Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Informační systém datových schránek

Michal Schuster

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Schuster Michal

Informatika

Název práce

Informační systém datových schránek

Anglický název

Information System of Data Boxes

Cíle práce

Bakalářská práce je tematicky založená na analýze současného stavu podpory systému datových schránek. Cílem teoretické části je a vysvětlení základních pojmů včetně vývoje datových stránek a platné legislativy týkající se dané problematiky. Cílem praktické části bakalářské práce bude provést rozbor informačního systému datových schránek a jeho využití. V závěru bakalářské práce bude provedeno vyhodnocení a porovnání zjištěných údajů a návrh doporučení.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. V praktické části bakalářské práce bude využita metoda analýzy užití datové schránky. Na základě syntézy teoretických výsledků a vlastního řešení budou formulovány závěry bakalářské práce.

Harmonogram zpracování

Studium odborných informačních zdrojů, stanovení dílčích cílů a postupu řešení: 05/2012 - 06/2012
Zpracování přehledu řešené problematiky: 07/2012 – 08/2012
Vypracování vlastního řešení, doporučení a závěry: 09/2012 02/2013
Tvorba finálního dokumentu práce: 02/2013 – 03/2013
Odevzdání práce a tezí: 03/2013

Rozsah textové části

30-40 stránek

Klíčová slova

Datová schránka, eGon, elektronický podpis, ochrana osobních údajů, časové razítko, formát a konverze dokumentů, Česká pošta, Ministerstvo vnitra

Doporučené zdroje informací

Ministerstvo vnitra ČR. Datové schránky [online]. 2011. Dostupné z <http://www.datoveschranky.info/>

Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších zákonů. Sbírka zákonů Česká republika. Břeclav: Moraviapress. ISSN 1211-1244.

Zákon č. 227/2000 Sb. o elektronickém podpisu, ve znění pozdějších zákonů. Sbírka zákonů Česká republika. Břeclav: Moraviapress

Zákon č. 499/2008 Sb. o archivnictví a spisové službě, ve znění pozdějších zákonů. Sbírka zákonů Česká republika. Břeclav: Moraviapress

LIDINSKÝ, Vít. ŠVARCOVÁ Ivana. BUDIŠ, Petr. LOEBL, Zbyněk. PROCHÁZKOVÁ, Barbora. eGovernment bezpečně. 1. vyd. Praha. Grada. 2008. ISBN 978-80-247-2462-1

PETERKA, Jiří. Báječný svět elektronického podpisu. Praha. CZ.NIC. 2011. ISBN 978-80-904248-3-8

BUDIŠ, Petr. HŘEBÍKOVÁ, Iva. Datové schránky. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-617-4

SMEJKAL, Vladimír. Datové schránky v právním řádu ČR. Praha. ABF a.s.. 2009. ISBN 978-80-7263-617-4

SMEJKAL, Vladimír. VALÁŠEK, Michal. Jak na datovou schránku. Praha. Linde. 2012. ISBN 978-80-86131-80-1

LAPÁČEK, Jiří. Jak na datovou schránku a elektronickou komunikaci s úřady. 1.vyd. Brno. Computer Press. 2012. ISBN 978-80-251-3680-5

Vedoucí práce

Rysová Hana, Ing.

Termín odevzdání

březen 2013

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Informační systém datových schránek" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3 2013 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Haně Rysové za odbornou pomoc a odborné konzultace při zpracovávání této bakalářské práce.

Informační systém datových schránek

Souhrn

Bakalářská práce se zabývá tématem datových schránek a aplikací pro jejich správu. Teoretická část zahrnuje vývoj e-Governmentu, dále projekty Czech POINT, Portál veřejné správy, elektronické podatelny a základní registry. Další část je věnována legislativní úpravě systémů datových schránek, kterou především reprezentuje zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Následující kapitoly se zabývají bezpečností ve správě datových schránek, autorizovanou konverzí dokumentů a ochranou osobních údajů. Praktická část bakalářské práce přibližuje webové rozhraní informačního systému datových schránek a dále aplikace pro privátní správu datových schránek.

Klíčová slova

Ministerstvo vnitra ČR, Czech POINT, datové schránky, informační systém datových schránek (ISDS), e-Government, elektronický podpis, certifikát, autorizovaná konverze dokumentů

Information System of Data Boxes

Summary

The thesis deals with the issue of data boxes and applications to manage them. The theoretical part includes the development of e-government projects, the Czech POINT portal of public administration, registrars and registries. The next section is devoted to legislation in the area of data boxes, which mainly represents the law No. 300/2008 Coll., on electronic acts and authorized the conversion of documents. The following chapters deal with security in the management of data boxes, authorized the conversion of documents and the protection of personal data. The practical part of the thesis presents the Web interface of information system data and applications for private management of the data boxes.

Keywords

The Ministry of Interior of the CZECH REPUBLIC, Czech POINT, data boxes, information system of data boxes (ISDS), e-Government, electronic signature, certificate, authorized document conversion

Obsah

Úvod 11

Cíl a metodika 13

1 E-Government 14

1.1 Vývoj e-Governmentu 14

1.2 Prvky e-Governmentu 16

1.2.1 Czech POINT 17

1.2.2 Elektronické podatelny 18

1.2.3 Portál veřejné správy 18

1.2.4 Základní registry 19

2 Informační systém datových schránek 20

2.1 Legislativa datových schránek 20

2.2 Pojem datová schránka 20

2.3 Informační systém datových schránek 21

2.4 Zřízení datové schránky 21

2.4.1 Datová schránka fyzické osoby a podnikající fyzické osoby 22

2.4.2 Datová schránka právnické osoby 22

2.4.3 Datová schránka orgánu veřejné moci 23

2.5 Osoby oprávněné k přístupu do datové schránky 23

2.6 Přístupové údaje 24

2.7 Zpřístupnění a znepřístupnění datové schránky 24

2.8 Zrušení datové schránky 25

3 Bezpečnost v datové schránce 26

3.1 Elektronický podpis 27

3.1.1 Uznávaný a zaručený elektronický podpis 27

3.1.2 Princip činnosti 28

3.1.3 Hashovací funkce 28
3.1.4 Symetrická kryptografie 28
3.1.5 Asymetrická kryptografie 29
3.2 Certifikáty 30
3.3 Certifikační autorita 30
3.4 Časová razítka 31
4 Autorizovaná konverze dokumentů 32
4.1 Ověřovací doložka 33
4.2 Spisová služba 33
4.2.1 Životní cyklus dokumentu 33
4.3 Ochrana osobních údajů 34
5 Prostředí datových schránek 36
5.1 Začátky s datovou schránkou 36
5.2 Přihlášení do datové schránky 37
5.2.1 Ochrana certifikátem 37
5.2.2 Ochrana bezpečnostním kódem 37
5.2.3 Ochrana SMS kódem 38
5.3 Webové rozhraní datových schránek 38
5.3.1 Vytvoření a odeslání datové zprávy 39
5.3.2 Přidání nového uživatele 40
5.4 Statistiky datových schránek 41
6 Aplikace pro správu datové schránky 42
6.1 Aplikace Multischránka 42
6.1.1 Přihlášení do aplikace 42
6.1.2 Správa zpráv 43
6.1.3 Porovnání s webovým rozhraním ISDS 43

6.2 Aplikace Datovka 44
6.2.1 Přihlášení do aplikace 44
6.2.2 Prostředí aplikace Datovka 45
6.2.3 Odesílání datové zprávy 45
6.2.4 Datovka pro Android 46
6.2.5 IDatovka 46
6.3 Aplikace Datové schránky pro Android 46
Závěr 48
Seznam použitých zdrojů 50
Seznam obrázků 53
Seznam příloh 53
Příloha 54

Úvod

Téma bakalářské práce Informační systém datových schránek bylo zvoleno především z důvodu zájmu o oblast informačních technologií a zejména o oblast elektronické komunikace. Informační technologie se v současné době uplatňuje v mnoha pracovních odvětvích a vstupuje stále častěji do různých oblastí lidské činnosti. Nasazením e-Governmentu do praxe započal proces elektronizace oblasti veřejné správy. Do té doby probíhala komunikace mezi úřady a mezi úřadem a občanem pouze formou písemné komunikace. Spuštění e-Governmentu mělo přispět k úspoře nejen časové, ale i finanční, ale také snížení administrativního zatížení úředníků a občanů. Jeho hlavním cílem bylo dosáhnout toho, aby úřední dokumenty byly přijímány a odesílány v elektronické podobě a občan nemusel obíhat úřady, a zároveň prokazovat skutečnosti, které si může úřad dohledat v dostupných databázích. Úspěšným příkladem elektronizace veřejné správy je spuštění projektu Czech POINTu a spuštění projektu Informačního systému datových schránek. Systém datových schránek, který byl v České republice zaveden, je systémem zcela novým a hlavně unikátním. Obdobný systém pro komunikaci s úřady nebyl dosud v Evropě ani ve světě spuštěn ani provozován. Vznik datových schránek a jejich uvedení do praxe probíhalo velmi rychle. V období let 2007 až 2008 byl vypracován, ve spolupráci Ministerstva vnitra a Ministerstva spravedlnosti, návrh zákona. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů nabyl účinnosti 1. 7. 2009. Tímto dnem začala Česká pošta rozesílat obálky s přístupovými hesly do datových schránek, které byly povinně zřízeny orgánům veřejné moci a právnickým osobám zřízeným zákonem a zapsaným v obchodním rejstříku. Dnem 1. 11. 2009 byly aktivovány všechny datové schránky, a tím vstoupil Informační systém datových schránek do plného provozu.

Cílem bakalářské práce je provést analýzu současného stavu podpory systému datových schránek. Práce je rozdělena na část teoretickou a na část praktickou. Teoretickou část bakalářské práce tvoří čtyři kapitoly, které postupně popisují vývoj a prvky e-Governmentu, informační systém datových schránek a platnou legislativu s tím související, zabezpečení datových schránek a zpráv a autorizovanou konverzí dokumentů. Praktická část je členěna do dvou kapitol, ve kterých postupně bude proveden rozbor práce s datovou schránkou, tj. přihlášení do datové schránky, nastavení dodatečné ochrany přihlášení, popis prostředí webového rozhraní a seznámení se způsobem vytváření

a odesílání datových zpráv. Další kapitola bude věnována seznámení se s aplikacemi pro správu datové schránky. Závěr bakalářské práce bude věnován vyhodnocení a porovnání zjištěných údajů a návrh doporučení.

Cíl a metodika

Bakalářská práce je tematicky založená na analýze současného stavu podpory systému datových schránek. Cílem teoretické části je přiblížit rozvoj e-Governmentu v České republice a provést popis jednotlivých prvků tvořící e-Government. Dále jsou vysvětleny základní pojmy týkající se datových schránek, charakterizován vývoj systému datových stránek a jejich užití v souladu s platnou legislativou týkající se dané problematiky. Cílem praktické části bakalářské práce je provést rozbor informačního systému datových schránek a jeho využití. V závěru bakalářské práce je provedeno shrnutí a zhodnocení zjištěných údajů a návrh doporučení.

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů, a to odborných publikací týkajících se oblasti datových schránek, internetových portálů e-Governmentu Czech POINT, Portál veřejné správy, Ministerstva vnitra ČR. K vysvětlení legislativního zabezpečení systému datových schránek bylo užito úplné znění zákonů, které se týkají problematiky datových schránek. V praktické části bakalářské práce je využita metoda analýzy užití datové schránky. K vypracování praktické části byla zřízena datová schránka fyzické osoby, na které jsou vysvětleny postupy od žádosti ke zřízení datové schránky, přes vlastní užití datové schránky, tj. přihlášení do datové schránky, odeslání a přijetí datové zprávy a správu schránky. Další část je věnována aplikacím, které zajišťují přístup do datové schránky, a to aplikacím Multischránka a Datovka. Následující část bakalářské práce ukazuje na přiložených grafech zvyšující se počet zřízených datových schránek a rostoucí počet odeslaných datových zpráv. V závěru bakalářské práce jsou shrnuty získané informace z odborných zdrojů, provedeno zhodnocení těchto informací a formulováno doporučení, týkajíce se návrhu k rozšiřování a modernizaci systému datových schránek. Zároveň je navrženo doporučení fyzickým osobám k využívání datových schránek ke komunikaci s orgány veřejné moci, z důvodu úspory svého času.

1 E-Government

V současné době je již pojem e-Government pro spoustu lidí běžně používaným slovem, aniž by věděli, co všechno se pod tímto pojmem skrývá. Ve skutečnosti není jednoduché nalézt definici, která by plně vystihovala obsažnost tohoto pojmu. Odborná literatura zaměřená na tuto tématiku uvádí nejčastěji definice podle Ministerstva vnitra ČR nebo EU, ale objevují se i další.

Definice podle Evropské Unie:

- „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.“ (1 str. 11)

Definice podle Ministerstva vnitra České republiky

- „E- Government představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií a cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy ve vztahu ke svým uživatelům.“ (2 str. 11)

Pokud se zabýváme pojmem e-Government není možné se nedostat k pojmu elektronické komunikace. Tuto klíčovou část e-Governmentu je možné dále rozdělit na komunikaci státní správy s občany, tzv. Government-to-Citizen (G2C), komunikaci státní správy s obchodními společnostmi a podnikateli, tzv. Government-to-Business (G2B), a mezi orgány státní správy navzájem, tzv. Government-to-Government (G2G).

Zavést do praxe takhle komplikovanou a rozsáhlou koncepci není vůbec nic jednoduchého. Není možné vydat jeden zákon nebo vyhlášku a prohlásit, že je hotovo. Vyžaduje to dlouhý a pomalý vývoj vedoucí přes úpravu legislativy v mnoha oblastech, návrhy řešení s využitím dostupných technologií, až po jeho zavedení do provozu (2).

1.1 Vývoj e-Governmentu

Cesta realizace e-Governmentu v České republice započala roku 1999, a to vypracováním strategie „Státní infomační politika“ a tím začalo budování informační společnosti. V platnost vešla usnesením vlády č. 525 ze dne 31. května 1999.

Tato koncepce byla zaměřena do tří oblast:

1. informatizace veřejné správy
2. informační gramotnost
3. elektronický obchod

Za hlavní prioritu byla pokládána první oblast, tj. oblast informatizace veřejné správy.

Při vytváření koncepce se vycházelo primárně ze dvou dokumentů. První předlohou byl akční plán vydaný Evropskou unií již v roce 1994. V plánu „Cesta Evropy k informační společnosti“ byly stanoveny základní principy pro vytváření informační politiky v Evropě. Tím druhým dokumentem byly závěry pracovní skupiny Fóra o informační společnosti, které přijali na konferenci „Informační společnost přibližující administrativu občanům“, konající se v roce 1998. Byly zde stanoveny hlavní cíle při budování informační společnosti:

- právo na dostupnost veřejných informací
- poskytování veřejných služeb s využitím elektronických komunikačních prostředků
- komunikace a spolupráce veřejného a soukromého sektoru
- využívání osvědčených postupů a nástrojů, sjednocování standardů a zajištění informačního zdroje

V návaznosti na koncepci „Státní informační politika“ byla v témže roce přijata koncepce „Budování informačních systémů veřejné správy“, která si za hlavní cíl vytyčila zvýšení efektivnosti a důvěryhodnosti veřejné správy, zpřehlednění postupů a také omezení přebujelé byrokracie a vytíženosti účastníků řízení.

V souvislosti s přijímáním výše uvedených dokumentů bylo třeba vytvořit legislativní podmínky k jejich uplatnění v praxi. Přijetím právních předpisů České republiky bylo dosaženo slučitelnosti právního řádu ČR s právem EU. K zajištění právních podmínek, na základě kterých mělo dojít k efektivnímu budování informační společnosti, byly v průběhu let 1999-2001 přijaty zákony:

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- zákon č. 29/2000 Sb., o poštovních službách
- zákon č. 101/2000 Sb., o ochraně osobních údajů
- zákon č. 227/2000 Sb., o elektronickém podpisu
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy

Další zásadnější změny proběhly v roce 2004. Došlo k nahrazení předchozí koncepce z roku 1999, a to usnesením vlády č. 265 ze dne 24 března 2004, známou pod názvem „Státní informační a komunikační politika“. Podle ní se musí Česká republika zaměřit na oblasti:

- dostupné a bezpečné komunikační služby
- informační vzdělanost
- moderní veřejné služby online
- dynamické prostředí pro elektronické podnikání

Ale za nejdůležitější dokument týkající se budování informační společnosti je považováno usnesení vlády č. 1085 ze dne 20. září 2006. Toto usnesení obsahuje informace týkající se prosazování a implementace e-Governmentu v České republice v letech 1999-2006 a současně s ním byl schválen soubor opatření pro urychlení rozvoje e-Governmentu v České republice.

Z tohoto dokumentu vyplynula celá řada dalších legislativních opatření. Nově je umožněno použití dokumentů v elektronické podobě namísto dokumentů v listinné formě. Současně došlo k vytvoření předpokladu pro přijetí legislativních opatření, na základě kterých byly formovány podmínky pro vedení spisové služby v elektronických systémech. Klíčovými důsledky přijetí tohoto usnesení bylo zadání státní zakázky na vybudování infrastruktury kontaktních míst Czech POINT a pověření ministrů vnitra a informatiky úkolem, aby stanovili základní technické a organizační principy pro zřízení centrálních registrů veřejné správy.

V roce 2007 byl usnesením vlády č. 197 ze dne 28. února 2007 přijat návrh „Integrovaného operačního programu pro období 2007-2013“ a určeny základní cíle pro strategii „Efektivní veřejná správa pro období 2007 až 2015“. Hlavními oblastmi realizace jsou stanoveny veřejné služby, zdravotnictví, práce a sociální péče a místní rozvoj (2).

1.2 Prvky e-Governmentu

Projekt eGON byl zahájen ke konci roku 2006 a představuje komplexní projekt elektronizace veřejné správy, který měl za hlavní cíl usnadnění života občanům a zvýšení efektivity veřejné správy. Postava eGONa se stala symbolem e-Governmentu a zároveň je považována za živý organismus, ve kterém vše souvisí se vším. Jednotlivé části eGONa

představují prvky e-Governmentu, prsty Czech POINT, oběhová soustava je komunikační infrastruktura veřejné správy, srdcem je zákon č. 300/2008 Sb. a mozek představuje základní registry veřejné správy (3).

Psal se rok 2011 a eGON, který byl do té doby jediným symbolem e-Governmentu, dostal moderní partnerku. Ta přináší nový fenomén zvaný cloud computing nebo také sdílení softwarových i hardwarových prostředků pomocí sítě. Dále má zajistit, aby ICT projekty byly levnější a efektivnější. Úkolem těchto projektů je také přechod k modelu poskytování a odebírání služeb (4).

Obrázek 1. eGON a Klaudie
Zdroj: www.mvcr.cz

1.2.1 Czech POINT

Czech POINT, nebo také Český Podací Ověřovací Informační Národní Terminál je projekt, který měl za cíl zredukovat byrokracii ve vztahu občan a veřejná správa. Hlavní myšlenkou bylo, aby občan nemusel cestovat po několika různých úřadech, přestože potřeboval vyřídit jeden problém. Nyní stačí navštívit terminál Czech POINT. Kontaktní místo slouží jako místo výkonu veřejné správy a zprostředkovává komunikaci se státem na jediném místě (5).

Je to garantovaná služba umožňující získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, provést autorizovanou konverzi dokumentů, získat informace o průběhu správních řízení.

Co Czech POINT poskytuje:

- Výpis z katastru nemovitostí
- Výpis z obchodního registru
- Výpis z živnostenského rejstříku
- Výpis z rejstříků trestů
- Výpis bodového hodnocení řidiče
- Datové schránky
- Autorizovanou konverzi dokumentů
- Základní registry (6)

1.2.2 Elektronické podatelny

Dalším důležitým prvkem e-Governmentu jsou elektronické podatelny. Podle zákona č. 227/2000 Sb., o elektronickém podpisu jsou definovány jako „pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv“ (7), tzn. místo pro komunikaci s veřejnou správou. Zároveň orgány veřejné moci mají povinnost přijímat a odesílat datové zprávy, které mají přiložený zaručený elektronický podpis.

Dne 26. července 2004 byl tento zákon novelizován zákonem č. 440/2004 Sb. Předpis zavádí pojem „kvalifikované časové razítko“, které prokazuje existenci elektronického dokumentu v čase. Další novinkou je možnost používat „elektronické značky“. Pro ty se stejně jako pro zaručený elektronický podpis používá technologie digitálních podpisů. Rozdíl mezi nimi spočívá v tom, že elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy (2).

Zatím poslední úprava zákona proběhla ke dni 1. 7. 2012, zákon č. 167/2012 Sb., o elektronickém podpisu. Novela zavádí pojmy „uznávaný elektronický podpis“ a „uznávanou elektronickou značku“ (8).

1.2.3 Portál veřejné správy

Portál veřejné správy je komplexní informační systém vybudovaný na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Bývá též označován jako elektronická brána do veřejné správy a významně přispívá k rozvoji a přiblížení služeb obyvatelům České republiky. Stránky nabízejí přehledný přístup k velké většině

důležitých informací rozdělených podle skupin uživatelů, těmi jsou občané České republiky, podnikatelé a živnostníci, cizinci žijící v České republice a orgány veřejné moci. Nalezneme zde odkaz pro přihlášení do datové schránky nebo odkaz na stránky projektu Czech POINT. Mezi další funkce Portálu veřejné správy patří například vyhledávání zákonů, seznam držitelů datových stránek a věstníky ministerstev a krajů (9).

1.2.4 Základní registry

Základní registry jsou jedním ze základních pilířů e-Governmentu. Jejich cílem je ulehčit všem subjektům styk s veřejnou správou, tzn. snížit počet návštěv na úřadech s využitím moderních internetových technologií. Zároveň musí veřejná správa zajistit efektivní, transparentní a bezpečnou výměnu přesných a aktuálních údajů. Z toho vyplývá, že úředníci nemusí kontrolovat aktuálnost a správnost dat, čímž dochází ke zrychlení při vyřizování žádosti a snížení byrokracie. Projekt Základních registrů přešel do ostrého provozu 1. července 2012 a jak je uvedeno na domovské stránce základních registrů www.szrcr.cz (10) „*Tímto datem byl neodvratně zahájen dlouhodobý a v některých procesech i trvalý proces nápravy veřejné správy*“ (10).

2 Informační systém datových schránek

2.1 Legislativa datových schránek

Informační systém datových schránek je systémem veřejné správy, který je legislativně upraven zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Spolu s tímto byl přijat zákon č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů. V době než dne 1. července 2009 nabyly tyto zákony právní účinnosti, proběhla novelizace několika zákonů. Jedním byl zákon č. 7/2009 Sb., který upravuje zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů. Stejný den nabyl účinnosti i zákon č. 190/2009 Sb., který upravuje zákon č. 499/2004 Sb., o archivnictví a spisové službě (11). V souvislosti se zákonem o datových schránkách byly vydány dva prováděcí předpisy:

- Vyhláška č. 193/2009 Sb., o stanovení provádění autorizované konverze dokumentů
- Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění vyhlášky č. 422/2010 Sb. (12)

2.2 Pojem datová schránka

Datová schránka je elektronické úložiště, které slouží pro komunikaci v oblasti veřejné správy. Na základě zákona č. 300/2008 Sb., jsou datové schránky určeny k:

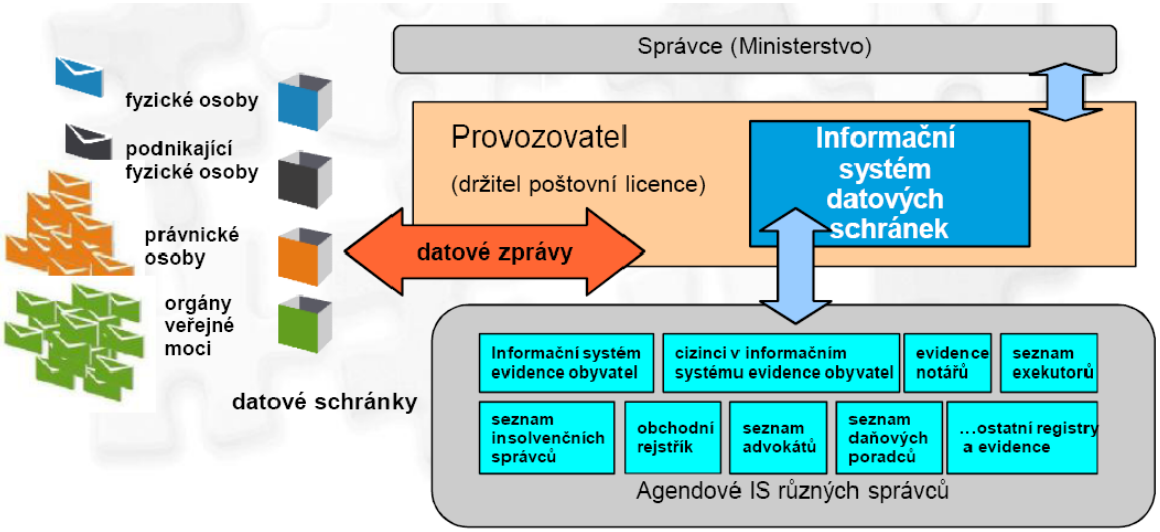
1. Doručování orgány veřejné moci
2. Provádění úkonů vůči orgánům veřejné moci
3. Dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob

I když se datová schránka může na první pohled zdát jako klasická elektronická komunikace, tak opak je pravdou. Datová schránka opravdu neslouží jako e-mail, či archiv zpráv. Jedná se o krátkodobé úložiště, tzn., že zprávy nejsou uložené ve schránce trvale, ale pouze dobu stanovenou zákonem a to po dobu 90 dnů. Informační systém datových schránek umožňuje uchovat zprávy i po delší dobu, k tomu provozovatel zřídil placenou službu datového trezoru (12).

2.3 Informační systém datových schránek

Činnost datových schránek je zajištěna v rámci informačního systému datových schránek, který je podle zákona č. 365/2000 Sb., informačním systémem veřejné správy. ISDS spravuje informace o datových schránkách a jejich uživatelích. Informační systém je pod správou Ministerstva vnitra ČR, kterému byla svěřena působnost pro zajištění důvěryhodnosti a integrity datových zpráv. Současně spravuje i informační systém, který předává informace uživatelům datových schránek o úkonech spojených s činností datové schránky, např. oznámení o doručení zprávy do datové schránky adresáta, oznámení, že datová schránka neexistuje a mnoho dalších.

Druhou institucí podílející se na činnosti ISDS, je Česká pošta. Je provozovatelem informačního systému a provádí některé informační činnosti v rámci ISDS. Je přímo zákonem určeným držitelem poštovní licence.



Obrázek 2. Informační systém datových schránek
Zdroj: Budiš. P., Hřebíková. I., Datové schránky. Str. 39

2.4 Zřízení datové schránky

Oprávnění ke zřízení a správě nových datových schránek má pouze Ministerstvo vnitra ČR z titulu správního úřadu pro oblast informačních systémů veřejné správy.

Datové schránky mohou být zřízeny dvěma způsoby:

a) ze zákona
b) na žádost

2.4.1 Datová schránka fyzické osoby a podnikající fyzické osoby

Datová schránka fyzické osoby je zřízena pouze na její žádost. To znamená, že zřízení datové schránky pro fyzickou osobu není povinné. Žádost podaná na kontaktním místě Czech POINT je vyřízena bezplatně a je zřízena Ministerstvem vnitra ČR do 3 pracovních dnů (12). Žádost musí splňovat určité právní náležitosti:

a) Jméno, Příjmení
b) Rodné příjmení
c) Den, měsíc a rok narození
d) Místo a okres narození, pro osoby narozené v cizině i stát, kde se narodil
e) Státní občanství
f) Úředně ověřený podpis (13)

Stejné podmínky platí i pro podnikající fyzické osoby. Výjimku tvoří advokáti, daňový poradci a insolvenční správci, kterým je schránka bezodkladně zřízena poté co ministerstvo obdrží informaci o jejich zapsání do stanovené evidence.

Důležitou poznámkou je, že subjekt může mít zřízenou pouze jednu datovou schránku. Výjimkou jsou subjekty, které mají několik právních postavení. To znamená, že může vlastnit jednu datovou schránku jako fyzická osoba a druhou jako živnostník.

2.4.2 Datová schránka právnické osoby

Datové schránky právnickým osobám zřídí Ministerstvo vnitra bezplatně podle zákona o datových schránkách, a to všem právnickým osobám zapsaným v obchodním rejstříku. V případě nově vzniklé právnické osoby dojde okamžitě ke zřízení datové schránky po jejím zapsání do obchodního rejstříku. Právnické osoby, které nejsou v obchodním rejstříku, musí pro zřízení datové schránky podat žádost.

Náležitosti, které musí žádost splňovat:

a) Název firmy
b) IČO
c) Sídlo firmy
d) Jméno, příjmení, datum narození a adresu pobytu oprávněné osoby pověřené jednat jménem právnické osoby
e) Stát registrace
f) Úředně ověřený podpis (13)

2.4.3 Datová schránka orgánu veřejné moci

Tento typ datové schránky je zřizován pro každý orgán územního samosprávného celku, pro orgány jednotlivých městských části hlavního města Prahy, ale i pro orgány mající právní subjektivitu. Její zřízení probíhá bezodkladně po jeho vzniku. Orgány veřejné moci mají možnost nechat si zřídit další datovou schránku, která slouží zejména pro vnitřní potřebu organizační jednotky. Novou schránku na žádost zřídí Ministerstvo vnitra ČR bezplatně do 3 pracovních dnů. Žádost musí obsahovat:

a) Název orgánu veřejné moci a název vnitřní organizační jednotky
b) Identifikační číslo ekonomického objektu
c) Adresu sídla
d) Jméno, příjmení, datum narození a adresu osoby, které mají být zaslány přihlašovací údaje (13)

2.5 Osoby oprávněné k přístupu do datové schránky

Jedním z hlavní záměrů datových schránek byla také bezpečnost. Z toho vyplývá, že datové schránky jsou jedním z nejbezpečnějších způsobů elektronické komunikace. Ochrana doručovaných zpráv a dokumentů je zde zajištěna nejen technologickými prostředky, ale také za pomocí pravidel přístupu (2). Tato pravidla jsou přesně stanovena v zákoně č. 300/2008 Sb., který zároveň rozlišuje a přesně specifikuje i osoby primárně oprávněné a osoby pověřené k přístupu do datové schránky. Mezi osoby, které jsou primárně oprávněny k přístupu:

- fyzická osoba, pro niž byla datová schránka zřízena
- podnikající fyzická osoba, pro niž byla datová schránka zřízena
- statutární orgán právnické osoby, člen statutárního orgánu právnické osoby nebo vedoucí organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro něž byla datová schránka zřízena
- vedoucí orgánu veřejné moci, pro něhož byla datová schránka zřízena (13)

Druhou skupinou osob jsou osoby, které mohou získat přístup do datové schránky z pověření osoby oprávněné. Tento přístup je pouze v rozsahu stanovených oprávnění a také s možností určit oprávnění k přístupu k dokumentům do vlastních rukou adresáta.

Přesný rozsah práv k vymezení rozsahu oprávnění k operacím je stanoven v provozním řádu informačního systému datových schránek. Poslední skupinou oprávněných osob tvoří tzv. administrátoři. Administrátoři jsou osoby určené k provádění úkonů ve vztahu k pověřeným osobám a vůči Ministerstvu vnitra ČR (2).

2.6 Přístupové údaje

Přístupové údaje slouží pro přihlášení oprávněných a pověřených osob do systému datových schránek. Tyto osoby jsou povinné zacházet s přístupovými údaji tak, aby nedošlo k jejich zneužití. V rámci zajištění bezpečnosti je po prvním přihlášení oprávněná osoba vyzvána ke změně hesla. Bezpečnostní heslo musí obsahovat prvky, které zvýší úroveň obtížnosti prolomení hesla. Mezi tyto prvky patří například používání malých a velkých písmen, použití číslic nebo povolených speciálních znaků. Tato změna hesla je po oprávněné osobě vyžadována každých 90 dní.

Informační systém datových schránek, potažmo Ministerstvo vnitra ČR nabízí institut „Zneplatnění přístupových údajů“. Tento institut je realizován pouze na žádost oprávněné osoby nebo osoby administrátora. Ministerstvo vnitra zneplatní údaje oprávněné osoby okamžitě po jeho oznámení, například když dojde k jejich ztrátě či odcizení, a zároveň zašle této osobě nové přístupové údaje (2).

2.7 Zpřístupnění a znepřístupnění datové schránky

Zpřístupnění datové schránky je provedeno prvním přihlášením oprávněné osoby do informačního systému datových schránek. Zpřístupnění však proběhne nejpozději 15 dní od doručení přihlašovacích údajů, i když se oprávněná osoba do datové schránky nepřihlásí.

Na druhé straně zneplatnění datové schránky pro fyzickou osobu a podnikající fyzickou osobu lze provést jen v případech stanovených zákonem a to i zpětně. Tyto případy jsou úmrtí, prohlášení za mrtvého, zbavení nebo omezení způsobilosti k právním úkonům nebo z důvodu výkonu trestu. U právnických osob je znepřístupnění datové schránky určeno ke dni odstranění záznamu ze zákonem stanovené evidence.

Je-li datová schránka znepřístupněna, je ji možné na žádost osoby nebo orgánu veřejné moci do 3 dnů opět zpřístupnit (14).

2.8 Zrušení datové schránky

Před každým zrušení datové schránky musí nejprve dojít k jejímu znepřístupnění. Zrušení schránky proběhne u každého typu schránky za jiných podmínek. Datová schránka fyzické osoby je zrušena po uplynutí 3 let od úmrtí, popř. prohlášení za mrtvého. U podnikajících fyzických osob a právnických osob je to po uplynutí 3 let od odstranění ze zákonem stanovené evidence. A datová schránka orgánu veřejné moci zruší Ministerstvo vnitra po třech letech od jeho zrušení (13).

3 Bezpečnost v datové schránce

Při návrhu informačního systému datových schránek, ale i všech aplikací v rámci e-Governmentu, byla na prvním místě bezpečnost. Samotný přechod z papírových dokumentů k elektronickým dokumentům, jejich zpracování a nakládání s nimi nesmí znamenat snížení úrovně bezpečnosti. Mezi požadavky na bezpečnost informačního systému datových schránek patří dostupnost, tzn., že elektronická komunikace bude dostupná, bezpečná a efektivní. Důvěrnost nám zase zaručuje, že nejde k porušení listovního tajemství. Informační systém musí také zaručit neměnnost dokumentu během zpracování a během jeho přenosu. Dále musí být zaručena i autentizace a autorizace nebo přesný čas (2).

Co vlastně tato bezpečnost představuje pro běžného uživatele. Nejlépe je to vystihli pánové Ing. V. Smejkal a M. A. Valášek ve své publikaci „*Bezpečnost informačního systému datových schránek je zcela mimo kontrolu uživatele. Jedná se do jisté míry o náboženskou zkušenost: nemůžeš pochopit, musíš uvěřit*“ (12 str. 172).

Na základě výše uvedené rady, zaměříme svou pozornost na bezpečnost datové schránky z hlediska jejího uživatele. Existuje nejpravděpodobněji velké množství rad a návodů, ale nejužitečnější seznam doporučení se nachází na informačním portálu datových schránek. Bezpečnostní desatero uživatele ISDS:

1. Bezpečný přístup k datové schránce
2. Aktualizovaný bezpečnostní software a operační systém
3. Datová schránka jako účet internetového bankovnictví
4. Kvalitní a aktualizovaný antivirový program
5. Osobní oboustranný firewall
6. Nepracovat na účtu administrátora
7. Záloha důležitých dat
8. Bezpečné bezdrátové připojení
9. Nedůvěřovat neověřeným zprávám
10. Užívat jen legální software z prověřených zdrojů (15)

3.1 Elektronický podpis

Pojem elektronický podpis byl zaveden do právního řádu České republiky zákonem č. 227/2000 Sb., o elektronickém podpisu. Označuje specifická data připojená k dokumentu a nahrazující při elektronické komunikaci vlastnoruční podpis. Tato data obsahují jednoznačné informace, která identifikují vlastníka podpisu. Elektronický podpis také poskytuje prostředek, který příjemci zprávy zaručuje, že ve zprávě či dokumentu nedošlo k žádné změně (16).

3.1.1 Uznávaný a zaručený elektronický podpis

Uznávaný elektronický podpis možná získal své pojmenování tím, že tento podpis úřad „uzná“, při elektronické komunikaci. To znamená, pokud má uživatel dokument opatřený uznávaným elektronickým podpisem, musí ho úřady uznávat a pracovat s ním jako kdyby byl podepsaný vlastnoručně. Vezmeme-li zaručený elektronický podpis, tak již podle názvu dostáváme určité záruky, které poskytuje na rozdíl od vlastnoručního podpisu. Mezi záruky, které podpis zajišťuje, patří identifikace. Ta pomáhá přesně identifikovat osobu, která tento dokument podepisovala a poskytuje údaje o jeho identitě. Další věcí, co zaručený elektronický podpis garantuje je integrita dokumentu, což znamená neměnnost dokumentu. Nezaručí nám, že nemůže dojít ke změně podepsaného dokumentu, ale spolehlivě poznáme, když k této změně dojde. Poslední zárukou je nepopíratelnost. Přesněji nepopíratelnost odpovědnosti podepsané osoby resp. že podepsaná osoba nemůže tvrdit, že elektronický podpis k dokumentu nevytvořila.

Naopak existuje i pár věcí, které zaručený elektronický podpis poskytnout nemůže. Konkrétně jsou to důvěrnost, autorizace a autentizace. Pod důvěrností se rozumí, zajištění toho, aby se s jeho obsahem nemohl seznámit nikdo cizí. V praxi je možné zajistit toto pomocí šifrování, ale rozhodně ne elektronickým podpisem. U autorizace jde především o práva k určitým úkonům a pod autentičností lze chápat jako pravost dokumentu (16).

3.1.2 Princip činnosti

Princip činnosti je možno přirovnat k velmi dobře známému posílání dopisů. Běžný dopis také podepíšeme a na poště ho opatří razítkem. Není to sice nejpřesnější přirovnání, ale pro bližší představu to stačí. Připojením elektronického podpisu na konec dokumentu je vytvořen otisk dokumentu tzv. hash. Tento otisk je pomocí soukromého klíče podepisujícího zašifrován a je přidán k elektronickému podpisu. Výsledkem toho je elektronicky podepsaný dokument. Po doručení dokumentu se provede ověření pravosti dokumentu porovnáním otisku dokumentu s dešifrovaným otiskem. Otisk je dešifrován s pomocí veřejného klíče, který byl přiložený k elektronickému podpisu. Platnost klíčů je potvrzena certifikátem, který byl vydán a elektronicky podepsán certifikační autoritou. Výsledkem je ujištění příjemce, že přijatý dokument je opravdu od správné osoby a jeho obsah nebyl pozměněn (17).

3.1.3 Hashovací funkce

Jedná se o matematický algoritmus, který pracuje na principu jednosměrné transformace. Vstupní data (například dokument nebo zpráva) jsou převedena na jednoznačnou hodnotu pevné délky, kterou označujeme jako hash nebo také česky otisk. Tato hash hodnota představuje původní dokument.

Hashovací funkce mají v počítačové praxi mnoho využití. Používají se v diagnostice hardwaru, kde se například používá pro detekci chyb, u softwaru například pro implementaci tabulek nebo třeba i pro rychlejší vyhledávání a porovnávání dat.

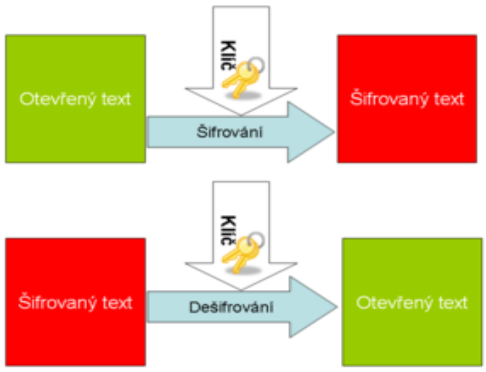
Nejpoužívanější hashovací algoritmy:

- SHA 1
- SHA 2
- MD5

3.1.4 Symetrická kryptografie

Symetrická kryptografie je šifrovací algoritmus, který využívá k šifrování i dešifrování jeden stejný klíč. Z toho vyplývá asi největší výhoda symetrické kryptografie, a tou je výpočetní rychlost. Naopak nevýhodou je, že se nejdříve obě strany musí dohodnout na stejném klíči. A z toho plyne následné nebezpečí, že může dojít k prozrazení

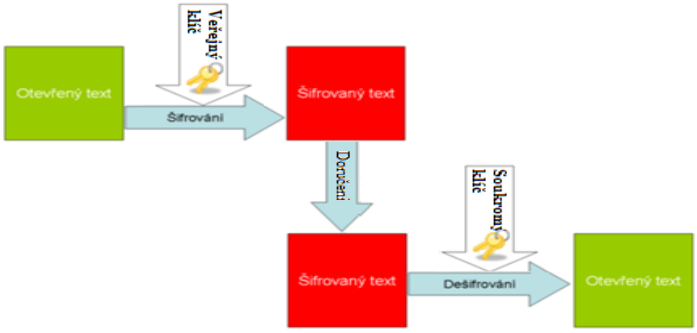
klíče jednou ze stran. Symetrické šifry dělíme na 2 druhy. Prvním jsou proudové šifry, ty zpracovávají šifru po jednotlivých bitech. Druhým jsou blokové šifry, které nejdřív rozdělí otevřený text do bloků stejné velikosti a ty pak dále zpracovává. U posledního bloku upraví velikost, aby odpovídala dané velikosti bloků (18).



Obrázek 3. Symetrické šifrování
Zdroj: http://cs.wikipedia.org/wiki/Symetrick%C3%A1_kryptografie

3.1.5 Asymetrická kryptografie

Asymetrický šifrovací algoritmus využívá na rozdíl od symetrického šifrování dva různé klíče. Prvním klíčem je veřejný klíč, a ten se využívá k zašifrování zprávy. U tohoto klíče nevadí, pokud bude kdekoliv zveřejněný. Tím druhým je klíč soukromý nebo také privátní, ten pak slouží k dešifrování přijaté zprávy. Oba tyto klíče tvoří neoddělitelnou dvojici (18).



Obrázek 4. Asymetrické šifrování
Zdroj: Upraveno: http://cs.wikipedia.org/wiki/Symetrick%C3%A1_kryptografie

3.2 Certifikáty

Certifikát je datová struktura obsahující informace o určité osobě, tzn., že ji jednoznačně identifikuje. Umožňuje spárovat tyto údaje s jeho šifrovacími klíči, respektive s jeho elektronickým podpisem. Certifikát mimo těchto údajů obsahuje:

- datum počátku platnosti
- datum ukončení platnosti
- sériové číslo

Velmi důležitým údajem je podpis certifikační autority, aby bylo možné prokázat, že daný certifikát opravdu vydala tato certifikační autorita (2).

Existuje několik druhů certifikátů, ale v převážné většině případů se lze setkat buď s certifikáty kvalifikovanými, nebo s certifikáty komerčními. Kvalifikovaný certifikát je vytvořen tak, aby splňoval požadavky dané zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů ve znění zákona č. 226/2002 Sb. Hlavní účel tohoto certifikátu spočívá v komunikaci občanů se státní správou. Využití má i pro firmy, pro něž znamená časovou úsporu a volnost (19). Naproti tomu komerční certifikát je využíván pro zasílání šifrované zprávy elektronickou poštou. Lze je využít i k jejich elektronickému podpisu. A neméně důležitou informací je, že komerční certifikáty nemusí být akceptovány při komunikaci s úřady (17).

3.3 Certifikační autorita

Certifikační autorita je důvěryhodná instituce, která je poskytovatelem certifikačních služeb. Zajišťuje registraci žádostí, vydávání nových certifikátů, správu certifikátů, archivaci a další činnosti. Vystupuje jako důvěryhodný a nezávislý subjekt, který při vzájemné komunikaci subjektů prostřednictví jim vydaných certifikátů identifikuje subjekty a jejich klíče (2).

Existují dvě úrovně certifikačních autorit. Prvním jsou kvalifikované certifikační autority, které musí splňovat všechny náležitosti stanovené zákonem, a ve své funkci mohou vydávat kvalifikované certifikáty. Pokud jakákoliv z těchto kvalifikovaných certifikačních autorit požádá stát, aby zkontroloval, zda splňuje podmínky uvedené v zákoně, a aby průběžně dál prováděl kontroly, může takové certifikační autoritě být udělena tzv. akreditace. Po udělení akreditace se z kvalifikované certifikační autority stává

akreditovaná certifikační autorita. Samotná akreditace je spíše nutný základ pro splnění požadavku na uznávanou komunikaci s orgány veřejné moci. Pro uznávaný elektronický podpis je vyžadován kvalifikovaný certifikát vydaný uznávanou certifikační autoritou (16).

V České republice jsou v současné době tři akreditované certifikační autority. Tyto autority jsou zveřejněny na webových stránkách Ministerstva vnitra ČR.

Poř. číslo	Udělena akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb	Akreditace udělena
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	15.3.2002
2.	Česká pošta, s. p. identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	15.7.2005
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	12.9.2005

Aktualizace ke dni 1.11.2011

Obrázek 5. Akreditované certifikační autority
Zdroj: www.mvcr.cz

3.4 Časová razítka

Analogii časového razítka můžeme hledat u elektronického podpisu. Zásadním rozdílem však je, že z časového razítka nelze zjistit, kdo konkrétní dokument podepsal. Informaci, kterou nám razítko poskytuje, je to, kdy bylo časové razítko k dokumentu připojeno. Vzniká tím nezpochybnitelný důkaz, jak dokument vypadal v daném okamžiku (17).

Čas je důležitý v mnoha dalších ohledech. Nejen certifikáty dříve či později pozbývají platnosti, ale s pomocí kvalifikovaného časového razítka lze přesně prokázat, kdy byl dokument odeslán nebo přijat, kdy byl podepsán a zda byl elektronický podpis v době jeho připojení platný (17).

4 Autorizovaná konverze dokumentů

Jedním z cílů e-Governmentu bylo omezení množství návštěv na úřadech a jejich nahrazení elektronickou komunikací. K této komunikaci je však zapotřebí mít potřebné dokumenty nejen v listinné podobě ale i v podobě elektronické.

V této chvíli právě nastupuje institut autorizované konverze dokumentů. Institut autorizované konverze byl do právního řádu České republiky zaveden zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi. Zajišťuje úplný převod dokumentu z digitální podoby do listinné podoby a naopak. Zároveň provede ověření shody obou dokumentů a připojí k nim ověřovací doložku. Takto vzniklý dokument má stejné právní účinky, jako originální dokument nebo ověřená kopie dokumentu.

Mohla by tu vzniknout i mylná domněnka, že při ověřování dochází i k vidimaci dokumentu, tzn. ověření pravdivosti údajů, ale jediné co je ověřeno je shoda vstupního a výstupního dokumentu.

Autorizovanou konverzi dělíme podle funkce na dvě skupiny. První je autorizovaná konverze na žádost. Ta slouží pro širokou veřejnost pro konverzi různých dokumentů. Konverzi provádí kontaktní místa veřejné správy Czech POINT. Druhou skupinou jsou autorizované konverze v moci úřední. Tato konverze slouží pouze pro vnitřní potřeby úřadů. Využívají při tom rozhraní vytvořené v rámci Czech POINT, které se nazývá CzechPOINT@Office (20).

Existuje také několik důvodů, kdy autorizovanou konverzi nelze provést:

- Jedná-li se o jedinečný dokument, který nelze konverzí nahradit (občanský průkaz, pas, řidičský průkaz, cenné papíry aj.)
- Dokument obsahuje změny, vsuvky nebo škrty, které mohou oslabit věrohodnost dokumentu
- Není jasné, zda je dokument listinné podobě prvopis, vidimovaný dokument nebo je to jen jeho kopie či opis
- Pokud dokument listinné podobě obsahuje plastický text (17)

4.1 Ověřovací doložka

Ověřovací doložka nese základní informace o provedené konverzi. K dokumentu je přiložena okamžitě poté, co je ověřena shoda vstupního s výstupním dokumentem. Ověřovací doložka připojená ke konvertovanému dokumentu nám zaručuje správnost a legitimnost dokumentu. Držitel dokumentu tak získá jistotu, že dokument vznikl procesem autorizované konverze a ne pouze vytištěním nebo oskenováním dokumentu. Ověřovací doložka má své specifické údaje pro jednotlivé typy konverze, převod dokumentu z listinné podoby do digitální obsahuje trochu jiné informace než ověřovací doložka pro dokument převedený z digitální podoby do listinné (21).

4.2 Spisová služba

Spolu s uvedením informačního systému datových schránek do ostrého provozu, vyvstal na většině úřadů jeden velký problém. Tím problémem je archivování přijatých dokumentů. Tato povinnost je dána zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. Spisová služba zajišťuje úplnou správu dokumentů v podobě listinné i digitální. Ve skutečnosti se nemusí jednat pouze o doručené dokumenty, ale i o dokumenty vzniklé z činností původce. Původcem je myšleno orgány, které mají povinnost tuto službu vykonávat, např. organizační složky státu, samosprávní celky, státní podniky, školy a školská zařízení, právnické osoby zřízené státem atd. (22).

4.2.1 Životní cyklus dokumentu

Životní cyklus dokumentu je započat okamžikem doručení datové zprávy v ePodatelně, daného úřadu. Samozřejmě to samé platí i pro dokumenty, které dorazili v listinné podobě. V další fázi cyklu jsou veškeré přijaté dokumenty zaevidovány do elektronického systému a jim přidělen jedinečný identifikátor a jednací číslo. Zaevidované dokumenty se posléze předávají příslušné organizační složce nebo pověřené osobě, která musí potvrdit jeho převzetí. Po převzetí se může začít se zpracováním dokumentu. Při vyřizování by mělo dojít ke kompletaci všech dokumentů a jejich spojení v jeden spis. Zkompletovaný a vyřízený spis je podepsán statutárním orgánem nebo oprávněnou osobou, která byla statutárním orgánem pověřena. Takto zpracovaný dokument je odeslán jeho původci.

Všechny vyřízené dokumenty a spisy je nutno archivovat. Pro jejich ukládání se zřizuje tzv. spisovna, kde jsou uloženy v listinné podobě po dobu určenou ve spisovém a skartačním řádu (po dobu trvání skartační lhůty). Poslední fází životního cyklu je vyřazení dokumentu. Jinak řečeno, když uplyne doba, po kterou měl být daný dokument archivován, je dokument fyzicky zničen nebo za určitých podmínek předán archivu k trvalému uložení (23).

4.3 Ochrana osobních údajů

Problematika týkající se ochrany osobních údajů je již dlouhodobě řešený problém. Riziko krádeže a zneužití dat nebo identity s rozvojem informační technologie značně vzrostlo. Toto vzrůstající riziko vedlo k založení „Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat“. Spolu se směrnicí Evropského parlamentu a Rady „O ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto osob“ se staly základem úpravy české legislativy a výsledkem byl zákon č. 101/2000 Sb., o ochraně osobních údajů (24).

Tento zákon jednoznačně vymezuje definice a rozdělení jednotlivých druhů osobních údajů, subjekty odpovědné za zpracování osobních údajů i způsob jak je zpracovávat nebo znehodnotit. Za osobní údaj je považována jakákoliv informace, která se týká určeného nebo určitelného subjektu. Tento subjekt lze přímo či nepřímo identifikovat, na základě jednoho či více prvků specifických pro jeho identitu. Osobní údaje můžeme dál rozdělit, a to na citlivé údaje a údaje anonymní. Citlivé údaje jsou zákonem vymezené jako konkrétní výčet vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů. Anonymní údaje je takový údaj, který je buď v původním tvaru, nebo který po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů (25).

Subjekt, který určuje účel a prostředky jakými budou dané osobní údaje zpracovávány, zpracování provádí a zodpovídá za něj, je označován jako správce. Zpracování osobních údajů je jakákoliv operace nebo soustava operací, které provádí správce nebo zpracovatel s osobními údaji. Zpracování začíná již shromážděním osobních údajů a jejich následným uchováním. Ale zpracováním se také rozumí jejich vyhledávání,

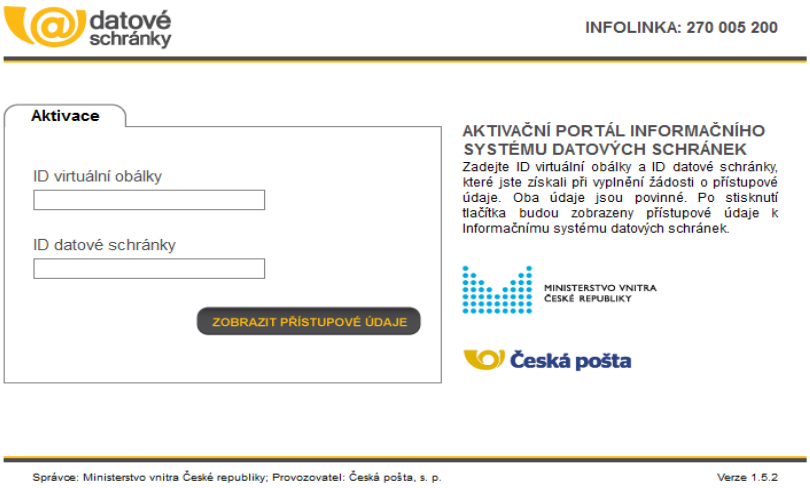
používání, předávání, výměna, zveřejňování i likvidace. Aby bylo možné s údaji jakkoliv nakládat, je potřeba souhlas se zpracováním údajů. Ten může dát jen subjekt údajů, ale ani tak s nimi nemůže být nakládáno v rozporu se zákonem (24).

5 Prostředí datových schránek

Praktická části bakalářské práce bude zaměřena na seznámení s prostředím datové schránky. První krůčky uživatele budou ukázány na webovém rozhraní Ministerstva vnitra www.mojedatovaschranka.cz. Další část bude orientována na pár aplikací, které datové schránky podporují. Vybrané aplikace jsou Multischránka a Datovka a také novinka mezi aplikace pro přistup k datové schránce Datové schránky pro Android.

5.1 Začátky s datovou schránkou

Nová cesta komunikace pro občany s úřady začíná podání žádosti a kontaktním místě Czech POINT. Po vyřízení žádosti žadatel obdrží potvrzení žádosti o zřízení datové schránky. Toto potvrzení obsahuje řadu důležitých informací počínaje číslem jednacím a identifikačním číslem pro vás zřízené datové schránky. Podrobnější instrukce, které provedou aktivací datové schránky, bude doručena poštou na adresu trvalého bydliště, nebo na emailovou adresu uvedenou v žádosti. Doručený e-mail obsahuje kromě odkazu na aktivační portál pro získání přihlašovací údaje, ale také informace odkazující na vydavatele certifikátu. Pro bezpečný přístup k datové schránce je nutné stáhnout certifikáty vydané certifikační autoritou PostSignum. Po instalaci certifikátu a přidání bezpečnostní výjimky je možné přejít k získání přihlašovacích údajů.



Obrázek 6. Aktivační portál ISDS
Zdroj: https://www.czechpoint.cz/aktivacniportal/activationLink.do?code=08473aec84a3f4144aece7b4cd7a3ac9c

V tuto chvíli je opět třeba dokument obdržený při podání žádosti. Po vyplnění dat na aktivačním portálu, dojde k zobrazení přihlašovacích údajů k datové schránce.

5.2 Přihlášení do datové schránky

Následující část bude věnována webovému portálu Informačního systému datových schránek. Úvodní stránka nabízí čtyři různé metody pro přihlášení. Všechny metody využívají uživatelské jméno a heslo, které uživatel již získal. Kromě toho tři ze způsobů přihlášení využivají další dodatečné bezpečnostní prvky, tj. certifikát, bezpečnostní nebo SMS kód. Následuje jen vyplnění CAPTCHA kódu a odeslání formuláře.

Obrázek 7. Přihlašovací formulář ISDS
Zdroj: www.mojedatovaschranka.cz

5.2.1 Ochrana certifikátem

Dodatečná ochrana pomocí certifikátu umožňuje použít při autentizaci klientský certifikát. Tento certifikát musí být vydán akreditovaným poskytovatel certifikačních služeb, ale nejedná se o certifikát kvalifikovaný, nýbrž o certifikát nekvalifikovaný nebo také nazývaný komerční či veřejný.

5.2.2 Ochrana bezpečnostním kódem

Druhou možností, jak dodatečně zabezpečit datovou schránku je použití bezpečnostního kódu. Jedná se o jednorázové heslo, které lze využít jen pro jediné přihlášení, posléze je již bezcenné, tzn., že odpadá problém vyzrazení hesla. Takový kód lze získat dvěma způsoby a to buď pomocí softwarového, nebo hardwarového generátoru.

Softwarový generátor je speciální aplikace, která nejčastěji běží na chytrých telefonech s vlastním operačním systémem. Výhoda spočívá v jejich dostupnosti, avšak nevýhoda spočívá ve ztrátě zařízení, na kterém je daná aplikace provozována. Ztráta telefonu znamená zároveň ztrátu generátoru.

Druhý způsob využívá hardwarového zařízení, které připomíná přívěšek na klíče. Skládá se z displeje a tlačítka, které po stisku tlačítka vygeneruje požadovaný kód. Výhoda tohoto zařízení spočívá v jeho jednoduchosti, tzn., že není možné ho jakkoliv zvenčí ovlivnit. Co se týče nevýhod, těch je hned několik. Za nejzásadnější lze považovat, že neexistuje žádný výrobce, který by vyráběl generátor odpovídající norně pro datovou schránku. Nemalým problém je také jeho poruchovost. V případě, že dojde k poruše zařízení, je nutné kromě výměny zařízení zařídit i zneplatnění starých přihlašovacích údajů a požádat o vydání nových.

5.2.3 Ochrana SMS kódem

Poslední možností jak zvýšit zabezpečení své datové schránky je SMS kód. Informační systém datových schránek nabízí možnost zaslání SMS zprávy s heslem na mobilní telefon. Stejně jako v předchozím případě se jedná o jednorázově vygenerované heslo, ale tentokrát zaslané přes operátora.

Tento přístup není vázán na konkrétní mobilní telefon či SIM kartu, ale na telefonní číslo. Z toho vyplývá, že i v případě krádeže mobilního telefonu nemůže dojít ke ztrátě citlivých údajů. Jediné, co je potřeba vyřídit, je zablokování původní SIM karty a vyžádat si u operátora novou SIM kartu se stejným telefonním číslem. Jediná nevýhoda spojená s tímto zabezpečením vzniká právě zainteresováním třetí strany tj., operátora, a to tím, že tato služba je zpoplatněná. Každá zaslaná SMS stojí 3 Kč.

5.3 Webové rozhraní datových schránek

Úvodní informace, která se zobrazí, při každém přihlášení obsahuje počet nově příchozích datových zpráv. Potvrzením této informace se přejde do seznamu doručených zpráv. Tato stránka obsahuje tři hlavní ovládací prvky, kterými jsou záložky Zprávy, Ověření datové zprávy a Nastavení. Již zmíněný seznam dodaných zpráv se nachází v první záložce. Kromě toho obsahuje také seznam odeslaných zpráv a záložku pro vytvoření nové datové zprávy.

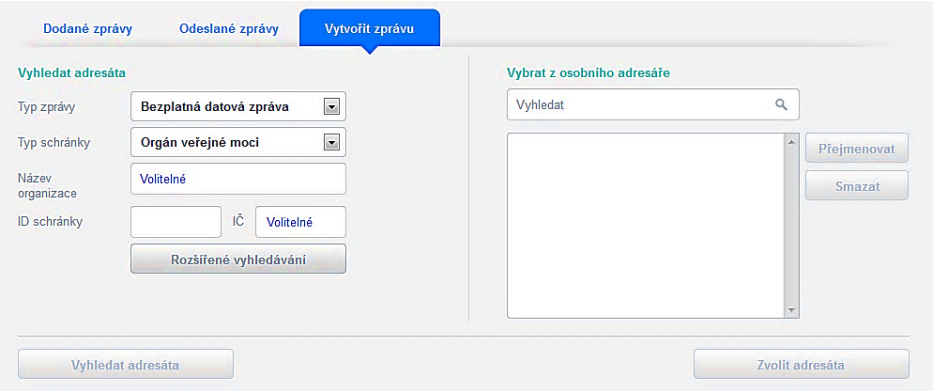
Záložka „Ověření datové zprávy“ poskytuje dvě funkce. První funkcí je ověření autenticity a neporušitelnosti datové zprávy, tzn. umožňuje vybranou staženou datovou zprávou zkontrolovat a následně podá informaci, zda je možné této zprávě důvěřovat. Druhá funkce je „Přerazítkovat“. Tato funkce slouží pro ověření dlouhodobé průkaznosti.

Systém si načte datovou zprávu, ověří ji a automaticky k ní přiloží novou rozšířenou značku, která splňuje parametry dlouhodobé průkaznosti. Jinými slovy provede obnovení časového razítka. Obě tyto funkce je možné provést u libovolné datové zprávy, a není nutné být jejím příjemcem nebo odesílatelem. Jedinou podmínkou, kterou je potřeba splnit je formát načítaného souboru *.zfo.

Poslední záložkou je „Nastavení“, ta obsahuje základní údaje o přihlášeném uživateli schránky a infomace o datové schránce. Za pozornost zde stojí možnost zásílání upozornění na příchozí zprávy do e-mailové schránky, nebo využít placené služby České pošty a nechat si posílat SMS upozornění na konkrétní číslo. Dále existuje možnost zajistit si přistup k datové schránce přes externí aplikace prostřednictvím certifikátů spisové služby nebo konkrétních hostovaných spisových služeb. Je zde velké množství dalších nastavení, ale poslední zmíněný údaj je seznam uživatelů, které mají oprávnění pro přístup k datové schránce spolu s možností přidání dalšího uživatele.

5.3.1 Vytvoření a odeslání datové zprávy

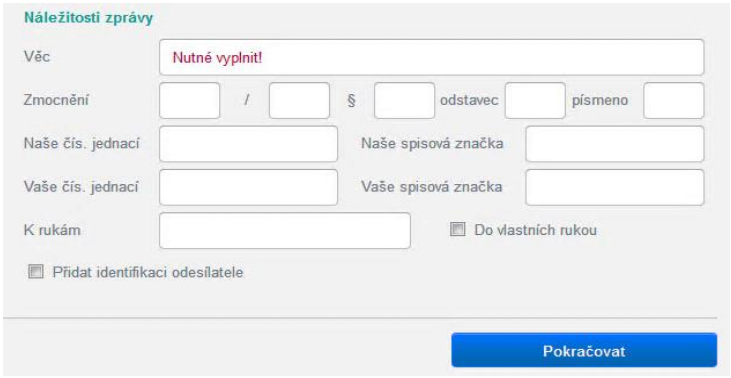
Postup vytvoření a odeslání nové datové zprávy je rozdělen do tří kroků. V prvním kroku probíhá vyhledání požadované datové schránky pomocí ID schránky. Pokud uživatel tento údaj nezná, ISDS nabízí možnost rozšířeného vyhledávání. V takovém případě je nejprve nutné vybrat typ schránky a následně zadat údaje, které datovou schránku dokáží jednoznačně identifikovat.



Obrázek 8. Vyhledání datové schránky
Zdroj: www.mojedatovaschranka.cz

Úspěšným vyhledáním datové schránky začíná druhý krok, jímž je sestavení obálky zprávy. Formulář obsahuje pouze jediný povinný údaj, podle kterého by adresát měl jednoznačně poznat důvod, proč mu byla daná zpráva zaslána. Za zmínku zde stojí políčko

Do vlastních rukou, které zprávě zajišťuje vyšší stupeň důležitosti, a políčko Přidat identifikaci uživatele, které umožní příjemci zobrazit si informace o odesílateli zprávy.

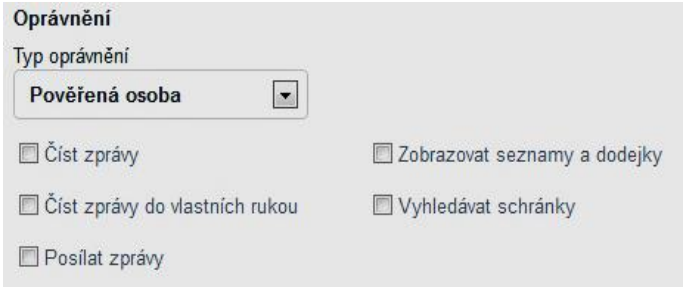


Obrázek 9. Obálka datové zprávy
Zdroj: www.mojedatovaschranka.cz

V posledním třetím kroku se už jen k datové zprávě připojí příloha. Každá datová zpráva musí obsahovat alespoň jeden dokument, jehož velikost nesmí přesáhnout 10 MB a musí splňovat požadavek na podporovaný formát. Následuje už jen odeslání sestavené datové zprávy a vypsání informace o úspěšném odeslání datové zprávy (popř. neúspěšném).

5.3.2 Přidání nového uživatele

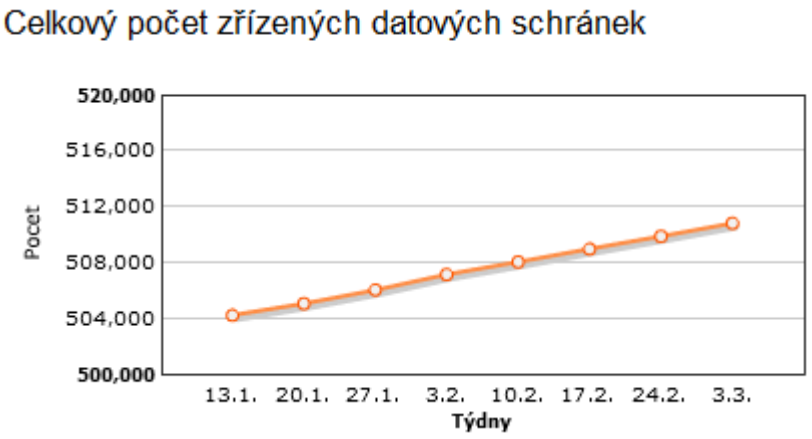
Oprávněné osobě je dána možnost poskytnout přístup k datové schránce další osobě. Tuto funkci lze nalézt na odkazu Seznam uživatelů. Zde jsou v tabulce uvedeny veškeré osoby s právem přístupu ke schránce. V případě, že potřebuje přidat nového uživatele, použije tlačítko Přidat uživatele. Otevře se formulář, ve kterém je nutné podrobně specifikovat osobu, které je umožněn přístup. Ve spodní části formuláře se nachází volba Typ oprávnění, zda se bude jednat o osobu pověřenou nebo o administrátora, a sada políček pro výběr konkrétních oprávnění.



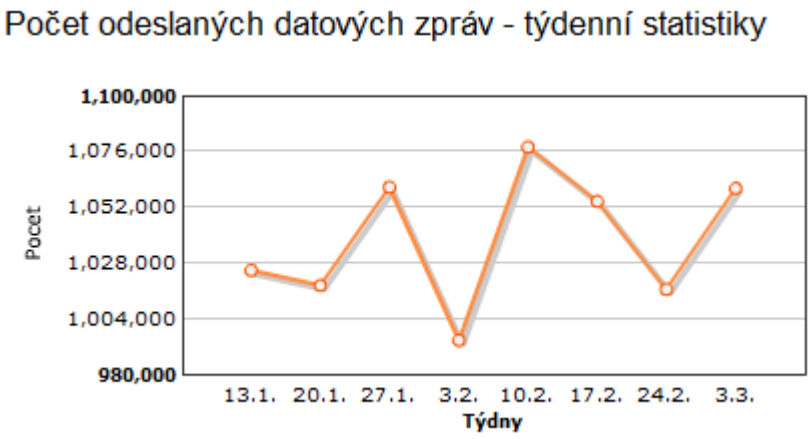
Obrázek 10. Oprávnění nového uživatele
Zdroj: www.mojedatovaschranka.cz

5.4 Statistiky datových schránek

Ze statistických údajů, jednoznačně vyplývá masivní využívání datových schránek a velká úspěšnost doručování. Již v porovnání krátkého období necelého roku, ode dne 27.5 2012 (12), kdy počet zřízených datových schránek činil 469 140, do dne 9.3 2013, kdy se tento počet navýšil na 510 799 (viz., první graf). Druhým porovnávaným statistickým údajem je celkový počet odeslaných datových zpráv, který činil ke dni 27.5 2013 - 82 492 813 odeslaných zpráv-. Během tohoto období do dne 9.3 2013 se zvýšil počet datových zpráv téměř o 40 milionů datových zpráv, a to na 120 168 540. Druhý graf ukazuje informace o počtu odeslaných datových zpráv dle týdenních statistik za poslední dva měsíce. Průměrná úspěšnost doručení přihlášením tvoří 97,4% (26).



Obrázek 11. Celkový počet zřízených datových schránek
Zdroj: http://www.datoveschranky.info

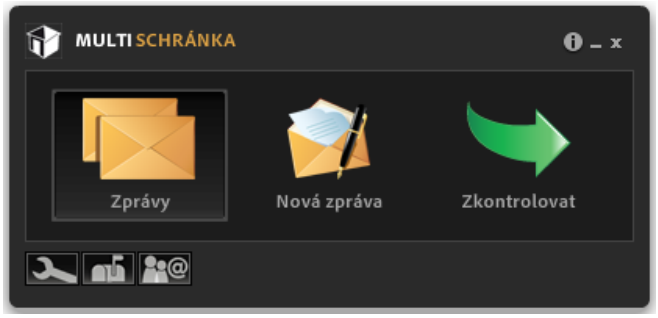


Obrázek 12. Počet odeslaných datových schránek - týdenní statistiky
Zdroj: http://www.datoveschranky.info

6 Aplikace pro správu datové schránky

6.1 Aplikace Multischránka

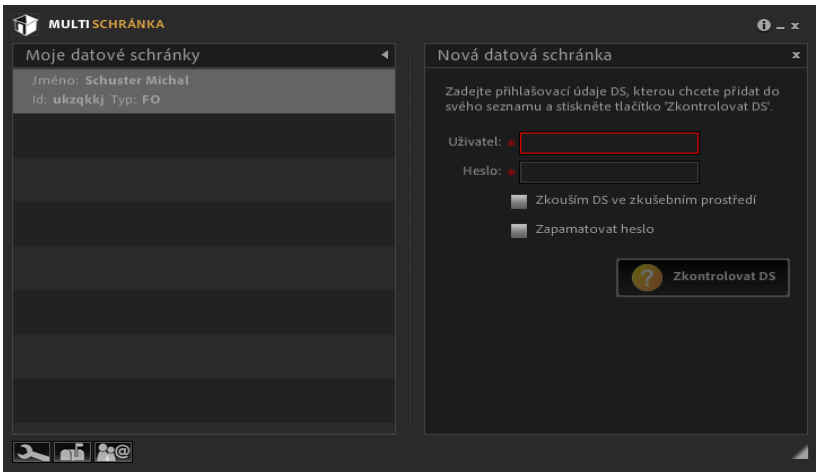
Multischránka je klientská aplikace, která slouží pro obsluhu webového rozhraní datových schránek. Nabízí úplnou a bezpečnou správu datové schránky. Tato aplikace pracuje v prostředí Adobe Air, což umožňuje využívat tuto aplikaci na operačních systémech Windows, Linux i MAC OS. Multischránka je dostupná ve dvou verzích, a to v základní verzi, která je zdarma, nebo si lze zakoupit plnou licencí.



Obrázek 13. Hlavní obrazovka Multischránky
Zdroj: Vytvořeno: aplikace Multischránka

6.1.1 Přihlášení do aplikace

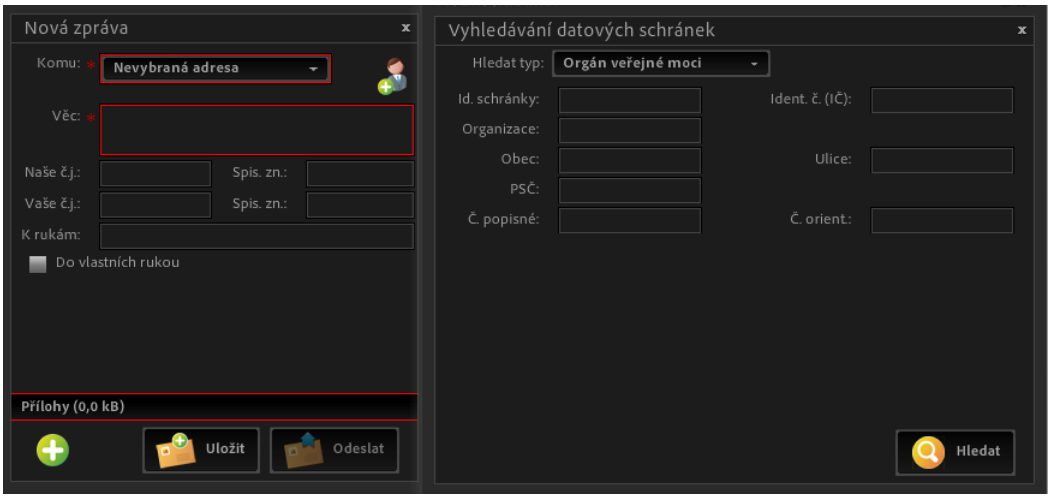
Při prvním přihlášení do aplikace, je uživatel vybídnut k vyplnění přihlašovacích údajů k datové schránce. Po zadání údajů je provedena kontrola, zda datová schránka existuje. Po potvrzení existence datové schránky se zobrazí identifikační údaje a zpřístupní se tlačítko pro přidání do seznamu spravovaných datových schránek.



Obrázek 14: Přihlášení do aplikace Multischránka
Zdroj: Vytvořeno: aplikace Multischránka

6.1.2 Správa zpráv

Hlavní obrazovka aplikace nabízí tři základní volby, a to Zprávy, Nová zpráva a Zkontrolovat. Možnost Zprávy dává přehledný výpis o přijatých a odeslaných zprávách, které je možné podle různých filtrů řadit nebo prohledávat. Tuto možnost především uvítají podnikatelé a právnické osoby, pro snadný přehled v desítkách či stovkách datových zpráv. Druhá možnost Nová zpráva nabízí možnost odesílání datových zpráv. To probíhá podobně jako ve webovém rozhraní ISDS, kde nejprve je potřeba vybrat datovou schránku, na kterou se bude zpráva posílat. Výběr datové schránky je možný z adresáře, ve kterém jsou již použité kontakty nebo přes tlačítko Doplnit adresář, kde uživatel může vyhledat další kontakty. Po zvolení subjektu, kterému bude zpráva doručena, je potřeba vyplnit předmět zprávy a přidat přílohy. V tomto okamžiku má uživatel dvě možnosti, pokud uživatel pracuje v off-line režimu, tak může datovou zprávu uložit a poslat až se připojí k internetu nebo zprávu jednoduše odeslat.



Obrázek 15. Vytváření nové zprávy
Zdroj: Vytvořeno: aplikace Multischránka

Posledním aktivním prvkem hlavní obrazovky je Zkontrolovat. Potvrzením tohoto tlačítka uživatel aktivuje hromadnou aktualizaci všech datových zpráv a v případě, že pomocí Multischránky spravuje více datových schránek, aktualizuje stavy všech datových zpráv ve všech napojených datových schránkách.

6.1.3 Porovnání s webovým rozhraním ISDS

Jak aplikace Multischránka, tak webové rozhraní ISDS dávají do rukou uživatelů datových schránek silný nástroj pro jejich správu. V oblasti správy datových zpráv nabízí

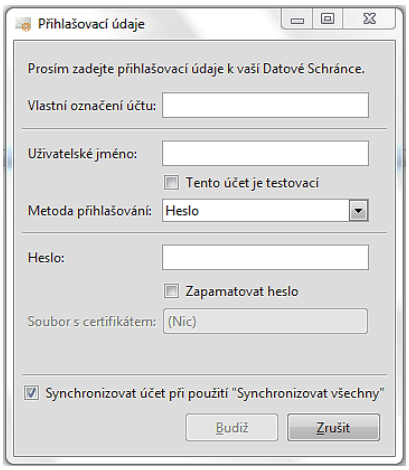
aplikace Multischránka možnost vytvořit si vlastní filtry, podle kterých je vyhledávání v přijatých a odeslaných zprávách mnohem přehlednější. Aplikace má také nadto v oblasti archivace zpráv, ISDS podle zákona uchovává zprávu po dobu 90 dní, ale naproti tomu Multischránka umožňuje zprávy uložit a tím archivovat zprávy po neomezeně dlouhou dobu. V aplikaci je dále možnost vytvořit si vlastní adresář se seznamem kontaktů, se kterými již proběhla komunikace, nebo s nimiž se komunikovat teprve chystáte. Asi největší výhodou práce s aplikací je to, že uživatel může spravovat více datových schránek najednou.

6.2 Aplikace Datovka

Aplikace Datovka je multiplatformní desktopová aplikace zajišťující přístup k Datovým schránkám od sdružení CZ.NIC. Mezi podporované platformy patří MS Windows, Mac OS a Linux ve více distribucích (Ubuntu, Fedora, OpenSUSE aj.). Mimo těchto operačních systémů sdružení vydalo verze aplikace pro mobilní zařízení, přesněji pro zařízení iPhone a iPad a pro zařízení pracující na systému Android.

6.2.1 Přihlášení do aplikace

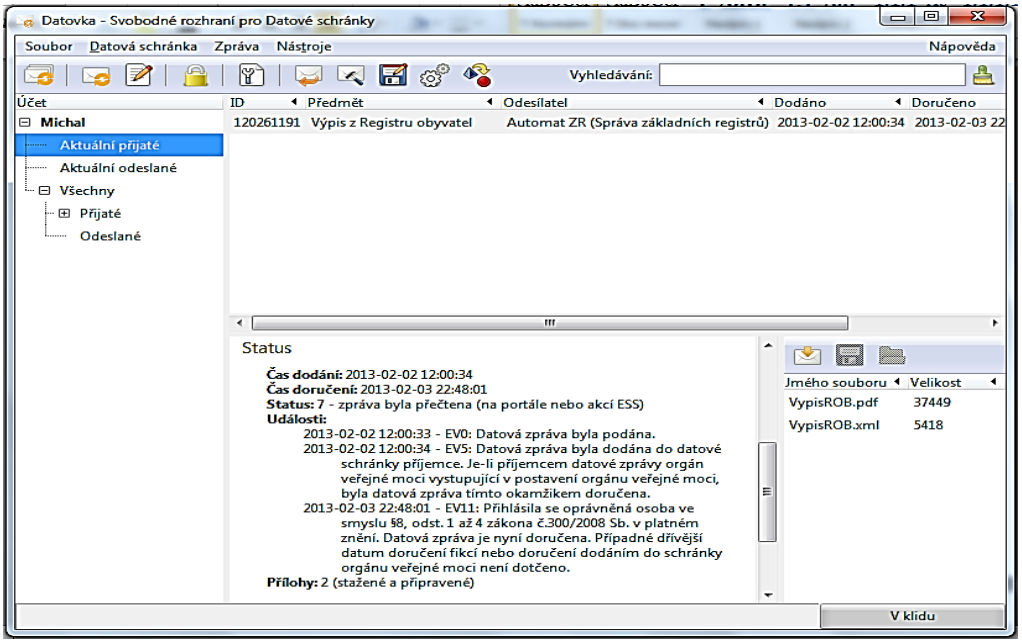
Rozhraní aplikace Datovka podporuje všechny metody autentizace webového rozhraní ISDS, tzn., že podporuje dodatečnou ochranu s pomocí bezpečnostního kódu, SMS kódu a certifikátu. Tyto metody již byly popsány v kapitole 5.2. Po vyplnění a odeslání přihlašovacích údajů se uživatel ocitá v rozhraní, které vzhledem nejvíce připomíná běžného poštovního klienta.



Obrázek 16. Přihlášení do aplikace Datovka
Zdroj: Vytvořeno: aplikace Datovka

6.2.2 Prostředí aplikace Datovka

Hlavní okno aplikace lze rozdělit na několik důležitých částí. V levé části obrazovky se nachází okno, které obsahuje účty přihlášené v aplikaci. Vybráním názvu účtu se zobrazí detailní informace o konkrétním účtu a jeho vlastníkovi. Další položky účtu obsahují všechny přijaté a odeslané zprávy a dále všechny zprávy řazené podle určitého období. Na pravé straně je zobrazen výčet zpráv, dále pak výpis stažené hlavičky zprávy a seznam přiložených příloh.



Obrázek 17. Aplikace Datovka
Zdroj: Vytvořeno: aplikace Datovka

6.2.3 Odesílání datové zprávy

Okno pro vytvoření nové datové zprávy se zobrazí aktivování třetí položky v panelu nástrojů Vytvořit a odeslat novou zprávu. Zobrazení okno vyžaduje vyplnit údaje předmět, alespoň jednoho adresáta zprávy, vyhledávání datové schránky se zobrazí po stisknutí tlačítka „+“. Vyhledání datové schránky je nezbytným úkonem při odesílání nové zprávy. Je však také možné za tímto účelem použít samostatnou funkci v menu "Nástroje". Pro úspěšné vyhledání datové schránky je nutné znát její ID, IČ příslušného subjektu nebo jeho název. Při vyhledávání pomocí názvu je potřeba uvést alespoň tři písmena ze začátku názvu. Posledním činností je připojení alespoň jedné přílohy a odeslání zprávy.

6.2.4 Datovka pro Android

Zatím nejnovějším přírůstkem do řady aplikací Datovka je mobilní aplikace pro operační systémy Android od verze 2.2. Aplikace nabízí možnost kdykoliv zkontrolovat si stav své datové schránky, přečíst si nové datové zprávy včetně příloh. Tato aplikace je v současné době ve fázi beta verze, tzn., že aplikace nemá „vychytané všechny mouchy“, a tak sdružení CZ.NIC vydává varování, že ji uživatel používá na vlastní riziko. Krom bezpečnosti je další slabou stránkou této aplikace pouze jednosměrná komunikace mezi ISDS a aplikací Datovka. V důsledku to znamená, že aplikace nepodporuje vytváření a odesílání nových datových zpráv.

6.2.5 IDatovka

Vývoj aplikace pro mobilní zařízení se neomezil pouze na operační systém Android, ale poskytuje možnost připojit se do ISDS i vlastníkům iPhone a iPad. Tato aplikace, podobně jako verze pro Android, nabízí uživatelů pouze možnost číst si a stahovat příchozí nebo odchozí zprávy, ale není zde možnost vytvářet a odesílat nové datové zprávy. Umožňuje také nastavit a následně přistupovat do více datových schránek.

Bezpečná komunikace se serverem je zde zajištěna bezpečným šifrovaným protokolem pro přenos dat TLS, tj. zamezuje odposlouchávání či falšování zpráv posílaných po síti. Dalším bezpečnostním prvkem aplikace je autorizace PINem. Aplikace pří spuštění programu požaduje zadání PIN kódů, nebo v případě byla aplikace po dobu delší pěti minut přepnuta na pozadí.

6.3 Aplikace Datové schránky pro Android

Druhou aplikací v pořadí, která dává uživatelům možnost prohlížet si svou datovou schránku, je aplikace Datové schránky. Tento software je dostupný ve dvou verzích, a to verze Datové schránky FREE a verze Datové schránky FULL. Rozdíly mezi verzemi jsou patrné na první pohled. Ve verzi FREE může uživatel přistupovat pouze do jedné schránky a při přihlášení dochází k určité časové prodlevě. Oproti tomu verze FULL nabízí možnost pracovat s libovolným množstvím schránek a obsahuje widget, který upozorňuje na nově příchozí zprávy. Nevýhodou vyvažující tyto funkce je cena tohoto produktu, která na internetové obchodu Google play činí 300 Kč.

Při práci s datovou schránkou je uživatel omezen, jako u všech aplikací pro mobilní zařízení, pouze tím, že může v datové schránce přijímat a zobrazovat zprávy, ale odesílání zpráv možné není. Aplikace také dovede archivovat zprávy, ale jen pokud k tomu uživatel zadá příkaz, tzn., že neprobíhá automatická archivace.

Obrázek 18. Android aplikace Datové schránky
Zdroj: https://play.google.com/store

V současné době tento segment trhu aplikací pro přístup k datové schránce na operačním systému ještě není úplně vyčerpán. Vyskytují se zde pouze dva produkty, které toho v praxi ještě moc neumí. Pokud uživateli stačí aplikace poskytující čtení zpráv, pak jsou tyto aplikace ideálním řešením. Vyžaduje-li uživatel možnost odeslat datovou zprávu, potom musí využít webové rozhraní mojedatovaschranka.cz, které se po odstranění závislosti na Form Filleru stalo použitelné i v prostředí mobilních zařízení. To ovšem neznamená, že bude stagnovat nabídka a neobjeví se aplikace poskytující i tuto službu.

Závěr

Česká republika spuštěním e-Governmentu nastoupila cestu postupné elektronizace veřejné správy s cílem poskytování rychlejších, levnějších a spolehlivějších služeb občanům. Hlavním úkolem bylo zajistit, aby občan, podnikatel již nemusel obíhat různé úřady za účelem vyřízení své žádosti a k tomu nemusel dokládat potřebné informace k ověření, ale aby podal svou žádost elektronickou cestou a úřad si skutečnosti k ověření zajistil z dostupných databází. Příkladem je projekt Czech POINT, kdy občan získá dokument vydávaný veřejnou správou na jednom místě. K tomu je ale třeba zajistit propojenost jednotlivých registrů veřejné správy. Sdílení databází registrů veřejné správy přispěje k efektivnějšímu a rychlejšímu fungování veřejné správy. Na základě zákona č. 111/2009 Sb., v platném znění, jsou základními registry - základní registr obyvatel, základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci, základní registr územní identifikace, adres a nemovitostí a základní registr agend orgánů veřejné moci a některých práv a povinností.

Spuštění projektu Informační systému datových schránek lze označit jako reformu veřejné správy v oblasti doručování. Projekt byl do ostrého provozu spuštěn 1. 11. 2009 a zcela změnil pravidla doručování ve veřejné správě. Datová schránka je bezpečným komunikačním prostředkem, a zároveň slouží jako krátkodobé a hlavně důvěryhodné úložiště dat. Při provozu datových schránek se objevily i vedlejší efekty, které pomohly k vyhledání tzv. mrtvých společností a opravení chybných údajů v registrech. Hlavní výhoda datových schránek je však spatřována ve zvýšené úspěšnosti doručování, a tím zvýšení vymahatelnosti práva.

Na základě zákona č. 300/2008 Sb., v platném znění jsou datové schránky automaticky zřízeny ministerstvem - právnické osobě zřízené zákonem, právnické osobě zapsané v obchodním rejstříku a organizační složce podniku zahraniční právnické osoby zapsané v obchodním rejstříku a orgánu veřejné moci, bezodkladně po jejím vzniku. Nově od 1. 7. 2012 jsou automaticky zřizovány datové schránky podnikající fyzické osobě, a to advokátům a daňovým poradcům, kterým by měly na úřady zasílat zprávy pouze prostřednictvím datové schránky.

Po zavedení Informačního systému datových schránek do plného provozu se objevila celá řada protestů a stížností, ale systém již několik let funguje bez problému

a stále přibývá uživatelů datových schránek a hlavně stoupá počet odeslaných datových zpráv.

Samozřejmě i systém datových schránek prochází vývojem a modernizací, stále dochází k jeho vylepšování. Nejběžnějším způsobem pro práci se systémem datových schránek, je použití webového rozhraní. Výhodou užití webového rozhraní je jeho snadná dostupnost, avšak lze najít i určité nevýhody, např. nedostatek informací o bezpečnostním zajištění, krátkodobé uchovávání zpráv. Další možností pro správu datové schránky je použití speciálních aplikací, které jsou uživatelsky přívětivější. Výhodou je neomezená doba archivace zpráv a s tím spojená možnost práce v offline režimu. Užití speciálních aplikací je také obecně bezpečnější. Nevýhodu lze spatřovat v nutnosti zakoupení software, jeho instalaci a aktualizaci. Konkrétně porovnávané aplikace Multischránka a Datovka nabízejí možnost pro správu jedné datové schránky verzi zdarma. Aplikace pro mobilní zařízení dávají uživatelům pouze možnost číst si a stahovat příchozí nebo odchozí zprávy, ale nemohou vytvářet a odesílat nové datové zprávy.

Informační systém datových schránek lze hodnotit jako vhodného pomocníka pro komunikaci fyzických a právnických osob s orgány veřejné moci a mezi orgány veřejné moci navzájem. Po zkušenostech z praktického využívání vlastní datové schránky a po seznámení s využíváním datové schránky v organizaci, ve které byla vykonávána bakalářská praxe, lze jen doporučit fyzickým osobám a podnikajícím fyzickým osobám, aby si datovou schránku také zřídili. A to zejména s ohledem na postupující proces elektronizace veřejné správy, kdy přibývá dokumentů, které je třeba podávat pouze v elektronické podobě, stává se datová schránka důležitým a praktickým pomocníkem. Jak vyplývá ze statistických údajů, dochází při používání datové schránky k úspoře finančních prostředků a hlavně k úspoře času uživatelů datových schránek.

Na závěr je třeba zdůraznit hlavní moto e-Governmentu: *„Úřady nemají obíhat občané, ale dokumenty v elektronické podobě“* (24 str. 11), které s přihlédnutím k aktuální statistice odeslaných datových správ, je plněno.

Seznam použitých zdrojů

1. **SMEJKAL, Vladimír.** *Datové schránky v právním řádu ČR.* Praha : AFB a.s., 2009. ISBN 978-80-86284-78-1.

2. **BUDIŠ, Petr a HŘEBÍKOVÁ, Iva.** *Datové schránky.* Olomouc : ANAG, 2010. ISBN 978-80-7263-617-4.

3. eGON jako symbol eGovernmentu. *Ministerstvo vnitra České republiky - www.mvcr.cz.* [Online] © 2010. [Citace: 20. 1 2013.] Dostupné z: http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu-moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx.

4. Ministerstvo vnitra představilo Klaudii, nový symbol eGovernmentu. *Ministerstvo vnitra České republiky - www.mvcr.cz.* [Online] © 2010. [Citace: 21. 1 2013.] Dostupné z: http://www.mvcr.cz/clanek/ministerstvo-vnitra-predstavilo-klaudii-novy-symbol-egovernmentu.aspx.

5. **LIDINSKÝ, Vít, ŠVARCOVÁ, Ivana a a kol.** *eGovernment bezpečně.* Praha : Grada, 2008. ISBN 978-80-247-2462-1.

6. Co poskytuje Czech POINT | Czech POINT. *Czech POINT.* [Online] © 2013. [Citace: 25. 1 2013.] Dostupné z: http://www.czechpoint.cz/web/?q=node/23.

7. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů. *Sbírka zákonů Česká republika.* Břeclav : Moraviapress.

8. Zákon č. 227/2000 Sb., o elektronickém podpisu. *Ministerstvo vnitra České republiky - www.mvcr.cz.* [Online] © 2010. [Citace: 21. 1 2013.] Dostupné z: http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx.

9. Portál veřejné správy. *Ministervo vnitra České republiky - www.mvcr.cz.* [Online] © 2010. [Citace: 21. 1 2013.] Dostupné z: http://www.mvcr.cz/clanek/portal-verejne-spravy.aspx.

10. Co jsou to základní registry. *szrcr.cz.* [Online] © 2010-2013. [Citace: 22. 1 2013.] Dostupné z: http://www.szrcr.cz/co-jsou-to-zakladni-registry.

11. Datové schránky a činnost správních orgánů. *Ministerstvo vnitra České republiky - www.mvcr.cz.* [Online] © 2010. [Citace: 22. 1 2013.] Dostupné z: http://www.mvcr.cz/clanek/datove-schranky-a-cinnost-spravnich-organu-871401.aspx.

12. **SMEJKAL, Vladimír a VALÁŠEK, Michal.** *Jak na datovou schránku praktický manuál pro každého.* Praha : Linde a.s., 2012. ISBN 978-80-86131-80-1.

13. Zákon č. 300/2008 Sb, o elektronických úkonech a autorizované konverzi dokumentů. *Sbírka zákonů Česká republika.* Břeclav : Moraviapress.

14. Občan - fyzická osoba | Datové schránky. *datoveschranky.cz.* [Online] © 2011. [Citace: 22. 1 2013.] Dostupné z: http://www.datoveschranky.info/obcan/.

15. Bezpečnost | Datové schránky. *datoveschranky.info.* [Online] © 2011. [Citace: 24. 1 2013.] Dostupné z: http://www.datoveschranky.info/cz/dulezite-informace/bezpecnost-id34682/.

16. **PETERKA, Jiří.** *Báječný svět elektronického podpisu.* Praha : CZ.NIC, 2011. ISBN 978-80-904248-3-8.

17. **LAPÁČEK, Jiří.** *Jak na datovou schránku a elektronickou komunikaci s úřady.* Brno : Computer press, 2012. ISBN 978-80-251-3680-5.

18. Kryptologie. *kryptologie.uhk.cz.* [Online] © 2003. [Citace: 25. 1 2013.] Dostupné z: http://kryptologie.uhk.cz/54.htm.

19. Autorizovaná konverze dokumentů. *digitální-podpis.cz.* [Online] © 2012. [Citace: 13. 2 2013.] Dostupné z: http://www.digitalni-podpis.cz/autorizovana-konverze-dokumentu.

20. Autorizovaná konverze | Czech POINT. *czechpoint.cz.* [Online] © 2013. [Citace: 20. 1 2013.] Dostupné z: http://www.czechpoint.cz/web/?q=node/362.

21. Ověřovací doložka | Czech POINT. *Czech POINT.* [Online] © 2013. [Citace: 27. 1 2013.] Dostupné z: http://www.czechpoint.cz/web/?q=node/470.

22. Zákon č.499/2004 Sb., o archivnictví a spisové službě a o změně dalších zákonů. *Sbírka zákonů Česká republika.* Břeclav : Moraviapress.

23. Spisová služba. *inkam.cz.* [Online] © 1993-2013. [Citace: 27. 1 2013.] Dostupné z: http://www.inkam.cz/SPISOVA-SLUZBA/Spisova-sluzba-a-zivotni-cyklus-dokumentu.html.

24. **MARCHAL, Stanislav A., PROKEŠ, Josef a a kol.** *Právní aspekty eGovernmentu v České republice.* Praha : Linde a.s., 2011. ISBN 978-80-7201-855-0.

25. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. *In. Sbírka zákonů Česká republika.* Břeclav : Moraviapress.

26. CZ.NIC Labs - Datovka. *CZ.NIC Labs.* [Online] © 2013. [Citace: 19. 2 2013.] Dostupné z: https://labs.nic.cz/page/969/datovka/.

27. CZ.NIC Labs - iDatovka. *CZ.NIC Labs.* [Online] © 2013. [Citace: 19. 2 2013.] Dostupné z: https://labs.nic.cz/page/1283/datovka-pro-android/.

28. CZ.NIC Labs - iDatovka. *CZ.NIC Labs.* [Online] © 2013. [Citace: 19. 2 2013.] Dostupné z: https://labs.nic.cz/page/831/idatovka/.

29. Datové schránky pro Android. *ABC Linuxu.* [Online] Argonit s.r.o., © 1999-2013. [Citace: 19. 2 2013.] Dostupné z: http://www.abclinuxu.cz/clanky/datove-schranky-na-androidu.

30. Kvalifikovaný a komerční certifikát. *bezpecnyklic.cz.* [Online] © 2010. [Citace: 25. 1 2013.] Dostupné z: http://www.bezpecnyklic.cz/bezpecnyklic/kvalifikovany_a_komercni_certifikat.html.

31. Czech POINT. *czechpoint.cz.* [Online] © 2013. [Citace: 19. 1 2013.] Dostupné z: http://www.czechpoint.cz/web/.

32. Úvodní schránka | Datové schránky. *datoveschranky.info.* [Online] © 2013. [Citace: 19. 1 2013.] Dostupné z: http://www.datoveschranky.info/.

33. Statistiky | Datové schránky. *datoveschranky.info.* [Online] © 2011. [Citace: 17. 2 2013.] Dostupné z: http://www.datoveschranky.info/cz/statistiky-id34635/.

34. Historie českého eGovernmentu. *www.czrestart.cz.* [Online] New Times Publishing, s.r.o., © 2011 - 2012. [Citace: 20. 1 2013.] Dostupné z: http://www.czrestart.cz/egovernment/historie-ceskeho-egovernmentu.

35. Datové schránky. *mojedatovaschranka.cz.* [Online] [Citace: 20. 1 2013.] Dostupné z: https://www.mojedatovaschranka.cz.

36. Občan - Portál veřejné správy. *Portál veřejné správy.* [Online] © 2013. [Citace: 24. 1 2013.] Dostupné z: https://portal.gov.cz/portal/obcan/.

Seznam obrázků

Obrázek 1. eGON a Klaudie 17
Obrázek 2. Informační systém datových schránek 21
Obrázek 3. Symetrické šifrování 29
Obrázek 4. Asymetrické šifrování 29
Obrázek 5. Akreditované certifikační autority 31
Obrázek 6. Aktivační portál ISDS 36
Obrázek 7. Přihlašovací formulář ISDS 37
Obrázek 8. Vyhledání datové schránky 39
Obrázek 9. Obálka datové zprávy 40
Obrázek 10. Oprávnění nového uživatele 40
Obrázek 11. Celkový počet zřízených datových schránek 41
Obrázek 12. Počet odeslaných datových schránek - týdenní statistiky 41
Obrázek 13. Hlavní obrazovka Multischránky 42
Obrázek 14: Přihlášení do aplikace Multischránka 42
Obrázek 15. Vytváření nové zprávy 43
Obrázek 16. Přihlášení do aplikace Datovka 44
Obrázek 17. Aplikace Datovka 45
Obrázek 18. Android aplikace Datové schránky 47

Seznam příloh

Příloha 1. Žádost o zřízení datové schránky fyzické osoby 54

Příloha


MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

datové schránky

I S 2 S a + B f W 6

Žádost o zřízení datové schránky
fyzické osoby

podle zákona č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů

Údaje o fyzické osobě

Jméno:	Příjmení:	
Druhé jméno:	Rodné příjmení:	Datum narození:

Místo narození

Místo:	Okres:	Stát:	Státní občanství:

Místo trvalého pobytu nebo jiná doručovací adresa (obligatorní údaj dle §37 odst. 2 správního řádu)

Ulice	Číslo popisné:	Číslo orientační:
Obec:	PSČ:	Stát:

Nepovinné údaje

pro adresáty, kteří chtějí být vyrozuměni o dodání datové zprávy do datové schránky

Kontaktní e-mail:

Způsoby podání žádosti:

1. Žádost doporučujeme podat osobně na libovolném kontaktním místě veřejné správy Czech POINT. Tento úkon je bezplatný a navíc vám podpis ověří rovnou na místě.
2. Žádost v elektronické podobě opatřete zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a odešlete na e-podatelnu Ministerstva vnitra (posta@mvcr.cz)
3. Žádost v listinné podobě opatřenou vaším úředně ověřeným podpisem odešlete na kontaktní adresu: Ministerstvo vnitra České republiky, Sekce rozvoje a proj. řízení ICT v oblasti veřejné správy, nám. Hrdinů 1634/3, 140 21 Praha 4.

Příloha 1. Žádost o zřízení datové schránky fyzické osoby