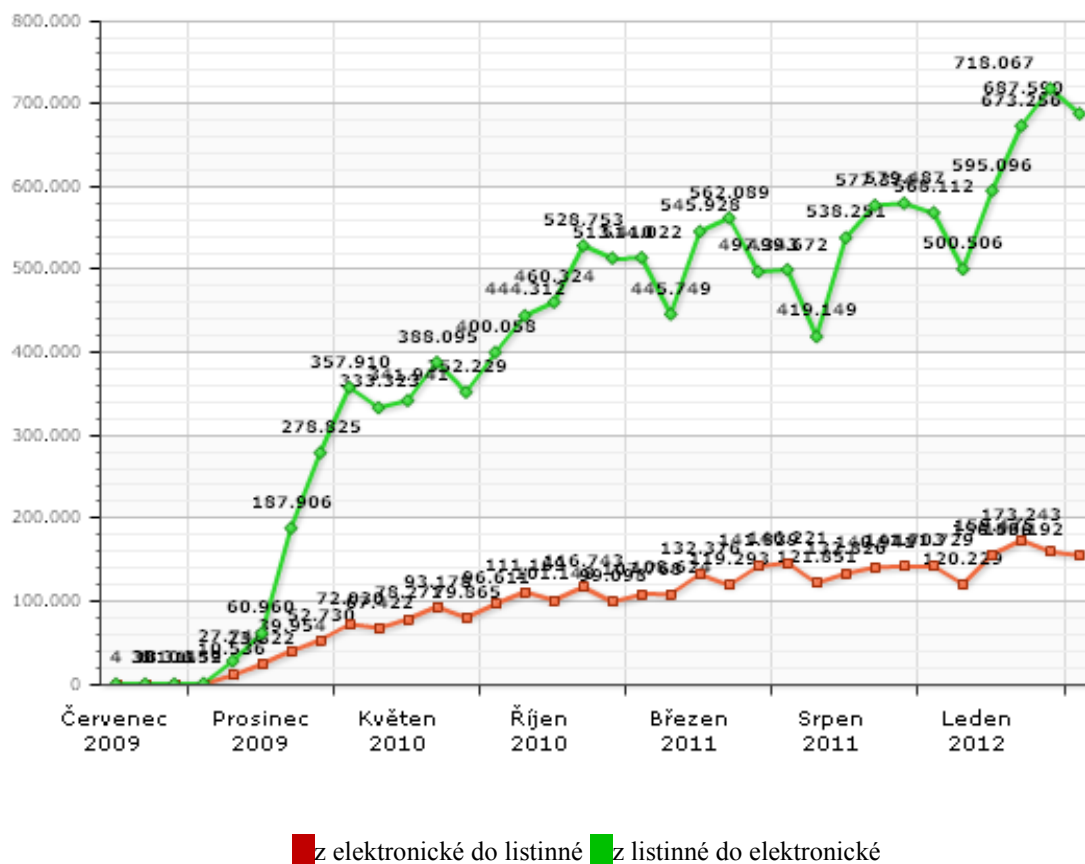
Podle slovníku cizích slov můžeme chápat význam slova *konverze* jako přeměnu, změnu, obrat. Autorizovanou konverzi dokumentů definujeme jako úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky. (6) Dokument, který tímto převede-

ním vznikl, má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl. Díky tomu se přibližuje zrovnoprávnění elektronické komunikace s komunikací listinnou. U autorizované konverze dokumentu se nepotvrzuje správnost a pravdivost údajů v souladu s právními předpisy, ale stejně jako je tomu u vidimace, pouze shoda.

Podrobnostmi o autorizované konverzi dokumentů se zabývalo Ministerstvo vnitra České republiky, které stanovilo detaily toho se týkající ve vyhlášce č. 193/2009 Sb.

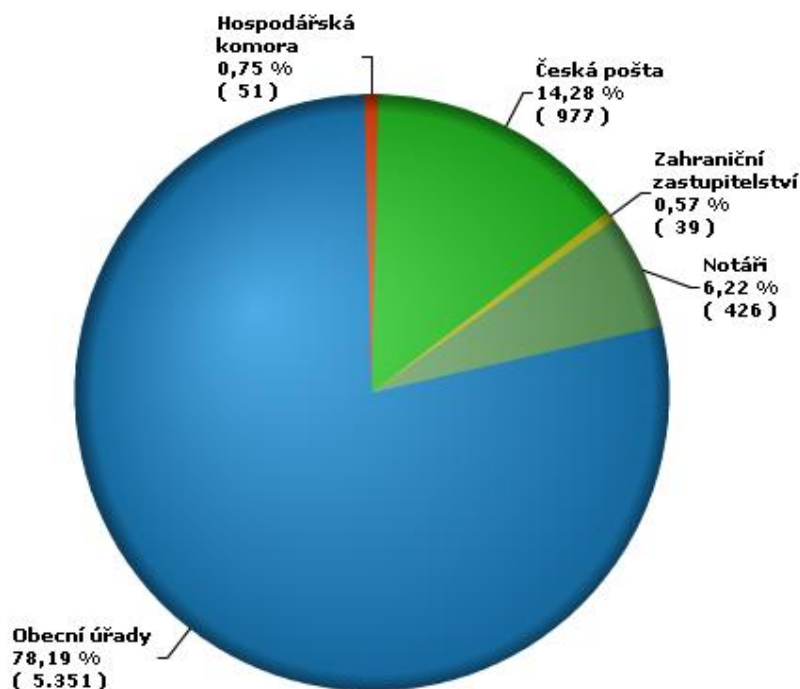
Podle zákona rozlišujeme dva typy autorizované konverze: na žádost a z moci úřední. Oba takto zkonvertované dokumenty mají stejné právní účinky.

*Autorizovaná konverze z moci úřední* je prováděna orgány veřejné moci pro výkon své působnosti. Pro orgán veřejné moci je toto právo výlučné a nelze jej přenést na jiný subjekt. Od počátku tohoto roku statistiky Czech POINTU zaznamenaly výrazně vyšší nárůst konverze z moci úřední. V březnu uvádí dokonce 718 067 konverzí z listinné do elektronické formy. Opačná forma naopak klesá. Jak 10. 4. 2012 uvedl Czech POINT na svém webu, dalo by se říct, že orgány veřejné moci přišly konečně elektronickým dokumentům na chuť. Není to ale tak docela pravda. Většinu konverzí do elektronické formy stále provádějí exekutoři. Ti už dávno pochopili výhody plynoucí z převodu do elektronické formy a zastavili papír na vstupu do úřadu. (7)



Obrázek 2: Autorizovaná konverze z moci úřední (zdroj www.czechpoint.cz)

*Autorizované konverze na žádost* provádějí kontaktní místa veřejné správy, tj. notáři, krajské úřady, matriční úřady, obecní úřady, úřady městských částí nebo městských obvodů územně členěných statutárních měst a úřady městských částí hl. m. Prahy. Dále zastupitelské úřady, držitel poštovní licence, Hospodářská komora České republiky. Systém Czech POINTU - kontaktních míst veřejné správy - byl k 15. 5. 2012 tvořen 6.843 kontaktními místy. Největší podíl logicky tvoří obecní úřady, 78 % z celkové obsazenosti. Druhé „největší“ pokrytí 14%, má Česká pošta, s. p.. Celkové rozdělení kontaktních míst veřejné správy uvádím níže v grafu.



Obrázek 3: Pracoviště Czech POINT k 14. 4. 2012  
(zdroj [www.czechpoint.cz](http://www.czechpoint.cz))

## 2. Postup

Autorizovaná konverze dokumentů se provádí prostřednictvím elektronické aplikace systému kontaktních míst veřejné správy přístupné způsobem umožňujícím dálkový přístup. Systémem kontaktních míst, Czech POINTU, míníme soubor technického a programového vybavení Ministerstva vnitra ČR a elektronickou aplikací programové vybavení. Účelem je sjednocení provádění autorizované konverze všemi oprávněnými subjekty.

**Konverze z elektronické do listinné podoby** – elektronicky doručený dokument, který chce příjemce zprávy převést do listinné podoby je možné na Czech POINT přinést na CD/DVD. Druhou možností je poslat žádost o konverzi přímo z datové schránky do Úschovny (datového úložiště), kde se automaticky vygeneruje potvrzení o odeslání dokumentu ke konverzi (viz obr. č. 4), které pak na Czech POINT s sebou zákazník přinese.

Potvrzení obsahuje jeho jednoznačnou identifikaci a informace o datu vystavení a datu, kdy je nejpozději možné dokument vyzvednout z elektronické podoby do listinné.

**Potvrzení o odeslání dokumentu ke konverzi**

Potvrzuje, že dokument byl vložen do úschovny pro potřeby konverze v souladu s ustanovením zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, v platném znění. Dokument byl vložen pod pořadovým číslem:

**514217235527536103881**

**Důležitá upozornění**

Dokument může být na základě tohoto potvrzení předán ke konverzi z elektronické podoby do listinné pouze jednou. Po provedení konverze bude z úschovny dokument okamžitě odstraněn. Listinnou podobu dokumentu si můžete osobně vyzvednout na kterémkoli kontaktním místě Czech POINT nejpozději do 30 kalendářních dnů. Nebude-li konverze provedena, bude dokument z evidence odstraněn.

Seznam kontaktních míst Czech POINT naleznete zde: <http://www.czechpoint.cz/web/?q=node/62>

Datum vystavení: 11.5.2010

Ke konverzi nejpozději dne: 10.6.2010



**514217235527536103881**

Vytisknout konverzní lístek      Zavřít      Uložit konverzní lístek

Obrázek 4: *Potvrzení o odeslání dokumentu ke konverzi* (zdroj [www.datoveschranky.eu](http://www.datoveschranky.eu))

**Konverze z listinné do elektronické podoby** - listinu, kterou chce uživatel konvertovat, přinese na pracoviště Czech POINTu. Tady se provádí autorizované konverze za pomoci skeneru. Subjekt, který konverzi provedl, opatří výstup svou uznávanou elektronickou značkou nebo elektronickým podpisem a připojí také časové razítko. Výstup je předáván buďto na CD/DVD nebo je zaslán do tzv. Úschovny - úložiště konvertovaných dokumentů, kde si jej zákazník kdykoliv později vyzvedne.

Provedení autorizované konverze je **zpoplatněno**. Za každou započatou stránku je účtováno 30 Kč. Pokud bude konverze prováděna zastupitelským úřadem, činí tento poplatek 100 Kč za každou započatou stranu.

Zákon také pamatuje na případy, kdy nelze konverzi z různých důvodů provést. **Konverze se neprovádí**, pokud je dokument v jiné než listinné podobě či v podobě datové zprávy, nebo pokud je dokument zasláný datovou zprávou zvukový nebo audiovizuální záznam.

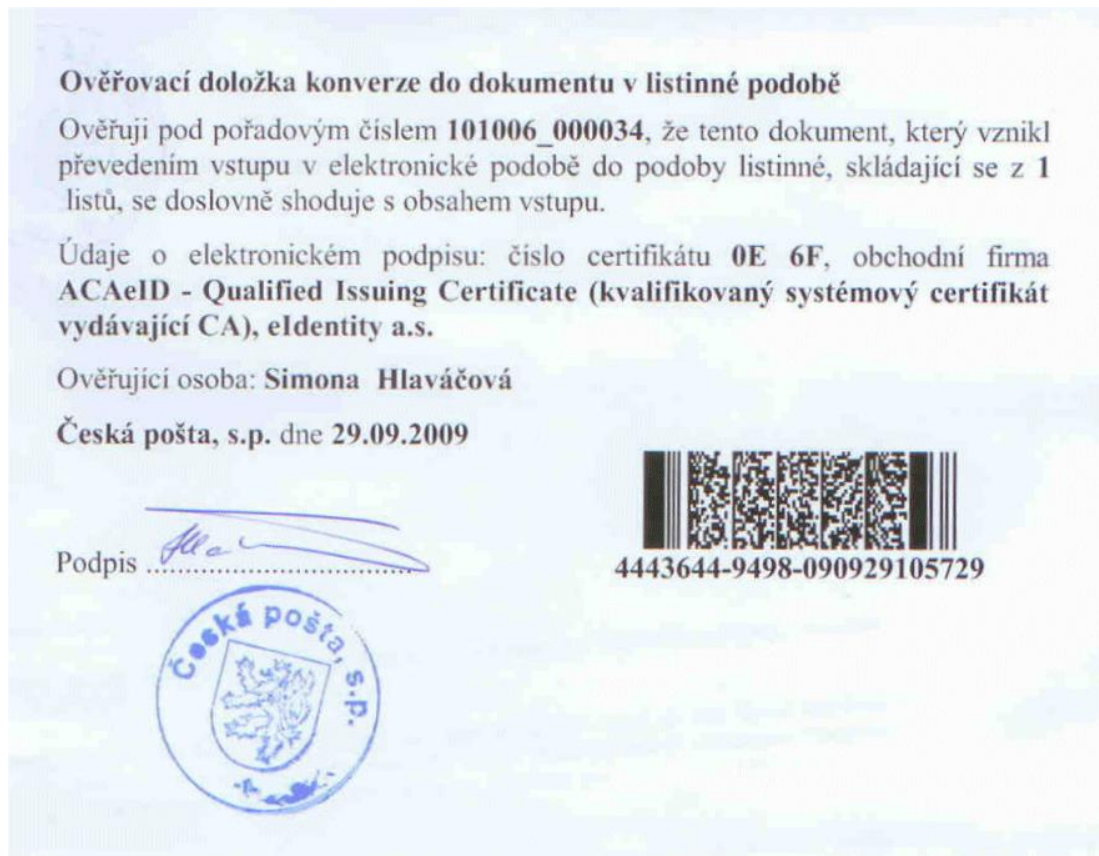
Také některé dokumenty listinné podoby nelze nahradit konverzí. Jedná se např. o občanský průkaz, cestovní doklad, zbrojní průkaz, řidičský průkaz, vojenskou knížku, služební průkaz, průkaz o povolení k pobytu cizince, rybářský lístek, lovecký lístek nebo jiný průkaz, vkladní knížku, šek, směnku nebo jiný cenný papír, los, sázenku, geometrický plán, rysy a technické kresby. Věrohodnost dokumentu také snižují případné změny, doplňky, škrty v něm uvedené. I v tomto případě nelze konverzi provést. Pokud není zřejmé, zda listina, určena ke konverzi, je prvopis, vidimovaný dokument, opis nebo kopie pořízena ze spisu nebo stejnopis písemného vyhotovení rozhodnutí anebo výroku rozhodnutí vydaného podle právního předpisu, podle zákona ji nelze konvertovat. Stejně tak nelze konvertovat i listiny opatřeny plastickým textem či plastickým razítkem. V případě konverze „na žádost“ nebude tato vyhotovena, pokud nebyl dokument v datové zprávě podepsán uznávaným elektronickým podpisem či uznávanou elektronickou značkou.

### 3. Pojem ověřovací doložka a její význam

S pojmem autorizované konverze úzce souvisí také pojem „ověřovací doložka“. Je nezbytnou součástí konverze dokumentu a obsahuje informace vztahující se k jejímu provedení. Obsahem ověřovací doložky je název subjektu, pořadové číslo, údaj o ověření, datum vyhotovení a další náležitosti, které uvádíme rozděleně podle druhu ověřovací doložky v tabulce č. 4. Názorně pak pro ověřovací doložku konverze do dokumentu obsaženého v datové zprávě na obrázku č. 5 a ověřovací doložku konverze do dokumentu v listinné podobě na obrázku č. 6.

Ověřovací doložka konverze do dokumentu obsaženého v datové zprávě	Ověřovací doložka konverze do dokumentu v listinné podobě
název subjektu, který konverzi provedl	název subjektu, který konverzi provedl
pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí	pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí
údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu,	údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu
údaj o tom, z kolika listů se skládá vstup,	údaj o tom, z kolika listů se skládá výstup
údaj o tom, zda vstup obsahuje vodoznak, reliéfní tisk nebo embossing, suchou pečeť nebo reliéfní ražbu, opticky variabilní prvek nebo jiný zajišťovací prvek	datum vyhotovení ověřovací doložky
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,
jméno, případně jména, a příjmení osoby, která konverzi provedla	datum a čas uvedené v kvalifikovaném časovém razítku, číslo kvalifikovaného časového razítka a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal, <b>byl-li vstup kvalifikovaným časovým razítkem opatřen,</b>
	otisk úředního razítka, jméno, popřípadě jména, příjmení a podpis osoby, která konverzi provedla

Tabulka 4: Náležitosti ověřovací doložky

Obrázek 5: *Ověřovací doložka do dokumentu v listinné podobě* (zdroj [www.lupa.cz](http://www.lupa.cz))Obrázek 6: *Ověřovací doložka konverze do dokumentu obsaženého v datové zprávě* (zdroj [www.lupa.cz](http://www.lupa.cz))

Ověřit autenticitu vydané autorizované konverze lze v Centrálním *úložišti ověřovacích doložek* na adrese <https://www.czechpoint.cz/overovacidolozky/search.do>.

## 2. Elektronický podpis, certifikáty a elektronické razítko

S užíváním datové schránky je neodmyslitelně spjat *elektronický podpis*, který je jedním z nástrojů bezpečné elektronické komunikace. V současné době je elektronický podpis založen na kombinaci kryptografických metod. Důležitým faktorem pro bezpečnost el. podpisu je délka šifrovacích klíčů, typy algoritmů, kvalita nosiče a ochrany klíčů (např. čipová karta), způsob implementace a mnoho dalších.

V České republice byl zákon o elektronických podpisech přijat v roce 2000. Ten definuje elektronický podpis jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. (8)

Na vyšší stupeň pak řadíme tzv. *zaručený elektronický podpis*. V praxi můžeme použít srovnání zaručený elektronický podpis = notářsky ověřený podpis a elektronický podpis = prostý podpis bez ověření.

Nezbytnou součástí systému, který využívá elektronický podpis je poskytovatel certifikačních služeb, tzv. certifikační autorita, vydavatel *certifikátů*. Ve své nejjednodušší formě obsahují certifikáty data pro ověření elektronického podpisu, identifikační údaje zajišťující nezaměnitelnost držitelů certifikátu a označení autority, která certifikát vydala. Tato certifikační autorita garantuje jedinečnost subjektů podle užití identifikace subjektu. V České republice jsou 3 akreditované certifikační autority, které jsou kvalifikovány pro vydávání kvalifikovaných certifikátů, vydávání kvalifikovaných systémových certifikátů a vydávání časových razítek. Jsou to První certifikační autorita, a.s., Česká pošta, s.p. a eidentity a.s. .

Proces tvoření certifikátu můžeme rozdělit do šesti dílčích kroků:

1. generování klíčů – potenciaální žadatel si sám pomocí dostupného softwarového vybavení vygeneruje dvojici klíčů.
2. příprava identifikačních dat a žádosti – žadatel sdělí své identifikační údaje a vyplní příslušný formulář
3. předání žádosti – certifikační autority mají svá kontaktní místa tzv. „registrační autority“, kam žadatel předá údaje nutné k vydání certifikátu

4. ověření informací – certifikační autorita si ověří, zda může žadateli certifikát vydat.
5. tvorba certifikátu – certifikační autorita vytvoří digitální dokument a ten podepíše svým privátním klíčem.
6. předání certifikátu – po dohodě je certifikát žadateli předán, zaslán či zveřejněn. V případě zveřejnění se připojuje informace o platnosti a stavu, což zvyšuje bezpečnost a důvěru jeho užívání.

Stejně bezpečnostní atributy jako kvalifikovaný certifikát nese tzv. *časové razítko*. Kvalifikované časové razítko prokazuje existenci elektronického dokumentu v čase. Jediným vydavatelem je TSA (Time Stamp Authority).

## 7. INFORMAČNÍ SYSTÉM DATOVÝCH SCHRÁNEK

### 1. Legislativa a provozovatel

Informační systém datových schránek (dále jen ISDS) je z právního hlediska definován v zákoně 300/2008 Sb. jako informační systém sloužící pro výkon veřejné správy.

Podle zákona o informačních systémech veřejné správy (Zákon č. 365/2000 Sb.) je správcem informačního systému veřejné správy Ministerstvo vnitra ČR, které za celý systém dopovídá. Ministerstvo podle zákona určuje účel a prostředky zpracování informací.

Informační systém se také řídí zákonem č. 101/2000 Sb. o ochraně osobních údajů.

Provozovatelem ISDS je *Česká pošta, s. p.*, který je určen přímo ustanovením zákona č. 300/2008 §14 odst. 2. Provozovatel provádí alespoň některé informační činnosti, které souvisejí s informačním systémem. Informačními činnostmi rozumíme získávání a poskytování informací, reprezentace informací dat, shromažďování, vyhodnocování, ukládání, uchovávání, vyhledávání, úpravu či pozměňování dat, předávání dat a jejich šíření, zpřístupňování, výměna třídění nebo kombinování, blokování a likvidace dat. Informační činnost je prováděna správcem, provozovatelem a uživateli IS a to za pomoci technických a programových prostředků.

### 2. Obsah ISDS

Informační systém datových schránek (dále jen ISDS) je informační systém veřejné správy, který zajišťuje bezpečnou a průkaznou elektronickou komunikaci mezi orgány veřejné moci na straně jedné a fyzickými a právníckými osobami na straně druhé jakož i mezi orgány veřejné moci navzájem. (9)

V informačním systému datových schránek se vedou tyto informace o datových schránkách: identifikátor datové schránky, datum zřízení, zpřístupnění, znepřístupnění a zrušení datové schránky, datum přihlášení, datum odeslání dokumentu nebo provedení úkonu z datové schránky. Všechny časové údaje jsou uvedeny s přesností na hodiny, minuty a sekundy.

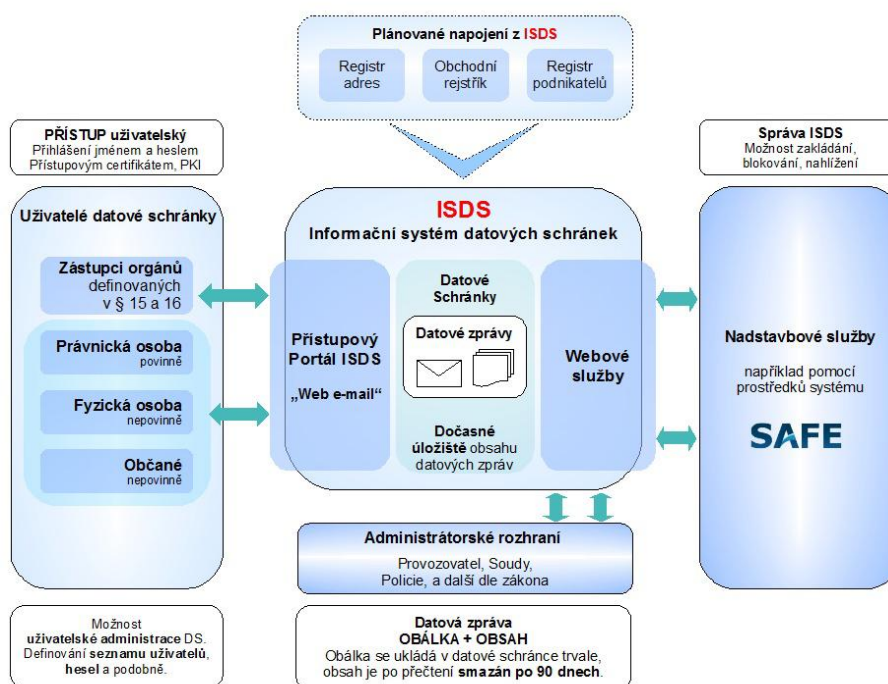
Dále jsou zde uvedeny údaje jména, příjmení, data a místa narození, adresa místa trvalého pobytu nebo jiného pobytu na území České republiky, také jméno a příjmení, popřípadě obchodní firma podnikající fyzické osoby, pro niž byla zřízena datová schránka, datum a místo jejího narození, adresa místa trvalého pobytu u občanů České republiky, místo, kde

má povolení k pobytu nebo k trvalému pobytu v České republice, včetně uvedení adresy, a adresa bydliště v cizině, jde-li o cizince, adresa bydliště v členském státě Evropské unie, ve kterém je usazen, jde-li o státního příslušníka členského státu Evropské unie, který nemá povolení k pobytu nebo k trvalému pobytu v České republice, místo podnikání a identifikační číslo osoby, bylo-li přiděleno,

Dále potom obchodní firma nebo název právnické osoby, pro niž byla zřízena datová schránka, sídlo a identifikační číslo osoby, bylo-li přiděleno. Název a sídlo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro kterou byla zřízena datová schránka, název orgánu veřejné moci, pro nějž byla zřízena datová schránka, sídlo a identifikační číslo osoby, bylo-li přiděleno,

ISDS vede také údaje o osobách oprávněných k přístupu do DS - jméno, popřípadě jména, příjmení, datum narození, adresa místa trvalého pobytu nebo jiného pobytu na území České republiky anebo adresa bydliště mimo území České republiky, rozsah přístupu a datum vzniku a zániku oprávnění k přístupu do datové schránky. Také nechybí údaje o administrátorovy - jméno, popřípadě jména, příjmení, datum narození, adresa místa trvalého pobytu nebo jiného pobytu na území České republiky anebo adresa bydliště mimo území České republiky.

V systému je uložena elektronická adresa nebo obdobný údaj pro vyrozumění o dodání datové zprávy do datové schránky, popřípadě kontaktní adresa, na niž má být adresátu doručováno; seznam kontaktních adres, u nichž byl dán souhlas k jejich zveřejněním.



Obrázek 7: Blokové schéma ISDS (zdroj [www.aipsafe.cz](http://www.aipsafe.cz))

### 3. Neveřejné údaje v ISDS

Údaje, které jsou vedené v ISDS jsou označeny za *neveřejné* a nelze je poskytnout jiným osobám. Výjimkou je kontaktní adresa, kterou může držitel datové schránky označit jako veřejnou.

Existují také případy, kdy jsou i neveřejné údaje poskytovány třetím osobám. Správci systému mohou zpracovávat informace nad rámec systému. Tyto informace mohou být poskytovány správním orgánům nebo soudům a to v souvislosti s vedením konkrétního případu.

Ministerstvo vnitra ČR je oprávněno k přístupu některých údajů za účelem správy informačního systému datových schránek v souladu se zákonem o evidenci obyvatel a rodných čísel. Má přístup k těmto údajům o státních občanech ČR: jméno (popřípadě jména), příjmení (změna příjmení), rodné příjmení, datum, místo a okres narození. U občana, který se narodil v cizině pak místo a stát. Dalším z údajů je rodné číslo, adresa trvalého bydliště a v neposlední řadě také údaj o zbavení nebo omezení způsobilosti k právním úkonům, datum úmrtí nebo datum rozhodnutí soudu o prohlášení za mrtvého.

Údaje jména a příjmení, rodného čísla popř. data narození jsou vedeny v systému o cizincích, kteří jsou matkou, otcem, jiným státním zástupcem, manželem, registrovaným partnerem nebo dítětem občana ČR.

Výše uvedené údaje jsou využívány především pro ověřování údajů vedených v informačním systému.

Ministerstvu vnitra jsou také poskytovány informace souvisejícím se zřízením, zrušením nebo znepřístupněním datových schránek, kde k těmto úkonům dochází ze zákona. Ministerstvo spravedlnosti poskytuje informace o zápisu, vedení nebo výmazu osoby ze seznamu insolvenčních správců, soud poskytuje údaje vedené v obchodním rejstříku, Česká advokátní komora o zápisu i výmazu osoby do seznamu advokátů. Notářská komora poskytuje údaje o zápisu a výmazu osob vedených v seznamu notářů. Exekutorská komora údaje ze seznamu soudních exekutorů, Komora daňových poradců údaje ze seznamu daňových poradců a správní orgán vedoucí evidenci podnikajících fyzických osob nebo právnických osob údaje z této evidence.

## **PRAKTICKÁ ČÁST**

## 8. SOUČASNÉ ŘEŠENÍ

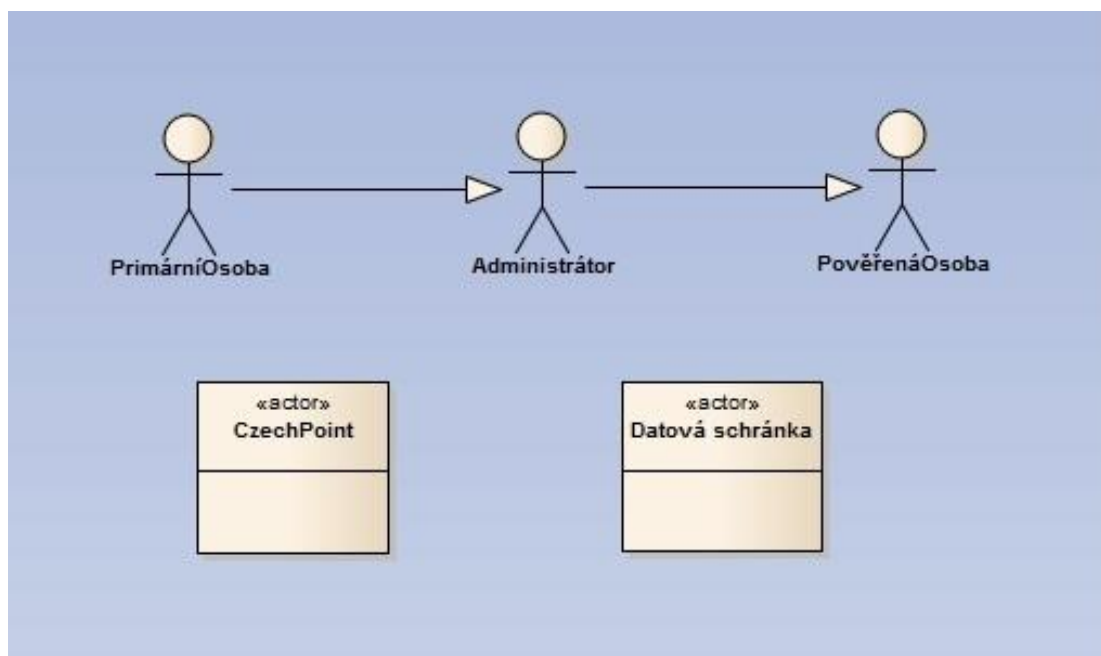
Následující část práce se zabývá analýzou informačního systému datových schránek, která byla vypracována metodou zpětného inženýrství. Popsané modely byly vytvořeny pomocí nástroje Enterprise Architect od společnosti Sparx Systems. Use Case modely jsou pro větší přehlednost rozděleny do čtyř balíků. Jednotlivé případy užití byly dále dekomponovány pomocí aktivitních diagramů.

### 1. Aktéři

Aktéři vystupující v rámci ISDS jsou:

1. Primární osoba
2. Administrátor
3. Pověřená osoba
4. Czech POINT
5. Datová schránka

Role jednotlivých aktérů byly popsány v teoretické části této práce, a tudíž se jimi nebude dále zabývat. Pro lepší představu hierarchie uživatelů uvádíme následující obrázek č. 7.



Obrázek 8: Aktéři

## 1. Případy užití (Use Case)

### 1. Přihlášení k ISDS

Pro správný chod ISDS je nutné nejdříve nainstalovat software 602XML Filler, který slouží k vykreslování a vyplňování formulářů a také ručně prohlásit za důvěryhodný certifikát obdrženy od certifikační autority (CA), jelikož žádná z českých CA dosud nesplnila podmínky pro zařazení do skupiny WebTrust. O nešťastnosti tohoto řešení budeme mluvit níže.

Pro samotné přihlášení k datové schránce může v současném řešení uživatel využít hned několik možností. Jsou to:

1. Přihlášení k ISDS pomocí jména a hesla
2. Přihlášení pomocí SMS kódu
3. Přihlášení pomocí bezpečnostního kódu
4. Přihlášení pomocí certifikátu

Přihlášení pomocí jména a hesla, doplněné o zadání kódu z obrázku, představuje základní způsob autentizace do systému datových schránek. Uživatel zadá své ID, které obdržel při aktivaci datové schránky a aktuální heslo. Dále opíše kód z obrázku pro ověření, že údaje neodesílá stroj a nejde tedy o virtuální útok. Systém následně ověří platnost zadaných informací, a pokud je vše v pořádku, přihlásí uživatel do systému. Je to základní způsob přihlašování, který s sebou nese řadu bezpečnostních rizik, a proto je vhodné použít rozšířené možnosti přihlašování. Všechny z rozšířených možností taktéž využívají ID a heslo uživatele, ale přidávají navíc vlastní zabezpečovací mechanismy. Úvodní přihlašovací stránka ISDS je zobrazena na obrázku č. 8.

**datové schránky** INFOLINKA: 270 005 200

**Přihlášení**

Uživatelské jméno (ID osoby):

Heslo:



Opište kód z obrázku

[Jste zde poprvé? »](#)  
[Nemůžete se přihlásit? »](#)  
[Nápověda »](#)

**PŘIHLÁSIT**

**DATOVÉ SCHRÁNKY**  
Datové schránky jsou informační systém veřejné správy zřízený podle zákona 300/2008 Sb.

**DALŠÍ MOŽNOSTI PŘIHLÁŠENÍ**

[CERTIFIKÁTEM >>](#)  
[SMS KÓDEM >>](#)  
[BEZPEČNOSTNÍM KÓDEM >>](#)

 MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY

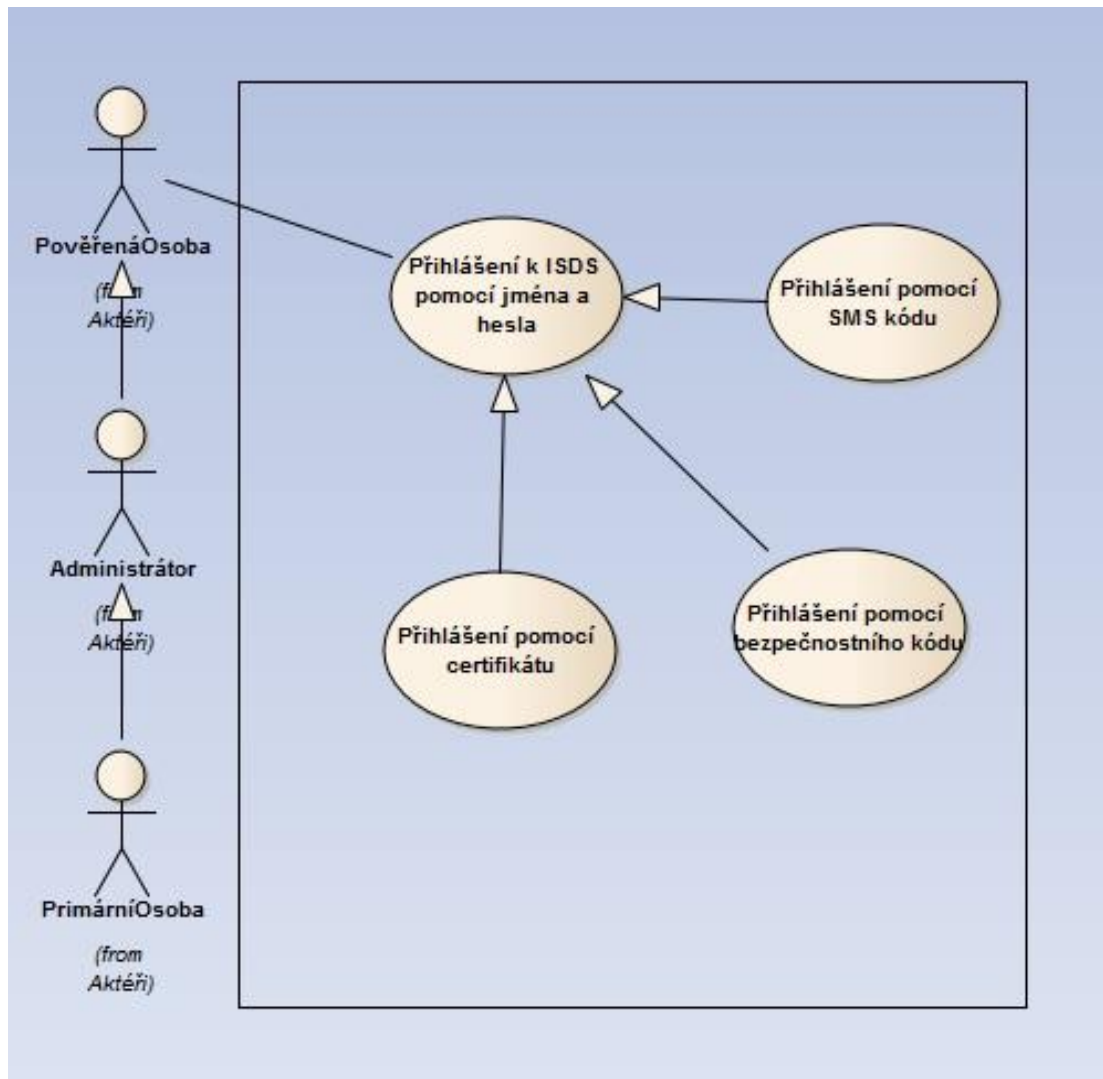
 Česká pošta

Správce: Ministerstvo vnitra České republiky; Provozovatel: Česká pošta s. p. [Ochrana osobních údajů](#) | [Prohlášení o přístupnosti](#)

Obrázek 9: Přihlašovací stránka

Jednou z možností rozšířeného přihlašování je využití jednorázových SMS kódů. Po zaregistrování mobilního telefonu uživatel vždy na dotaz obdrží prostřednictvím SMS jednorázový, časově omezený kód pro přihlášení do systému. Tento způsob přihlašování je ale bohužel zpoplatněn a tudíž většina uživatelů vlastnicích tzv. chytrý telefon dnes spíše volí variantu bezpečnostního kódu. Tato metoda je podobná té, která je uvedena výše, s tím rozdílem, že uživatel musí nejdříve do svého telefonu nainstalovat aplikaci pro generování kódů (token) a následně ji synchronizovat se svou datovou schránkou prostřednictvím šestnáctimístného hexadecimálního kódu. Poté opět při přihlašování použije vygenerovaného jednorázového a časově omezeného kódu.

Poslední možností rozšířeného přihlašování je zakoupení a instalace certifikátu CA. Tato varianta s sebou opět nese břímě zpoplatnění a navíc je řešení nevýhodné kvůli svázání s pouze jedním počítačem, na kterém je certifikát nainstalován. Uplatnění ovšem najde v případě, že uživatel chce využívat aplikací třetích stran a hostovaných spisových služeb. Use case model možností přihlašování je zobrazen na obrázku č. 9.



Obrázek 10: Přihlášení k DS

### 1. Nastavení datové schránky

Nastavení datové schránky je jedním z klíčových aspektů užívání.

Podívejme se tedy podrobněji na jednotlivé možnosti.

Změna hesla – uživatel má možnost nastavit si vlastní heslo, které ale z důvodu zabezpečení musí odpovídat požadavkům provozovatele. Daný formulář včetně požadavků vypadá následovně (obr. č. 9).



INFOLINKA: 270 005 200

**Změna hesla**

Uživatelské jméno:  
aamaw4

Staré heslo:

Nové heslo:

Opakujte nové heslo:

#### ZMĚNA HESLA DO DATOVÉ SCHRÁNKY


Heslo do datové schránky musí být minimálně 8 a maximálně 32 znaků dlouhé, musí obsahovat minimálně jedno velké písmeno, jedno malé písmeno a jedno číslo. Věnujte pozornost upozornění pod polem pro vložení nového hesla, které Vám oznámí, kdy je nové heslo dostatečně bezpečné.

**Nové heslo musí být jiné než kterékoliv dříve použité heslo.**

Povolené znaky jsou písmena (a-z, A-Z), číslice (0-9) a speciální znaky (! # \$ % & ( ) \* + , - . : = ? @ [ ] \_ { } ~).

Pro větší bezpečnost doporučujeme vytvořit heslo skládající se z více malých i velkých písmen, číslic a speciálních znaků.

Heslo nesmí obsahovat údaje datové schránky. Například nesmí obsahovat příjmení, id schránky, id uživatele atd. Heslo typu 12345, qwerty, asdfg je příliš jednoduché, není dostatečně bezpečné a proto není povoleno.

Vyšší bezpečnosti při vkládání hesla dosáhnete použitím tzv. grafické klávesnice. Ta zabraňuje případnému „odposlechu“ stisknutých kláves pomocí útočných programů. Grafickou klávesnici zobrazíte kliknutím na ikonku:  Po otevření grafické klávesnice se vedle polí pro zadávání hesla objeví označovač výstupu grafické klávesnice. Označovačem aktivujete pole, do kterého se bude grafickou klávesnicí vyplňovat heslo. Heslo pak vyfukujete myší na grafické klávesnici. Velká písmena a speciální znaky (např. @, #, \$, %, ...) můžete vkládat po kliknutí na klávesu Shift. Po vyplnění všech hesel grafickou klávesnicí zavřete a klikněte na tlačítko Změnit heslo. Špatně napsaný znak můžete smazat pomocí klávesy Back. Pro zvýšení bezpečnosti se grafická klávesnice zobrazuje vždy na jiném místě a v jiné velikosti. Grafickou klávesnicí využijete i v případě, že Vaše heslo obsahuje speciální znaky, u kterých si nejste jistí, jak se píšou.

Správce: Ministerstvo vnitra České republiky, Provozovatel: Česká pošta, s. p.

Obrázek 11: Změna hesla

Nastavení platnosti hesla – heslo je opět z důvodu bezpečnosti implicitně nastaveno na expiraci po 90-ti dnech. Jelikož si na toto nastavení množství uživatelů stěžovalo, došlo k implementování možnosti vypnout expirování hesla. Uživatel má tak možnost výběru, který scénář chce používat.

Nastavení upozornění e-mailem – uživatel má možnost nastavit si bezplatné notifikace na zvolenou e-mailovou adresu a to při následujících situacích:

1. přijetí nové zprávy
2. přijetí nové zprávy do vlastních rukou
3. nebylo-li možné zprávu odeslat (např. virus v zásilce)
4. v případě aktivní služby Datový trezor navíc ještě upozornění na konec předplatného nebo zaplnění datového trezoru

Nastavení upozornění na nové zprávy pomocí SMS – je obdobná služba jako e-mailové notifikace, s tím rozdílem, že tato je zpoplatněná. Uživatel může zvolit zaslání SMS při stejných případech, které jsou popsány výše. Navíc může zvolit frekvenci zasílaných upozornění a to následovně:

1. posílat upozornění ihned pro každou zprávu
2. posílat upozornění jednou denně jako sumární výpis

Nastavení notifikace expirace certifikátu – je jedna z nových funkcí systému. Pokud má uživatel aktivní upozornění e-mailem, zároveň ho systém automaticky prostřednictvím e-mailové zprávy, upozorní na expiraci zaregistrovaného certifikátu a to 12 dní předem, aby měl uživatel čas certifikát obnovit.

Nastavení poštovní datové zprávy – Poštovní datová zpráva (PDS) je komerční služba, prostřednictvím které lze zasílat datové zprávy mezi datovými schránkami fyzických osob, podnikajících fyzických osob a právnických osob navzájem. Aktivace těchto zpráv je možná prostřednictvím Czech POINTu. Bohužel v současném řešení není implicitně zapnuto ani přijímání těchto zpráv (které je zdarma) a tudíž pokud chce uživatel službu využívat, musí si svou datovou schránku pro příjem PDS explicitně nastavit.

Přidání uživatele – jak už víme, primární osoba datové schránky může zplnomocnit tzv. pověřenou osobu či administrátora (viz kapitola 2.5). Toto přidání je možné provést v nastavení DS s tím, že musíme vyplnit všechny povinné údaje o novém uživateli (tj. jméno, příjmení, rodné číslo a adresa trvalého bydliště) a můžeme mu nastavit následující práva:

1. číst zprávy
2. číst všechny zprávy
3. vytvářet zprávy
4. prohlížet seznamy zpráv
5. vyhledávat datové schránky

Editování uživatele – pokud má uživatel nastavena potřebný typ oprávnění, může editovat práva ostatních aktérů. Navíc je tu možnost editace vlastní kontaktní adresy.

Smazání přidaného uživatele – obdobně jako u editování, může uživatel za předpokladu vlastnění potřebných práv smazat jiného aktéra přiřazeného k DS.

Spravování certifikátů – uživatel má možnost zaregistrovat či smazat uživatelský nebo systémový certifikát, případně certifikát hostované spisové služby. Certifikáty je možno získat na nejbližší poště s kontaktním místem Czech POINT.

Nastavení přístupu poskytovatelům služby Hostovaných Spisových Služeb a Aplikací Třetích Stran – v případě úspěšně zaregistrovaného certifikátu hostovaných služeb, může uživatel nastavit svou datovou schránku pro přístup Hostovaných spisových služeb a aplikací třetích stran.

Nastavení funkce Datový trezor – tato funkce je další zpoplatněnou službou v rámci ISDS. V Datovém trezoru (DT) může uživatel zprávy archivovat, filtrovat a dále s nimi pracovat bez obav, že budou z důvodu uplynutí lhůty 90 dnů smazány.

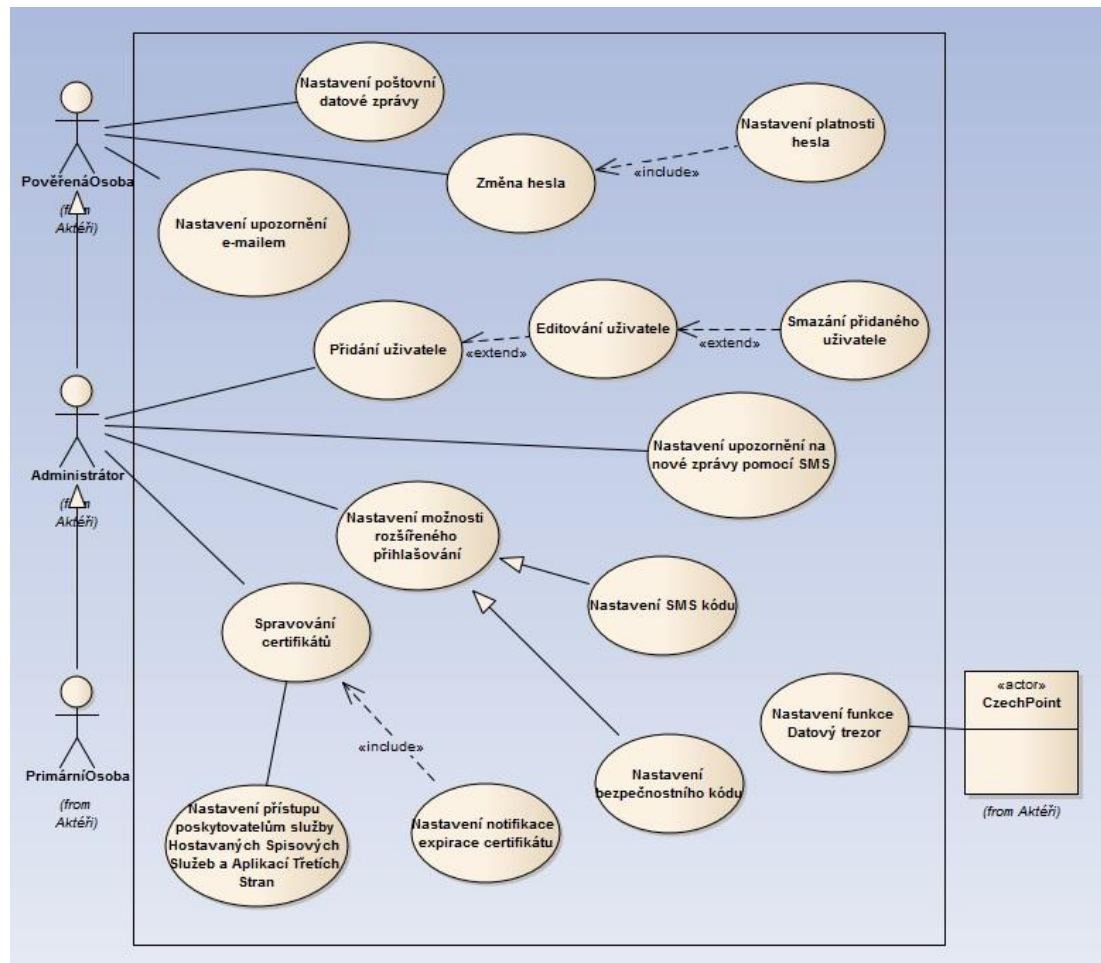
Navíc je DT bezpečným a garantovaným úložištěm, u kterého Česká pošta odpovídá za zabezpečení důvěrnosti a ochrany dat, která jsou uložena v informačních systémech služby Datový trezor. Tato garance je Českou poštou zaručena i pro případ ztráty či poškození zpráv nárokem na úhradu smluvní pokuty na rozdíl od běžných datových úschoven.

Službu Datový trezor je možno zřídit následujícími způsoby:

1. Osobní návštěvou na nejbližší poště s kontaktním místem Czech POINT.
2. Elektronicky bez nutnosti návštěvy pobočky. Na adrese [www.datovy-trezor.cz](http://www.datovy-trezor.cz) si uživatel může objednat nový Datový trezor, případně prodloužit platnost nebo navýšit kapacitu stávajícího Datového trezoru.

Nastavení možnosti rozšířeného přihlašování – v této části má uživatel možnost upravit, případně zrušit rozšířené možnosti přihlašování – pomocí SMS a bezpečnostního kódu (např. změna telefonního čísla, resynchronizace bezpečnostního tokenu, změna požadovaných upozornění, apod.)

Současné uživatelské možnosti nastavení datové schránky ilustruje, následující use case diagram (obr. č. 11).



Obrázek 12: Nastavení DS

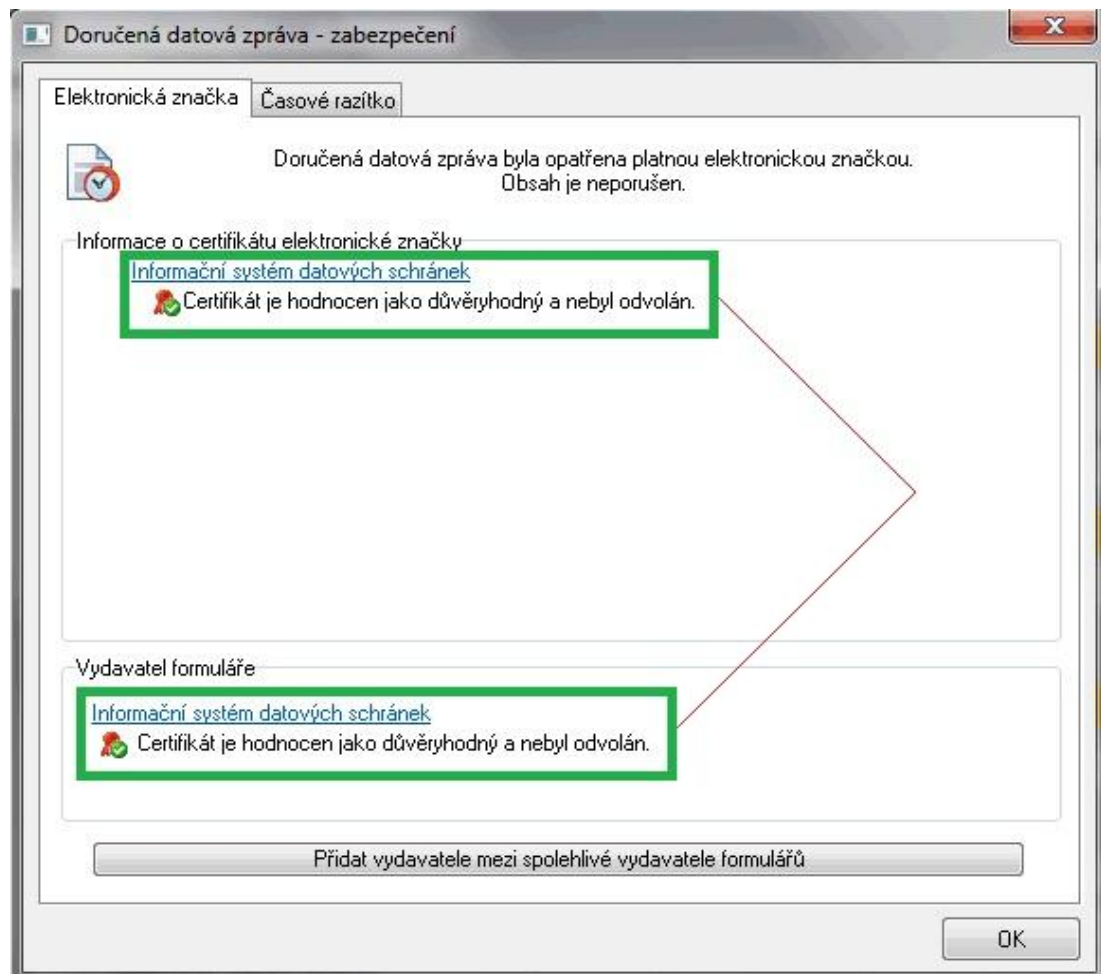
## 1. Práce s datovou zprávou

Práce s datovou zprávou je alfa a omegou celého systému datových schránek. Následující řádky popisují fungování stávajícího systému.

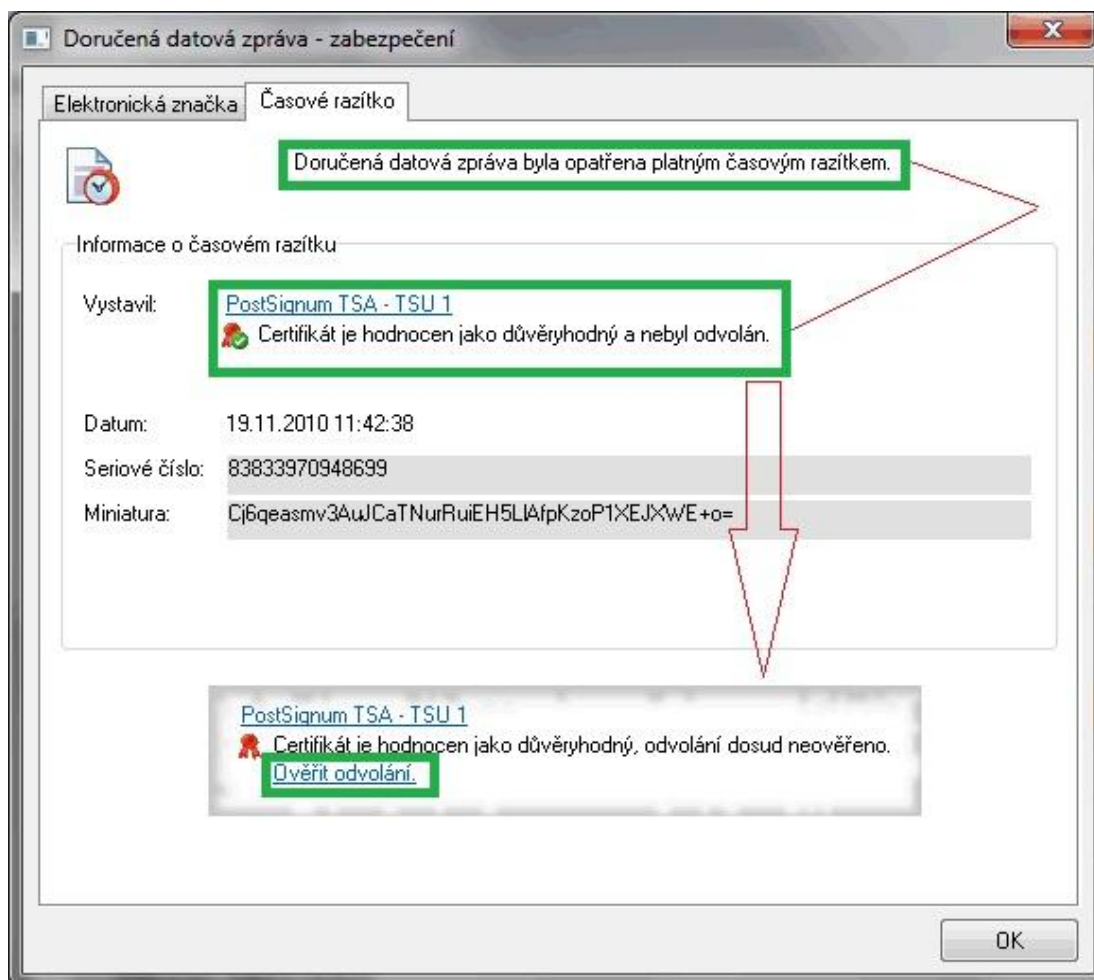
Přijetí datové zprávy – při přijetí datové zprávy systém uloží informace o doručení do logu (datum a přesný čas). Je to jednak z důvodu platnosti zprávy, která je v současném řešení 90 dní (Datová zpráva má trvanlivost „programátorských 90 dní“ – tedy přesně na vteřinu 90 dní od doručení zmizí, což je mnohými označováno za jeden ze zásadních problémů celého systému DS, jelikož „Právnických 90 dní“ ze zákona trvá do půlnoci.) a také z důvodu právnických. Pokud totiž uživatel zprávu obdrží, je ze zákona po 10-ti dnech považována za doručenu i když si ji nepřečte. Aktér je tedy považován za „informovaného“. Právě tímto krokem chtějí zákonodárci předejít nevyzvedávání důležitých zásilek.

Po doručení zprávy následně systém zkontroluje uživatelské nastavení notifikací a případně rozešle potřebná upozornění (e-mail, SMS).

Čtení datové zprávy – po obdržení datové zprávy může uživatel tuto číst, za předpokladu, že má přiřazena potřebná oprávnění. Po otevření datové zprávy systém zobrazí kromě samotné zprávy také informaci o jejím zabezpečení. Tímto je myšlena tzv. *elektronická značka* (obr. č. 12) a *časové razítko* (obr. č. 13).



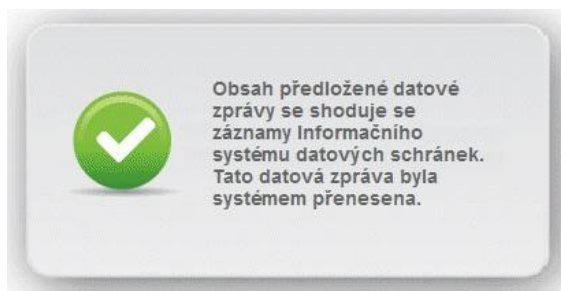
Obrázek 13: *Elektronická značka* (zdroj www.isdstest.cz)



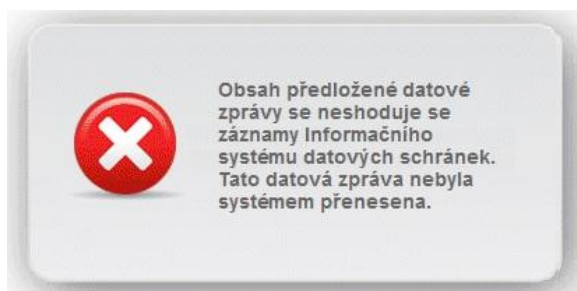
Obrázek 14: Časové razítko (zdroj www.isdstest.cz)

V příloze datové zprávy je potom uložena samotná písemnost, která byla zaslána odesílatel. Příjemce může dále celou datovou zprávu uložit na pevný disk ve formátu *.zfo* (formát softwaru 602XML), případně ji vytisknout. Stejně operace může provést také s příloženou písemností. Dokument v příloze lze také odeslat ke konverzi, která je popsána v kapitole 2.6. Speciálním případem zprávy je *doručenka*, která je taktéž zobrazena v přijatých zprávách.

Ověření datové zprávy – je funkce systému pro ověření pravosti datové zprávy. Uživatel načte do systému datovou zprávu ve formátu *.zfo* a ten následně prověří, zda s touto zprávou nebylo po doručení nepovoleně manipulováno (změna informací apod.). Ověření datové zprávy je provedeno pomocí časových razítek a elektronických podpisů. Po ověření pravosti datové zprávy lze důvěřovat celému jejímu obsahu (obr. č. 14). V opačném případě systém zobrazí chybovou hlášku (obr. č. 15).



Obrázek 15: Platné ověření DS



Obrázek 16: Nepatné ověření DS

Příprava a odesílání datové zprávy – při vytváření nové zprávy musí uživatel nejdřív zvolit příjemce. K jeho vybraní je nabídnuto hned několik možností:

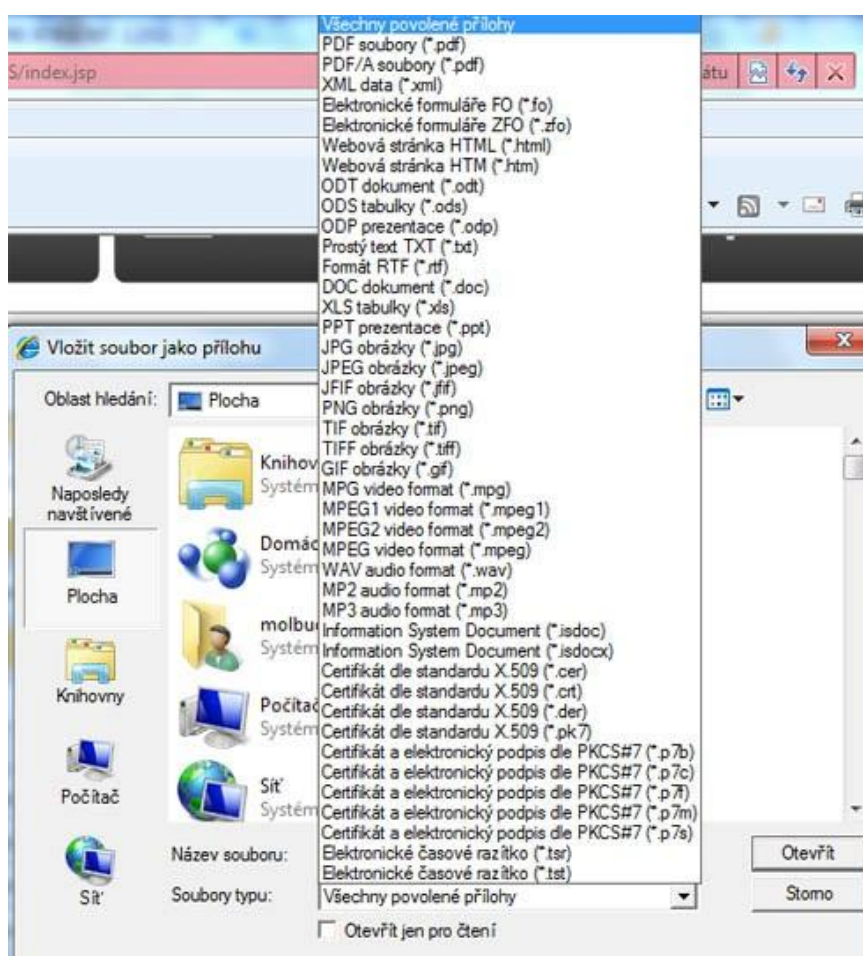
1. Adresování datové zprávy podle ID schránky
2. Adresování datové zprávy podle IČ
3. Adresování datové zprávy podle názvu organizace
4. Adresování datové zprávy z adresáře
5. Adresování datové zprávy ze seznamu posledních adresátů

Při vyhledávání adresátu tedy může uživatel použít ID schránky, identifikační číslo, nebo název organizace. K dispozici je také *rozšířené hledání*, kde je možno doplnit formulář o další položky, jako město, ulici, PSČ, atd. V případě, že ani tak nedojde k nalezení požadovaného adresáta, můžeme využít vyhledávání orgánů veřejné moci na adrese [portal.gov.cz/adresar](http://portal.gov.cz/adresar). Nutno podotknout, že vyhledávání v tomto adresáři funguje na dnešní poměry přinejmenším podivně a bez přesného názvu, ID či IČ je nelezání požadované položky poměrně problematické. V lepším případě má uživatel adresáta již uloženého ve svém adresáři nebo v seznamu posledních adresátů. Potom stačí jen vybrat požadovanou položku a systém vygeneruje novou zprávu s daným adresátem. Dále je nutné vyplnit věc datové zprávy a připojit písemnost(-i). Systém podporuje odesílání celé řady formátů sou-

borů, maximální velikost přílohy je však omezena na 10 MB. Z těch nepoužívanějších jsou to:

1. pdf, xml, html, txt, rtf, doc, xls, ppt, odt
2. jpg, jpeg, png, gif
3. mpg, mp3, mpeg, wav

Kompletní seznam podporovaných formátů ukazuje obr. č. 16.



Obrázek 17: Podporované formáty (zdroj [www.datovestranky.eu](http://www.datovestranky.eu))

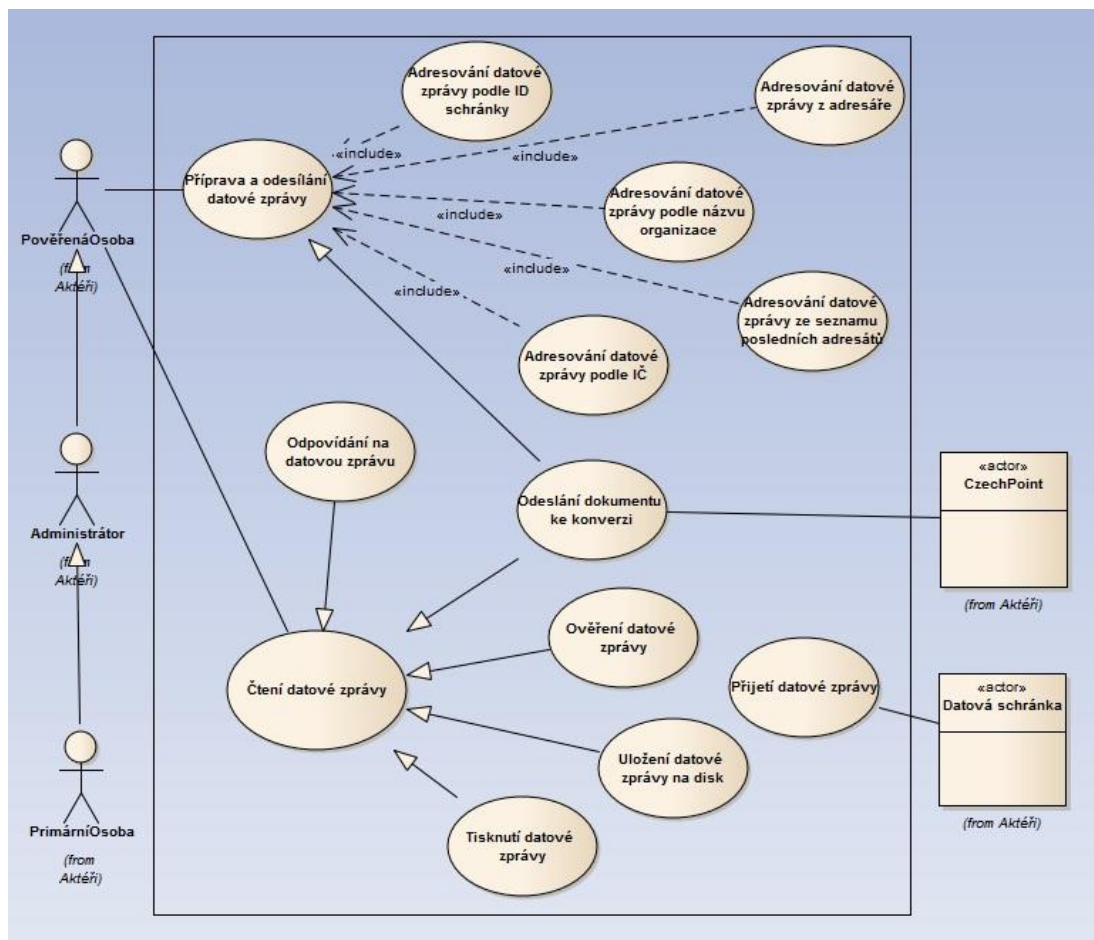
Po novelizaci vyhlášky přibyli ještě formáty následující:

1. docx, xlsx a pptx
2. dwg (AutoCAD DraWinG File Format) verze 2007 a vyšší

3. shp/dbf/shx (ESRI Shapefile)
4. dgn (Bentley MicroStation Format) verze V7 a V8
5. gml (Geography Markup Language Document)

Poté už je zpráva připravena k odeslání. To provede uživatel stiskem tlačítka *Odeslat datovou zprávu*. Je také možné rozepsanou zprávu uložit na disk, případně ji zrušit, čímž ale dojde k její ztrátě. Po odeslání datové zprávy systém uloží do logu datum, čas a ID odesílatele a potvrdí uživateli odeslání. Kromě této možnosti odesílání datové zprávy existuje ještě možnost odpovědět na přijatou datovou zprávu, při které je původní odesílatel automaticky vyplněn jako adresát nové zprávy.

Celkový přehled možností zacházení s datovou zprávu zobrazuje diagram případů užití na obr. č. 17.



Obrázek 18: Práce s DS

## 1. Práce s adresářem

Adresář je momentálně jedno z hlavních úskalí systému ISDS. Je to část systému, která by mohla projít zásadní změnou a jako taková bude také zmíněna v návrzích na zlepšení. Stávající situace je popsána dále.

Přidání adresáta do adresáře – při adresování zprávy, a tedy následném vyhledávání adresáta, má uživatel možnost tohoto přidat do adresáře. Systém uloží požadovaného adresáta do adresáře datové schránky, čímž zjednodušuje budoucí vyhledávání a adresování, které je popsáno v části 4.2.3.

Přejmenování adresáta v adresáři – uživatel má dále možnost přejmenovat adresáta v adresáři. Může to být z důvodů přehlednosti, případně pro snadnější identifikaci požadované položky. Jak ukazuje obr. č. 19, tak např. samotné Brno má celkem pět finančních úřadů (vyhledáno pomocí výše zmíněného adresáře na adrese [portal.gov.cz/adresar](http://portal.gov.cz/adresar)) a tak může být při adresování obtížné zvolit správného adresáta.

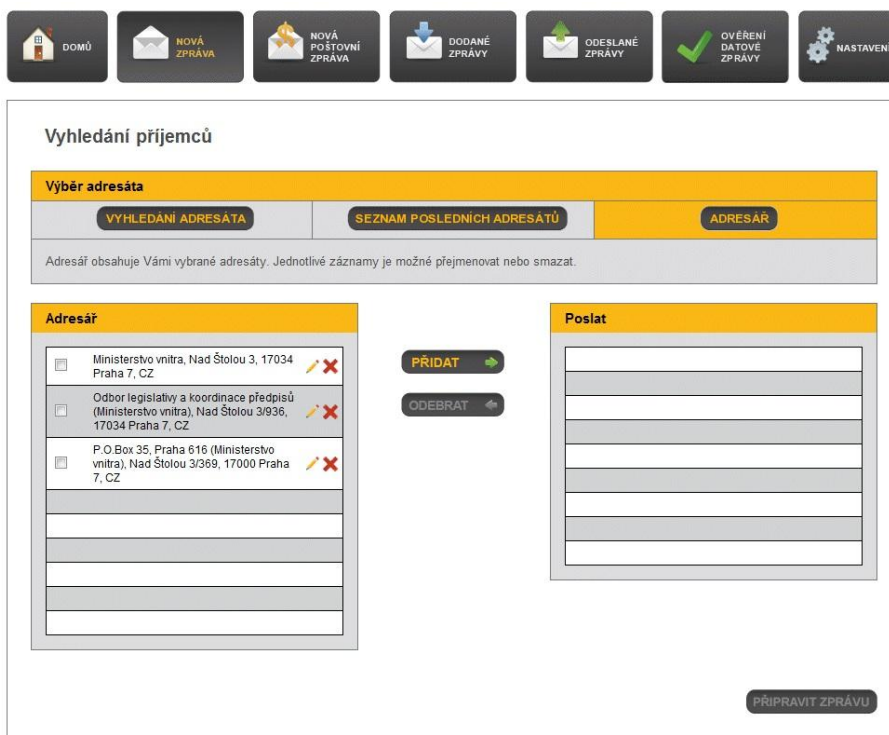
The screenshot shows a search interface with a search bar containing 'finanční úřad brno' and a 'Vyhledat' button. Below the search bar are two dropdown menus: 'podle názvu / jména' and 'Všechny datové schránky'. The search results are displayed in a table-like format with a sidebar on the left containing category links.

Category	Search Results
<a href="#">Orgány územní samosprávy</a>	Nalezeno 5 záznamů.
<a href="#">Orgány státní správy</a>	
<a href="#">Ostatní orgány veřejné moci</a>	
<a href="#">Soudní exekutoři</a>	
<a href="#">Notáři</a>	
<a href="#">Fyzické osoby</a>	
<a href="#">Podnikající fyzické osoby</a>	
<a href="#">Právnícké osoby</a>	
	<a href="#">Finanční úřad Brno I</a> Název subjektu: <b>Finanční úřad Brno I</b> (Jihomoravský)
	<a href="#">Finanční úřad Brno II</a> Název subjektu: <b>Finanční úřad Brno II</b> (Jihomoravský)
	<a href="#">Finanční úřad Brno III</a> Název subjektu: <b>Finanční úřad Brno III</b> (Jihomoravský)
	<a href="#">Finanční úřad Brno IV</a> Název subjektu: <b>Finanční úřad Brno IV</b> (Jihomoravský)
	<a href="#">Finanční úřad Brno-venkov</a> Název subjektu: <b>Finanční úřad Brno-venkov</b> (Jihomoravský)

Obrázek 19: Přejmenování adresáta

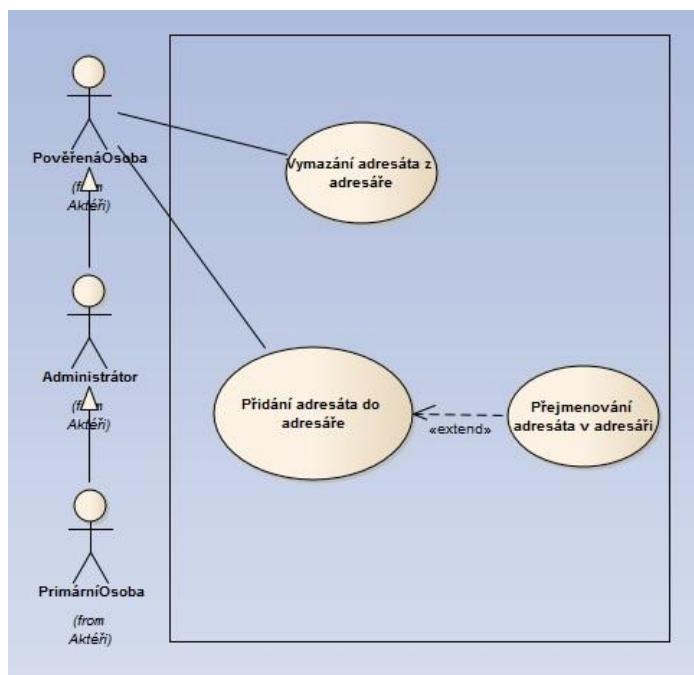
Vymazání adresáta z adresáře – uživatel má samozřejmě také možnost položky z adresáře odstraňovat.

Náhled adresáře ukazuje obr. č. 20.



Obrázek 20: *Vymazání adresáta z adresáře* (zdroj [www.lupa.cz](http://www.lupa.cz))

Celkový náhled na práci s adresářem zobrazuje diagram případů užití na obr. č. 21.



Obrázek 21: *Práce s adresářem*

Současný systém se dá označit jako funkční a je vidět, že od svého nasazení prošel už poměrně dlouhým vývojem. Na jednu stranu je dobře, že se provozovatel snaží systém postupně zlepšovat, na stranu druhou mu bylo hned od začátku vytýkáno spoustu věcí, které by se v alfa verzi objevit neměly (zabezpečení apod.), tím méně, když se týká tak citlivých informací. Na obranu ISDS můžeme říct, že je to systém stále poměrně mladý a tudíž se dají nedostatky předpokládat a s trochou benevolence i odpustit.

## 6. NEDOSTATKY SOUČASNÉHO ŘEŠENÍ

1. Za první nedostatek bych označil užívání softwaru 602XML filler. Vzhledem k celkové funkcionalitě systému nevidím objektivní důvod pro užívání tohoto softwaru. Celý systém by bez problémů mohl běžet jako „čistá“ webová aplikace. I pokud připustíme nutnost použití zvláštního formulářového systému, existuje přece široce podporovaný, rozšířený a používaný formát *pdf*. Užívání tohoto softwaru s sebou navíc nese úskalí v podobě nutnosti administrátorských práv pro uživatele počítače, který chce doplněk instalovat nebo aktualizovat. Tím pádem je prakticky vyloučena nezávislost na vlastním hardware, nemluvě o firmách, které mají vlastní politiky nastavování počítačových uživatelských práv pro své zaměstnance. Za zmínku stojí i ne příliš dobré odladění softwaru v rámci multiplatformního využití. Systém sice v současnosti funguje na všech běžných platformách, nicméně s řadou problémů.
2. Za další nedostatek považuji nešťastně zvolenou adresu pro portál datových schránek. V tomto případě si trůfám tvrdit, že na vině je provozovatel, který nezaregistroval potřebnou doménu před uvedením celého projektu a tudíž došlo k dnes již tradičnímu trendu, kdy si možné domény zaregistrovali lidé za účelem „zbohatnutí“. Navíc jelikož celý projekt běží pod záštitou Ministerstva vnitra České republiky, myslím si, že se dalo s jednoduchostí využít právě domény *gov.cz*. Adresa v této doméně, která je navíc pod kontrolou státu, je již na první pohled daleko důvěryhodnější než stávající *www.mojedatovaschranka.cz*. V souvislosti s datovými schránkami se neustále mluví o bezpečnosti, nicméně toto doménové řešení ve mně vyvolává pocit otevřené náruče směrem k phishingu a podobným útokům.
3. Jako třetí nedostatek bych označil poměrně složité ID, které si musí uživatel pro přihlašování pamatovat, a které není možno změnit. Za vhodnější řešení považuji možnost nastavit alias, jako je tomu například u e-mailových účtů. Uživateli by tento doplněk přinesl možnost pohodlnějšího přihlašování, bez nutnosti zapamatování si složitého přiděleného ID.
1. Dále tu máme ověřování thumbprintu certifikátu, které je v současnosti podle mého názoru zcela nedořešeno. Certifikační autorita PostSignum totiž navrhuje postup, kdy uživatel ověřuje thumbprint na téže stránce, kde samotný certifikát stahuje. Z bezpečnostního hlediska je tedy zcela bezcenný a naopak by se dal prohlásit

za škodlivý, protože dává uživateli falešný pocit bezpečí a navádí k postupu velice snadno zfalšovatelnému.

2. Současný adresář v ISDS je taktéž velkým nedostatkem. Uživatel nemá možnost jakéhokoliv třízení kontaktů do složek. Při větším množství přidaných adresátů se tak adresář stává velmi nepřehledným.
3. Přeposílání zpráv v současném systému není vůbec implementováno. Existuje sice jakási „manuální možnost“ jak zprávu přeposlat, ale toto řešení vnímám jako nedostačující. Uživatel totiž musí nejprve celou datovou zprávu uložit na disk, následně vytvořit zprávu novou a k ní připojit uloženou datovou zprávu. Myslím si, že by bylo daleko vhodnější implementovat přímé přeposílání zprávy, které ušetří jak čas, tak dodatečné úsilí.
1. Následující nedostatek se týká poštovní datové zprávy a tedy komunikace schránkou mimo orgán veřejné moci (soudy, exekutoři a státní úřady). Tato služba je zpoplatněná a druhá strana musí mít povolen příjem, jinak zprávu neobdrží, přestože finanční nároky jsou na straně odesílatele. Osobně považuji za logické, příjem těchto zpráv implicitně zapnout.
2. Dalším trnem v oku pro spoustu uživatelů je 90-ti denní platnost zprávy. V první řadě se jedná o „programátorských“ devadesát dní, a tudíž se zpráva smaže přesně po uplynutí tohoto období, i když zákon definuje lhůtu až do půlnoci. Navíc ve spoustě situací uživatel potřebuje pracovat se zprávou i po uplynutí tohoto období (např. při rozsudku soudu – Když si uživatel dokument nevytiskne a neprovedete konverzi, může se dostat do potíží, jelikož dokument za devadesát dní ze schránky zmizí. V takové situaci si musí na soudu nechat dokument znovu vyhledat). Existuje sice možnost využití služby datového trezoru, která je ovšem zpoplatněná. Za vhodnější řešení bych považoval prodloužení platnosti na jeden rok. Během tohoto období je uživatel schopen vyřídit většinu běžných datových zpráv.
3. Jako poslední v mém výčtu nedostatků bych uvedl systém SMS notifikací. Stávající řešení uživatele pouze upozorní na nově přichozí datovou zprávu, případně datovou zprávu do vlastních rukou. Vhodnější implementace notifikací by zobrazila také odesílatele a případně subjekt této zprávy. Takové řešení by uživateli usnadnilo zhodnocení závažnosti přijaté zprávy a tak i prioritu řešení či reakce.

Předcházející výčet nedostatků zdaleka nepostihuje všechny nedokonalosti stávajícího řešení systému. Je to jen část celku, kterou se budu zabývat na následujících stránkách.

#### 4. NÁVRHY NA VYLEPŠENÍ PRO SYSTÉM ISDS

5. Vynechání systému 602XML – použití běžných webových technologií: HTTP, HTML a JavaScript
6. Přesun na adresu např. [www.schranky.gov.cz](http://www.schranky.gov.cz) (doména gov.cz je pod kontrolou státu a adresy v ní jsou tedy už na první pohled důvěryhodnější)
7. Možnost nastavit alias jako u emailu (jednodušší přihlašování – uživatel si nemusí pamatovat složité ID)
8. Změna ověření thumbprintu certifikátu – Umožnění uživateli ověření certifikátu jiným kanálem:
  1. Vyzvat uživatele k tomu, aby zatelefonoval na infolinku certifikační autority nebo provozovatele datových schránek, kde mu bude thumbprint nadiktován
  2. Zapsat informace včetně thumbprintu přímo do papírových aktivačních instrukcí, které každý uživatel dostává při založení datové schránky
1. Možnost vytvoření vlastních složek v adresáři a možnosti jeho rozšířené úpravy
2. Možnost přeposílání zprávy jako jedna z voleb při čtení přijaté datové zprávy
3. Poštovní datová zpráva – komunikace schránkou mimo orgán veřejné moci – implicitně zapnout příjem těchto zpráv, protože v případě odesílání PDS platí za službu odesílatel.
4. Rozšířená doba platnosti zprávy – rozšířit dobu platnosti zprávy ze stávajících devadesáti dní na 365 dní.
5. Rozšířené oznamování pomocí SMS – odeslaná zpráva SMS bude obsahovat i název odesílatele a subjekt zprávy.
6. Třídění datových zpráv je už ve stávající verzi systému implantováno, ale já jsem ho při prvním návrhu nechtěně přehlédl. Jelikož je ale moje řešení jiné, mohlo by být použito jako doplněk k onomu již funkčnímu, a proto jsem se nakonec rozhodl ho v návrhu ponechat. Stávající řešení totiž počítá s výběrem požadovaného třídění z drop-down menu. Můj návrh řeší třídění kliknutím na název daného sloupce. Domnívám se, že pro lepší a intuitivnější použití by bylo nejlepší sjednocení obou těchto scénářů.

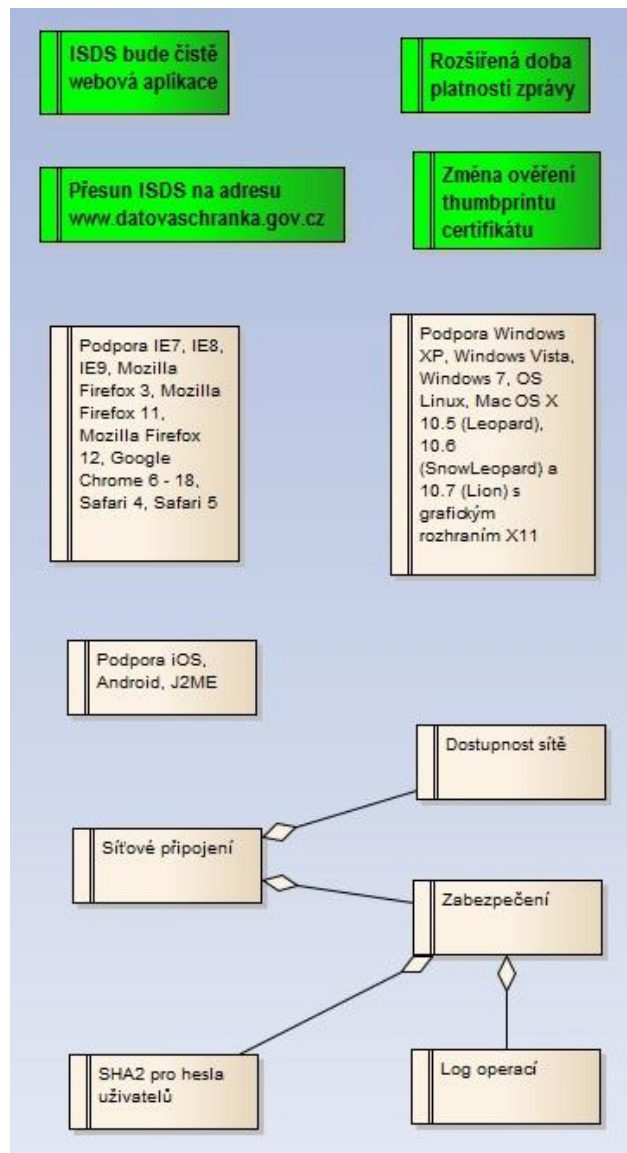
## 7. NAVRHOVANÉ ŘEŠENÍ

Tato část práce se zabývá upravenou analýzou informačního systému datových schránek, která byla vytvořena na základě studie současného stavu a jejího doplnění o návrhy na vylepšení. Nové, případně upravené části systému jsou pro lepší přehlednost zvýrazněny zelenou barvou pozadí. Přidané případy užití byly opět dekomponovány pomocí aktivitních diagramů a doplněny scénáři.

### 1. Požadavky

#### 1. Nefunkční požadavky

Obr. č. 22 zobrazuje souhrn nefunkčních požadavků na systém.



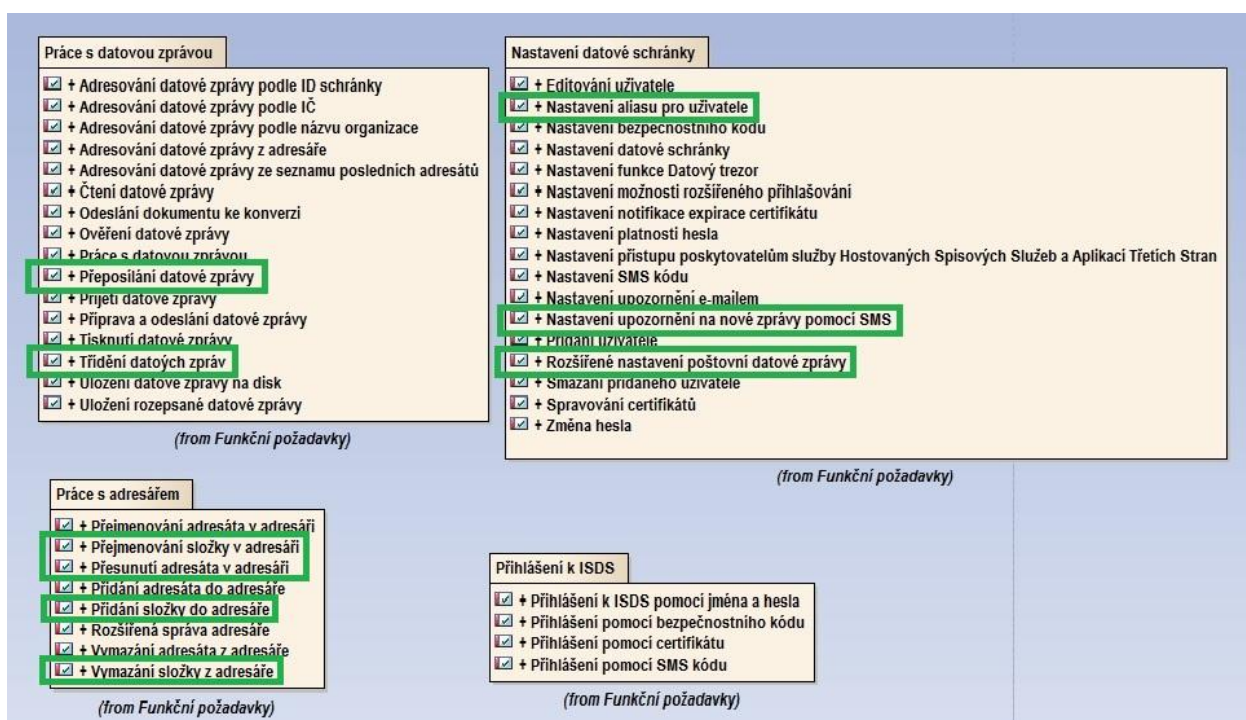
Obrázek 22: Nefunkční požadavky na systém

Nefunkční požadavky na nový systém jsou tedy následující:

1. ISDS bude čistě webová aplikace, která nebude využívat software 602XML. ISDS bude implementován za použití běžných webových technologií: HTTP, HTML a JavaScript
2. ISDS bude přesunut na adresu [www.datovaschranka.gov.cz](http://www.datovaschranka.gov.cz)
3. Doba platnosti zprávy bude rozšířena ze stávajících 90-ti dní na 365 dní
4. Ověření thumbprintu bude možnost provést prostřednictvím operátora na klientské lince a thumbprint bude také součástí papírových aktivačních instrukcí

### 1. Funkční požadavky

Obr. č. 23 z úsporných důvodů zobrazuje pouze souhrnný přehled funkčních požadavků na systém. Jednotlivé diagramy jsou součástí vypracovaného projektu, který je k dispozici na přiloženém CD v souboru datoveSchranky-navrh.eap.

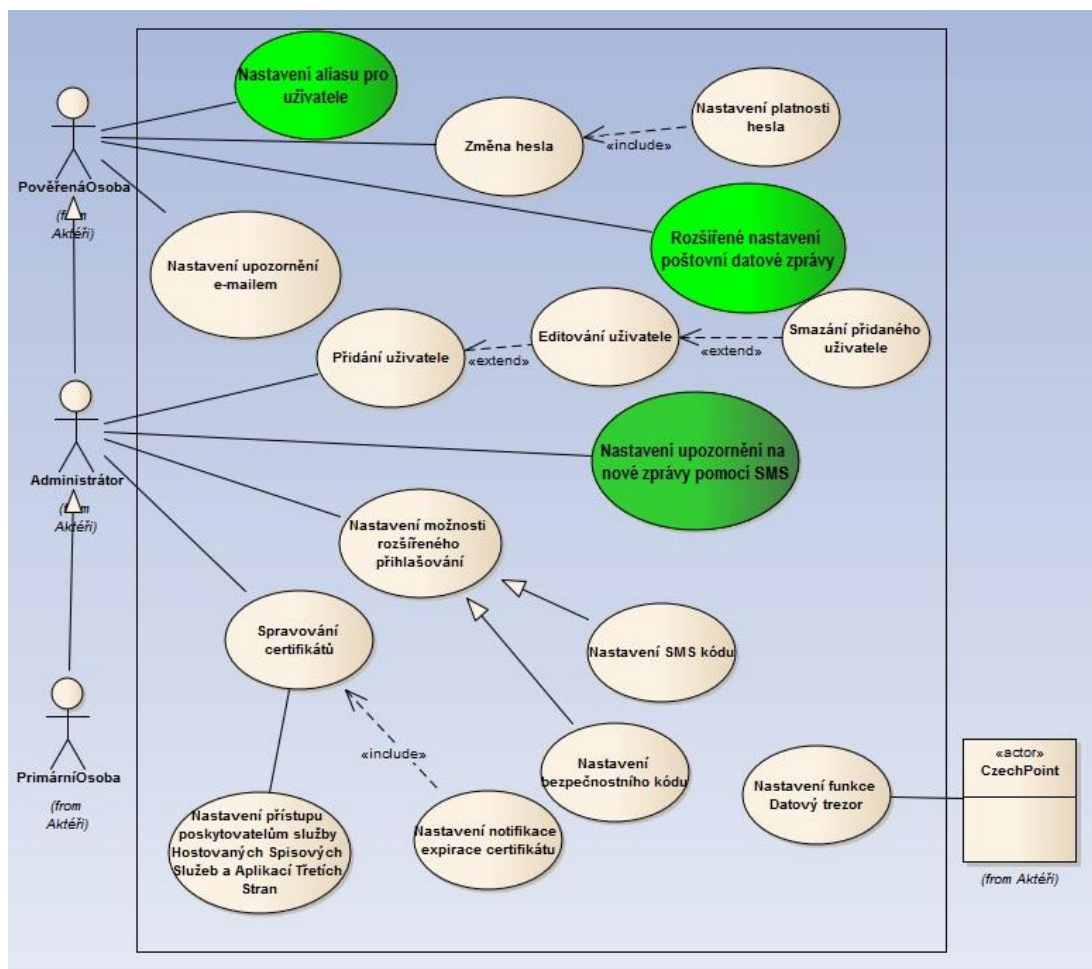


Obrázek 23: Funkční požadavky na systém

## 2. Případy užití (Use Case)

### 1. Nastavení datové schránky

Změny v nastavení datové schránky ilustruje obr. č. 24.



Obrázek 24: Změny v nastavení DS

Nové funkcionality oproti stávajícímu řešení jsou následující:

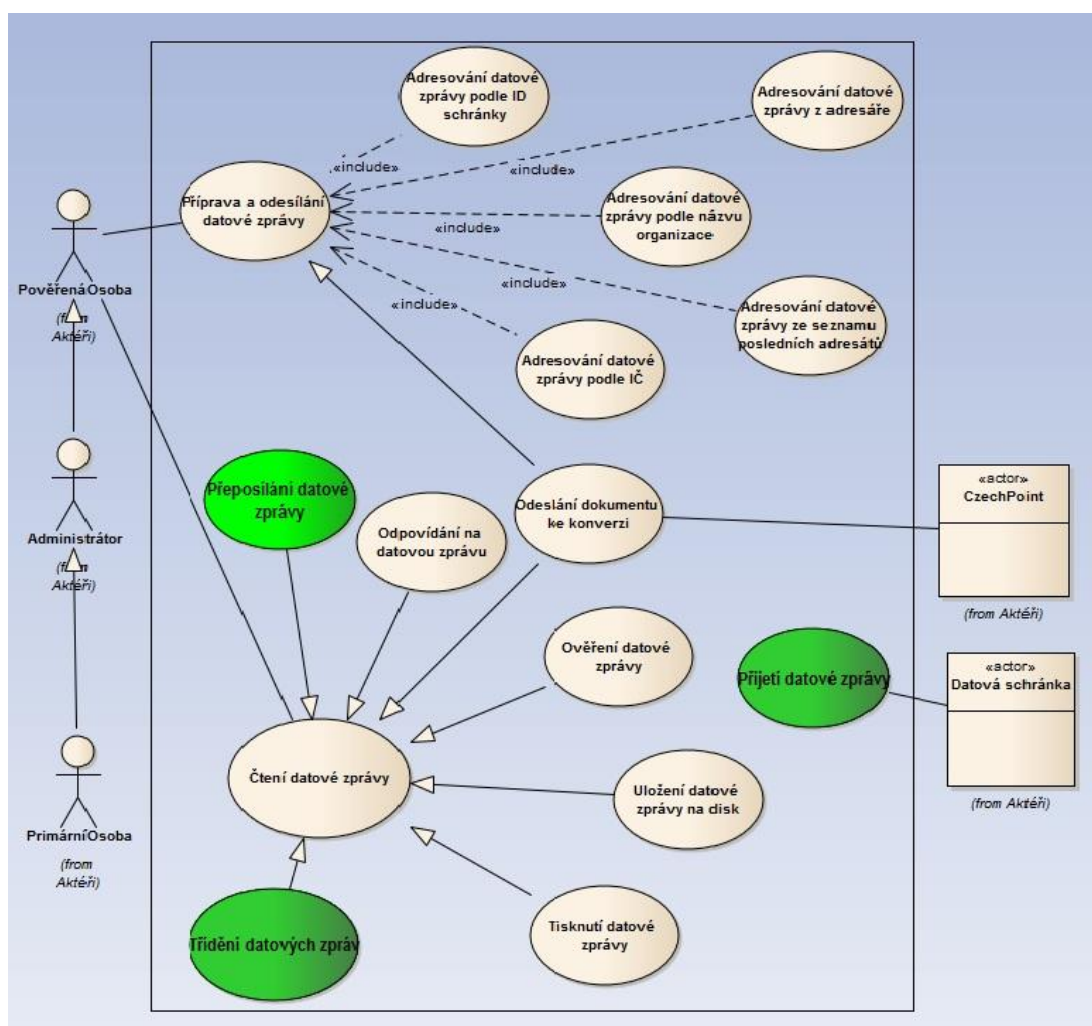
Nastavení aliasu pro uživatele – uživatel má možnost si nastavit libovolný alias z povolených znaků, pokud již tento není obsazen, který může následně používat pro přihlašování jako ID.

Rozšířené nastavení poštovní datové zprávy – oproti původnímu modelu dochází ke značnému zjednodušení, jelikož příjem Poštovní datové zprávy je implicitně zapnut. Uživatel tak automaticky může přijímat tyto zprávy ihned po aktivování datové schránky.

Nastavení upozornění na nové zprávy pomocí SMS – zde se ve funkcionalitě prakticky nic nemění, ale odeslaná datová zpráva obsahuje navíc proti původnímu řešení i informaci o odesílateli datové zprávy a její subjekt.

## 2. Práce s datovou zprávou

Nové funkcionality jsou opět vyobrazeny na upraveném diagramu případů užití obr. č. 25.



Obrázek 25: Změny práce s DS

Oproti stávajícímu řešení došlo k těmto změnám:

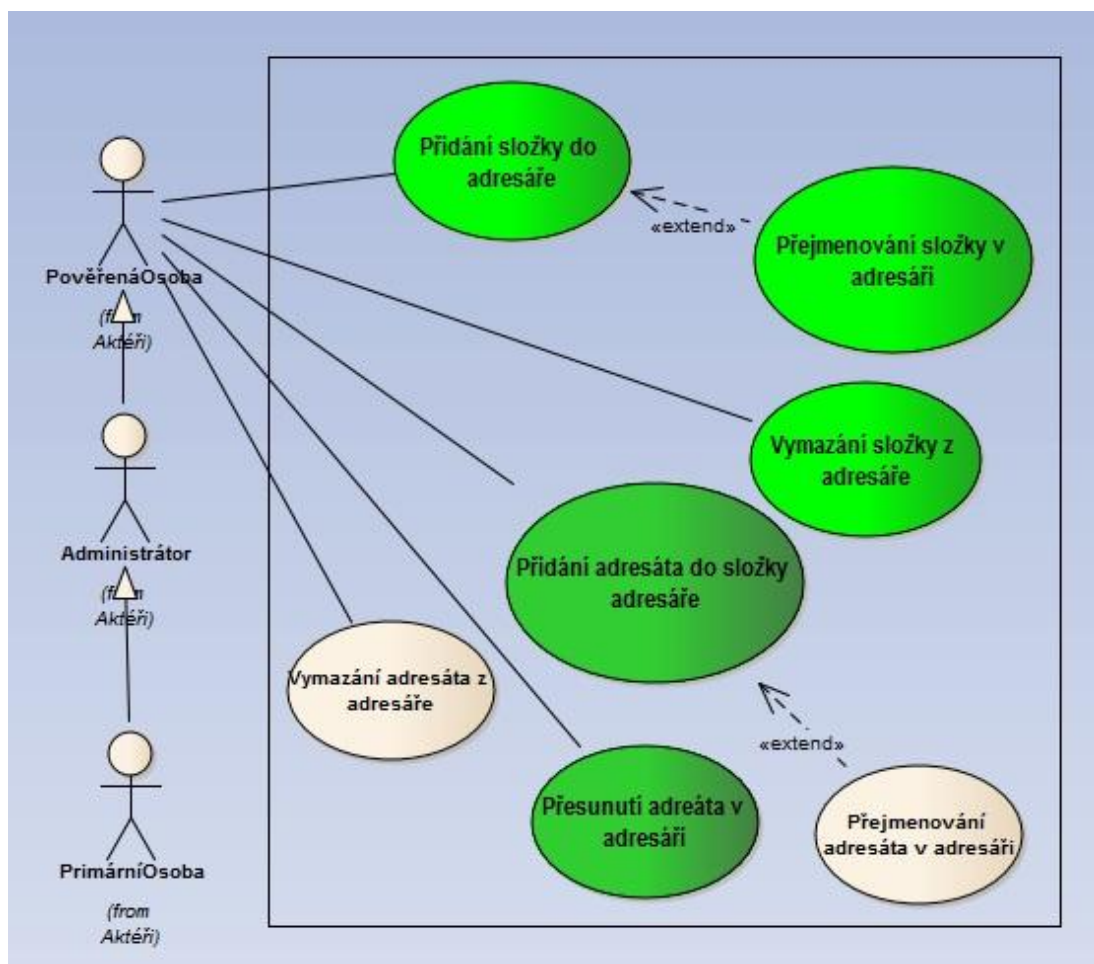
Přijetí datové zprávy – systém po přijetí nové datové zprávy nastaví její platnost místo devadesáti na 365 dní.

Přeposílání datové zprávy – je nová funkcionalita systému, která umožňuje datovou zprávu přeposlat přímo po jejím obdržení. Jak již bylo uvedeno výše, stávající systém tuto možnost nenabízí.

Třídění datových zpráv – je návrh doplňku k již implementovanému třídění zpráv pomocí výběru požadovaného seřazení z menu. Tento doplněk nabízí výběr kritéria řazení zpráv jako přímé kliknutí na název daného sloupce a tím zvolení požadovaného řazení zpráv.

### 3. Práce s adresářem

Změny v této části opět ukazuje upravený use case diagram na obr. č. 26.



Obrázek 26: Změny v práci s adresářem

Oproti stávajícímu řešení došlo k možnosti vytváření vlastní adresářové struktury uvnitř adresáře. Uživatel má jednak možnost přidání složky do adresáře, dále jejího přejmenování

a samozřejmě také vymazání. Navíc lze uložené adresáty v rámci složek přesouvat a tím vytvářet požadovanou strukturu. V současném řešení není jakákoli možnost vytváření vlastní hierarchie uvnitř adresáře.

### 3. Vyhodnocení

V navrhnutém modelu systému se objevila řada změn, která si klade za cíl jak zjednodušení ovládání systému, tak také zlepšení samotné funkcionality. Je nutno podotknout, že i upravený systém má k dokonalosti ještě daleko, nicméně bych ho označil jako krok kupředu.

Oproti původnímu modelu nabízí lepší zabezpečení, pohodlnější ovládání také rozšíření funkcí.

Oba modely vypracované v rámci této diplomové práce jsou dostupné na přiloženém CD.

Model studie současného systému nese název *datoveSchranky-studie.eap*, upravený model s navrhovanými změnami je pak uložen pod názvem *datoveSchranky-navrh.eap*.

## ZÁVĚR

Zákon č. 300/2008 Sb., zákon o elektronických úkonech a autorizované konverzi dokumentů, je sice v platnosti již třetím rokem, nicméně celý projekt datových schránek by se dal označit za mladý a jako takový také stále ve vývoji. Spoustu počátečních nedokonalostí se postupem času podařilo eliminovat, nicméně musíme jedním dechem dodat, že k dokonalosti zbývá urazit ještě dlouhou cestu. Přesto na mě projekt působí poměrně pozitivním dojmem, který by při správném přístupu a vývoji mohl v budoucnu ušetřit hodně času i zdrojů.

Účelem této práce bylo seznámit se se současným stavem a vývojem e-Governmentu v České republice a poskytnout užitečné informace o systému datových schránek a jeho fungování. Cílem předcházejících stránek byla zejména analýza informačního systému datových schránek a vypracování upraveného modelu tohoto systému s návrhem zlepšení stávající funkčnosti.

V první části jsme se seznámili s pozadím elektronické komunikace ve veřejné správě. Vymezili jsme základní pojmy (e-Government, autorizovaná konverze či elektronický podpis) a seznámili se se scénáři nasazení datových schránek.

V druhé části jsme vypracovali analýzu informačního systému datových schránek pomocí nástroje Enterprise Architect. Tento model jsme následně upravili s cílem zlepšit současný stav řešení.

ISDS trpí nepochybně ještě celou řadou dalších neduhů, na kterých by bylo potřeba v budoucnu zapracovat. Nezbyvá nám než doufat, že vývojáři nebudou lhostejní k návrhům a naopak budou mít snahu uvést systém do co možná nejlepšího stavu, aby nemusela vznikat taková řada aplikací třetích stran, které netrpí nedostatky stávajícího systému.

Přejme projektu datových stránek dlouhý život.

## CONCLUSION

Act No. 300/2008 Coll., The Act on Electronic Communication and authorized document conversion, is in force for three years now, but the whole project of data deposit boxes could be described as young and as such also still in development. A lot of initial imperfections were eliminated over the time, however we must add with the same breath, that there is still a long way to perfection. Yet the project has quite a positive impression on me, which with correct approach and development in the future could save a lot of time and resources.

The purpose of this study was to learn about the current state and future development of e-government in the Czech Republic and provide useful information about data deposit boxes system and its functioning. The aim of the previous pages was especially data deposit boxes information system analysis and development of modified model of the system with a proposal to improve existing functionality.

In the first part, we have become familiar with the background of electronic communications in public administration. We defined the basic concepts (e-Government, authorized conversion or electronic signature) and familiarize ourselves with the current data deposit boxes scenarios.

In the second part, we have developed data deposit boxes information system analysis using Enterprise Architect. We modified the model afterwards to improve the current solution state.

ISDS undoubtedly still suffers from a variety of other ailments, for which it would need to work on in the future. We must hope that developers will not be indifferent to the suggestions and will try to bring the system into the best possible condition, to prevent formation of such a number of third party applications that do not suffer the defects of the existing system.

Let's wish the data deposit boxes project long life.

## SEZNAM POUŽITÉ LITERATURY

- [1] BUDIS, Petr a Iva HREBIKOVA. *Datové schránky: fungování, doručování, bezpečnost, návody*. 1. vyd. Olomouc: ANAG, 2010, 287 s. ISBN 80-726-3617-0.
- [2] *Businessinfo: Datové schránky* [online]. © 1997-2011 [cit. 2012-02-03]. Dostupné z: <http://www.businessinfo.cz/cz/rubrika/datove-schranky/1001772/>
- [3] *CzechPoint: Datové schránky* [online]. © 2010 [cit. 2012-02-03]. Dostupné z: <http://www.czechpoint.cz/web/index.php?q=node/389>
- [4] Česká republika. Zákon o elektronických úkonech a autorizované konverzi dokumentů. In: č. 300/2008 Sb. 2008.
- [5] Česká republika. Zákon o elektronickém podpisu. In: *Zákon č. 227/2000 Sb.* 2000.
- [6] *Datové schránky* [online]. © 2010 [cit. 2012-02-03]. Dostupné z: <http://www.datoveschranky.eu/>
- [7] *Datové schránky* [online]. © 2011 [cit. 2012-02-03]. Dostupné z: <http://www.datoveschranky.info/>
- [8] *Ministerstvo vnitra České republiky: Datové schránky* [online]. © 2010 [cit. 2012-02-03]. Dostupné z: <http://www.mvcr.cz/datove-schranky.aspx>
- [9] *Portál datových schránek* [online]. © 2011 [cit. 2012-02-03]. Dostupné z: <https://www.czebox.cz/PortalDS/>
- [10] SMEJKAL, Vladimír. *Datové schránky v právním řádu ČR: zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, s komentářem*. 1. vyd. Praha: ABF, 2009, 176 s. ISBN 978-808-6284-781.

## SEZNAM POUŽITÝCH CITACÍ

1. Archiv stránek bývalého Ministerstva informatiky. <http://aplikace.mvcr.cz/archiv2008/micr/egovernment/default.htm>. [Online]
2. web Czech POINTU, slovník. <http://www.czechpoint.cz/web/?q=node/501>. [Online]
3. Závěr č. 84 ze zasedání poradního sboru ministra vnitra ke správnímu řádu ze dne 14. 12. 2009.
4. Zákon o elektronických úkonech a autorizované konverzi dokumentů. *Zákon č. 300/2008, §17, odst. 3.*
5. Zákon o elektronických úkonech a autorizované konverzi dokumentů. *Zákon č. 300/2008, §5 odst. 1.*
6. Datové schránky/ slovník pojmů. <http://www.datoveschranky.info/cz/o-datovych-schrankach/slovník-pojmu-id34696/>. [Online]
7. Czech POINT. <http://www.czechpoint.cz/web/?q=node/575>. [Online]
8. Zákon o elektronickém podpisu. *Zákon č. 227/2000 Sb., §2, písm. a).*
9. Tesař Pavel, Provozní řád ISDS. <http://www.mvcr.cz/soubor/provozni-rad-ids-pdf.aspx>. [Online]

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

DS	Datová schránka
ISDS	Informační systém datových schránek
CA	Certifikační autorita
PDS	Poštovní datová zpráva
PDS	Poštovní datová zpráva
DT	Datový trezor

**SEZNAM OBRÁZKŮ**

Obrázek 1: <i>EGON</i> (zdroj <a href="http://www.mvcr.cz">www.mvcr.cz</a> ).....	13
Obrázek 2: <i>Autorizovaná konverze z moci úřední</i> (zdroj <a href="http://www.czechpoint.cz">www.czechpoint.cz</a> ).....	25
Obrázek 3: <i>Pracoviště Czech POINT k 14. 4. 2012</i> .....	26
Obrázek 4: <i>Potvrzení o odeslání dokumentu ke konverzi</i> (zdroj <a href="http://www.datoveschranky.eu">www.datoveschranky.eu</a> ) .....	27
Obrázek 5: <i>Ověřovací doložka do dokumentu v listinné podobě</i> (zdroj <a href="http://www.lupa.cz">www.lupa.cz</a> ).....	30
Obrázek 6: <i>Ověřovací doložka konverze do dokumentu obsaženého v datové zprávě</i> (zdroj <a href="http://www.lupa.cz">www.lupa.cz</a> ) .....	30
Obrázek 7: <i>Blokové schéma ISDS</i> (zdroj <a href="http://www.aipsafe.cz">www.aipsafe.cz</a> ) .....	34
Obrázek 8: <i>Aktéři</i> .....	37
Obrázek 9: <i>Přihlašovací stránka</i> .....	39
Obrázek 10: <i>Přihlášení k DS</i> .....	40
Obrázek 11: <i>Změna hesla</i> .....	41
Obrázek 12: <i>Nastavení DS</i> .....	44
Obrázek 13: <i>Elektronická značka</i> (zdroj <a href="http://www.isdstest.cz">www.isdstest.cz</a> ) .....	45
Obrázek 14: <i>Časové razítko</i> (zdroj <a href="http://www.isdstest.cz">www.isdstest.cz</a> ).....	46
Obrázek 15: <i>Platné ověření DS</i> .....	47
Obrázek 16: <i>Nepatné ověření DS</i> .....	47
Obrázek 17: <i>Podporované formáty</i> (zdroj <a href="http://www.datovestranky.eu">www.datovestranky.eu</a> ) .....	48
Obrázek 18: <i>Práce s DS</i> .....	49
Obrázek 19: <i>Přejmenování adresáta</i> .....	50
Obrázek 20: <i>Vymazání adresáta z adresáře</i> (zdroj <a href="http://www.lupa.cz">www.lupa.cz</a> ) .....	51
Obrázek 21: <i>Práce s adresářem</i> .....	51
Obrázek 22: <i>Nefunkční požadavky na systém</i> .....	57
Obrázek 23: <i>Funkční požadavky na systém</i> .....	58
Obrázek 24: <i>Změny v nastavení DS</i> .....	59
Obrázek 25: <i>Změny práce s DS</i> .....	60
Obrázek 26: <i>Změny v práci s adresářem</i> .....	61

**SEZNAM TABULEK**

Tabulka 1: <i>Ceník poplatků</i> .....	17
Tabulka 2: <i>Přístupy</i> .....	21
Tabulka 3: <i>Přípustné znaky pro tvorbu uživatelského jména a bezpečnostního hesla</i> .....	23
Tabulka 4: <i>Náležitosti ověřovací doložky</i> .....	29

## SEZNAM PŘÍLOH

Nedílnou součástí této práce je CD s vypracovaným projektem a plným textem této práce.