VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

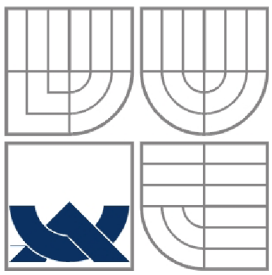
# SOFTWARE PRO OBSLUHU DATOVÝCH SCHRÁNEK

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

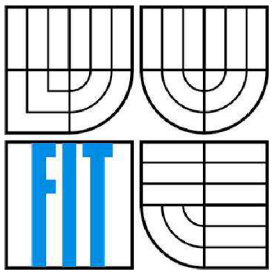
AUTOR PRÁCE
AUTHOR

PETR JANEČKA

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

# SOFTWARE PRO OBSLUHU DATOVÝCH SCHRÁNEK

SOFTWARE FOR MANAGEMENT OF DATA MAILBOXES

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

PETR JANEČKA

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. PAVEL OČENÁŠEK, Ph.D.

BRNO 2013

# Abstrakt

Tato bakalářská práce se zabývá rozborem aktuálního stavu elektronizace státní správy. Popisuje jednotlivé oblasti a jejich problémy. Dále se zaměřuje na informační technologie užívané v rámci eGovernmentu a popisuje jejich konkrétní implementaci. Pojednává o související legislativě a její aplikaci v praxi. Součástí práce je rozbor datových schránek. Stěžejní část potom tvoří návrh a implementace programu, který nahrazuje původní rozhraní pro obsluhu datových schránek.



# Klíčová slova

Datová schránka, eGovernment, datová zpráva, elektronický podpis, registry, šifrování, webové služby, certifikát, XML, SSL, legislativa



# Abstract

This bachelor's thesis deals with the analysis of the actual state of electronic government. It describes its individual sections and their problems. Also, it focuses on information technologies employed in eGovernment and describes their implementation. It elaborates on related legislature and its practical application. Part of the thesis is an analysis of data mailboxes. Pivotal section comprises design and implementation of a program which substitutes the original interface for data mailboxes operation.



# Keywords

Data mailbox, eGovernment, data message, electronic signature, registers, cryptography, web services, certificate, XML, SSL, legislature


# Citace

Petr Janečka: Software pro obsluhu datových schránek, bakalářská práce, Brno, FIT VUT v Brně, 2013.

# Software pro obsluhu datových schránek

## Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Pavla Očenáška, Ph.D. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Petr Janečka
15. května 2013

## Poděkování

Chtěl bych poděkovat vedoucímu práce panu Ing. Pavlu Očenáškovi, Ph.D. za jeho čas a vedení při vypracovávání bakalářské práce.

# Obsah

# 1 Úvod

V moderní době, kdy technika v mnoha oblastech nahrazuje či alespoň usnadňuje lidskou činnost, není divu, že se prosazuje i v rámci státní správy. Dochází tak k rapidnímu zjednodušení a urychlení úkonů jak úředních, tak občanských.

Samozřejmě spolu s výhodami elektronizace však přichází i rozličná úskalí. Ať už se jedná o problematiku bezpečnosti, která je kvůli nezastavitelnému pokroku a vynalézavosti člověka takřka vždy aktuální, či správné navržení informačního systému, je zapotřebí se s těmito úlohami vypořádat. V opačném případě lehce může dojít k situaci, kdy se přednost stává přítěží.

Tato bakalářská práce se zabývá současnými problémy elektronizace státní správy a jednotlivými technologiemi uplatněnými v této oblasti. Speciálně se zaměřuje na datové schránky a přístup k nim. Výsledkem práce je taktéž klientská aplikace, která umožňuje pracovat s datovými schránkami, přičemž je zde popsán jak její návrh, tak implementace.

V druhé kapitole je nastíněno, která dilemata nyní sužují elektronickou podobu státní správy a jaké technologie jsou využívány k řešení potřeb eGovernmentu. Taktéž je vysvětlen princip datových schránek a přistup k nim pomocí API.

Třetí kapitola je zaměřena na legislativu v rámci elektronizace. Její úlohou je přiblížit právo v této oblasti a jeho aplikaci.

Stěžejním cílem této bakalářské práce je vývoj klientské aplikace, která nahrazuje funkčnost původního rozhraní datových schránek. Její návrh je popsán ve čtvrté kapitole, zatímco popis implementace se nachází v kapitole pět, přičemž shrnutí je zdokumentováno v závěrečné části práce.

# 2 Elektronizace státní správy

Mnoho moderních zemí elektronizuje státní správu a Česká republika není výjimkou. Důvodů je hodně – lidé nemusejí stát dlouhé fronty u přepážek, náklady na prostředky a personál se redukují, přístup k informacím je diametrálně rychlejší a stejně tak jejich zpracování a odesílání, neboť velká část těchto úkonů probíhá elektronicky [1].

Elektronizace státní správy je výrazně spojována s pojmem eGovernment. Tento pojem je však v České republice mladý a nemalé procento lidí stále tíhne ke klasické osobní komunikaci na úřadech, přičemž o vymoženostech eGovernmentu nemá nejmenší tušení. Co se tedy pod tímto pojmem vlastně skrývá?

Definic je mnoho. Jednou z často užívaných pochází z publikace eGovernment bezpečně: „*eGovernment je využívání informačních technologií veřejnými institucemi pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních informačních služeb.*“ [2]

Cíl elektronizace je tedy jasný – ulehčit a zlepšit státní správu. Informační technologie poskytují širokou škálu možností, jak tohoto dosáhnout. Může se jednat například o elektronické podávání formulářů, které lidé vyplní z pohodlí domova a lehce zašlou na elektronickou adresu daného úřadu. Odpověď může následovat takřka hned, jelikož se eliminuje časová prodleva zapříčiněná zasíláním formuláře klasickou poštou či čekání ve frontách na podatelnách nebo úřadech. Významně se redukuje možnost, že by se poslaný dopis na cestě ztratil, případně že by se mu adresát vyhýbal.

Taktéž katalogizace dokumentů se stává podstatně jednodušší, neboť jejich uchovávání lze realizovat pohodlně v rámci počítačové databáze, která na rozdíl od fyzické zabírá minimální prostor. Přístup k takovéto databázi a vyhledávání v ní zabere nepatrný zlomek času ve srovnání s klasickým listinným pojetím.

Způsobů, kterými elektronizace státní správy přispívá k ulehčení běžných styků člověka s veřejnou správou, je nesčetně mnoho. Nicméně jak by se dalo očekávat, samotná elektronizace nepřináší čistě jen samá pozitiva. S nasazením informačních technologií vyvstává nemalý počet otázek, zvláště v takové sféře jakou je státní správa, která nesporně zasahuje do života každého občana.

## 2.1 Aktuální problémy

Jak již bylo zmíněno, elektronizace státní správy není úplně bezproblémovou záležitostí. Příkladem budiž zavádění nového centrálního registru vozidel, kdy celý systém zkolaboval hned v první provozní den.

Problémy však netkví jen v přechodu na nové technologie, nýbrž se mohou skrývat v mnoha jiných aspektech, ať už jde o bezpečnost či správný návrh informačního systému a odhad potřebných prostředků.

Nejčastěji se vyskytující problémy spočívají v těchto obecných okruzích:

- fragmentace informačních systémů a aplikací,
- špatná koordinace a komunikace mezi vrstvami státní správy,
- závislost na dodavateli řešení,
- směr vývoje eGovernmentu udáván spíše úředníky,
- bezpečnost.

Zejména první dva body se snaží řešit základní registry státní správy [3], kterému je věnována následující kapitola, nicméně vzhledem k různorodosti jednotlivých částí veřejné správy bude pravděpodobně ještě nějakou dobu trvat, než budou odstraněny úplně.

Specifickým problémem vyvstávajícím z prvního bodu jsou vzniklá řešení triviálních úkonů, která vyžadují použití aplikace, jež si uživatel musí nejprve nainstalovat do svého počítače. Příkladem budiž vyplňování elektronických formulářů, k čemuž je určen Software602 Form Filler[1].

Taktéž se může stát, že dané řešení není optimální či uživateli neposkytuje některé základní možnosti. Typickým případem této kategorie je rozhraní pro obsluhu datových schránek[2], jež neumožňuje uchovávat datové zprávy starší než 90 dní.

Závislost na dodavateli se v jistých oblastech může jevit jako řešitelný problém, zvláště když se přistoupí k otevřeným a veřejně dostupným technologiím, ovšem dosavadní politika vedená státem, kdy se na mnohé informační systémy vypisují zakázky pro soukromé firmy, řešení problému příliš nenahrává.

Taktéž zůstává otázkou účast občana na rozvoji eGovernmentu, jelikož vývoj má plně v režii stát. Jako hlavní překážkou se zde projevuje absence informovanosti ze strany veřejnosti. Málo lidí jeví zájem o elektronickou komunikaci se státní správou a nemalé procento dokonce ani nemá o eGovernmentu žádné povědomí [1].

Aktuálním problémem také zůstává bezpečnost a to ať už v oblasti podvržení identity, nebo například zabezpečení informačních systémů proti neoprávněnému vniknutí s cílem falšovat či zcizit data.

---

[1] volně dostupná aplikace od firmy Software602, dostupná na stránce http://www.602.cz/produkty/form_filler

[2] dostupné na http://www.mojedatovaschranka.cz

### 2.1.1 Základní registry

Základní registry jsou poměrně novou součástí českého eGovernmentu uvedenou do provozu na začátku července 2012. Jejich cílem je sjednotit klíčové databáze, které má státní správa k dispozici, a odstranit tak nejednotnost, redundanci a neaktuálnost jejich dat [4].

Samotná cesta k jejich spuštění započatá na začátku roku 2009 schválením dvou zákonů (č. 111/2009 Sb.[3] a č. 227/2009 Sb.[4]) byla doprovázena problémy a zpožděním a tento zdlouhavý proces se stal terčem kritiky.

Problémy však doprovází základní registry od spuštění až do dnešního dne. Před spuštěním informovalo Ministerstvo vnitra o jejich nepřipravenosti, což se negativně promítlo na jejich uplatnění v brzké době od jejich uvedení do provozu, kdy například některé obce byly nuceny vedle základních registrů spoléhat na klasicky získané informace (občanské průkazy, pasy) [5]. V krajním případě dokonce základní registry vůbec nebyly využity [6]. Ministerstvo vnitra původní zprávu ještě tentýž měsíc dementovalo a uvedlo, že většina problémů a rizik byla vyřešena a registry obsahují platná data [7].

S časem se nicméně projevily další nesrovnalosti [8], kupříkladu v možnosti zasílání změn osobních údajů třetím stranám (např. bance) předem určených uživatelem do druhého dne. Průběh problému začínal na faktu, že avizovaná funkce nebyla vůbec dostupná. Postupem času byla zprovozněna, avšak ne bez chyb. Zprávy o změnách údajů docházely i některým orgánům výkonné moci, což je v jejich případě redundantní, neboť mají automaticky přístup k aktuálním informacím, které se jich týkají.

Jako stěžejní problém se však projevila samotná data. Při udělení souhlasu se zasíláním o změnách může uživatel povolit zasílat pouze určitá data jako například bydliště. Jenže zpráva nemusí nutně obsahovat takové informace, které by vedly k jednoznačnému určení, o kterou osobu se jedná, čímž se tato schopnost základních registrů neguje.

Metodický postup, který popisoval východisko, byť poněkud neefektivní, byl znenadání stažen a jeho náhrada se doposud neobjevila. Komunikace a snaha problém vyřešit ze strany státu je v tomto případě nevýrazná. Jiří Peterka, konzultant v oblasti telekomunikací, dokonce uvádí, že přístup státní správy k problematice je nekonzistentní a volený způsob informování je chaotický [9].

Dalším bodem problematiky základních registrů je fakt, že vystupují hlavně jako informační základna, nikoliv jako informační systém určený k přímému použití uživateli. Proto se počítá s tím, že na registry budou postupně napojovány agendové informační systémy[5], což však v realitě neprobíhá dostatečně rychlým tempem a tato klíčová přístupová cesta k registrům tak zůstává do velké míry nevyužita [7].

---

[3] zákon č. 111/2009 Sb., o základních registrech ze dne 26. března 2009

[4] zákon č. 227/2009 Sb., Správa základních registrů ze dne 17. června 2009

[5] informační systém veřejné správy, který slouží k výkonu agendy

### 2.1.2 Centrální registr vozidel

Poměrně aktuálním tématem se jeví nový centrální registr vozidel, který má poskytovat oproti původnímu lepší bezpečnostní podmínky, dostupnost dat oprávněným osobám a vyšší robustnost. Jako stěžejní bod si klade napojení na základní registry [10].

V prvních dnech své existence se však ukázalo, že registr není schopen dostát svým cílům. Provoz doprovázely chyby, které měly za následek jeho kolaps. Mimo tento problém se projevily i jiné, například snížení rychlosti zpracovávání požadavků či obrovské množství chybných dat.

Tato situace způsobuje špatnou funkčnost souvisejících státních orgánů. Specificky lze zmínit problém měření rychlosti s pomocí kamerového systému, neboť chybné informace v centrálním registru vozidel neumožňují jasně určit pachatele přestupku.

Zásadním problémem je taktéž fakt, že centrální registr vozidel nebyl od začátku napojen na základní registry, což bylo jedním z prvotních cílů.

### 2.1.3 Elektronický podpis

Elektronický podpis je, jak již název napovídá, elektronická varianta klasického podpisu, kterým se stvrzuje platnost daného dokumentu. Nejedná se však o ruční podpis převedený do digitální podoby, nýbrž o řetězec znaků.

Specificky v souvislosti se státní správou se užívá tzv. zaručeného elektronického podpisu, k jehož sestavení se využívá asymetrická kryptografie a k ověření lze použít certifikát. Dalším pojmem je uznávaný elektronický podpis, což je bezpečnější varianta zaručeného. Certifikát k jeho ověření v tomto případě vydává poskytovatel certifikačních služeb, který je k tomuto úkonu akreditován [11].

Při užití zmíněných podpisů vyvstává problematika ověřování platnosti. S postupem vývoje informačních technologií v oblasti kryptografie není zaručeno, že někdo nemůže daný podpis získat a k souvisejícímu dokumentu vytvořit podvržený, který bude vydávat za platný. Jelikož bude dokument stvrzen tímto podpisem, bude považován za pravý a zjistit, že se jedná o podvrh, případně určit, který dokument je pravý, bude takřka nemožné.

Tento problém řeší například časové přerazítkování novým podpisem před uplynutím platnosti toho starého, což by při užití složitějšího šifrování s novým razítkem výrazně redukovalo zmíněnou hrozbu, nicméně je třeba tuto činnost provádět kontinuálně.

Jedná se však pouze o jednu z uznávaných variant. Z důvodu zachování digitální kontinuity ze zákona platí, že dokument v digitální podobě je pravý, pokud se neprokáže opak[6]. Z toho vyplývá, že dokument, u jehož podpisu vypršela platnost, můžeme stále považovat za pravý, pokud jeho pravost nikdo nezpochybní [11]. Tím se však potenciálně otevírají zadní vrátka ke zneužití.

---

[6] zákon č. 499/2004 Sb., o archivnictví a spisové službě ze dne 30. června 2004

### 2.1.4 Datové schránky

Datové schránky slouží jako elektronická úložiště určené k doručování elektronických dokumentů mezi fyzickými a právnickými osobami a orgány veřejné moci. Jejich cílem je zjednodušení a zefektivnění veřejné správy.

Představují však další problematiku v oblasti bezpečnosti. Z hlediska hrozeb je sice málo pravděpodobný úspěch útoku na samotné servery provozující datové schránky, o to víc je však možné uspět s útokem na úrovni klienta.

Na rozdíl od listinné podoby, kdy se dokumenty zasílají poštou, zde vzniká poměrně mnoho způsobů zneužití, které může útočník využít ve svůj prospěch. Uživateli, který se do rozhraní datových schránek přihlašuje pomocí hesla, může být toto heslo zcizeno například za použití „keylogger“ aplikací[7], „phishingu“[8], či v krajních případech ukradnutím samotného počítače s přístupem k datové schránce, nebo úvodní obálkou zaslanou úřadem, která obsahuje přístupové údaje. Datové schránky umožňují přihlašování také pomocí osobních certifikátů, ovšem i tyto certifikáty mohou být zcizeny a zneužity cizí osobou [12].

Problémy v této oblasti tedy hrozí zejména uživatelům, což by v případě úředníka pracujícího pro orgán veřejné moci mohlo mít za výsledek dalekosáhlé škody. Tyto problémy lze omezit snad jen obezřetností a důsledností uživatele.

Většina zmíněných bezpečnostních problémů však není vyhrazena pouze pro datové schránky. Bezpečnost a ochrana přihlašovacích údajů je zásadní otázkou takřka u každého informačního systému.

### 2.1.5 Bezpečnost osobních údajů

Již byly zmíněny specifické problémy týkající se bezpečnosti, ovšem existují i některé další společné pro celé spektrum eGovernmentu. Jak je známo, stát uchovává o občanu mnoho informací a zvláště při elektronické podobě veřejné správy otázka ochrany osobních údajů nabírá na citlivosti.

Zákon v tak komplikované oblasti, jakou informační technologie představují, nedokáže dokonale pokrýt všechny případy a možnosti zneužití. Ovšem hrozba se nutně nemusí objevit z cizí strany. Elektronické evidence mohou někdy zlákat úředníka k tomu, aby shromažďoval a uchovával více a informací než je zapotřebí, a to i v době, kdy nutnost získávání potřebných dat již nebude aktuální [1].

---

[7] program, který zachytává stisknutí jednotlivých kláves

[8] podvodné vydávání se za důvěryhodnou instituci (např. banka) za účelem získat z uživatele citlivé informace, nejčastěji se provádí pomocí emailových zpráv, které odkazují na internetové stránky shodné se stránkami instituce, za kterou se útočník vydává

## 2.2 Užívané technologie a nástroje

Jelikož je elektronizace státní správy do velké míry záležitostí informačních technologií, je nasnadě, že bude využívat rozličné množství nástrojů. Jedním ze základních stavebních bloků eGovernmentu jsou informační systémy založené na databázových technologiích. Tyto systémy využívají k autentizaci hesla, která bývají v průběhu přenosu zpravidla šifrována. Nemalé množství informačních systémů také poskytují webová rozhraní, která jsou implementovány pomocí jazyků HTML, PHP či platformy ASP.

Vzhledem ke snaze zajistit interoperabilitu dostupných služeb je kladen důraz na disponování aplikačním rozhraním, které by umožnilo vzájemnou komunikaci mezi informačními systémy. Příkladem takové služby jsou datové schránky.

Dalším aspektem je využití otevřených standardů, což značně usnadňuje nejen vývoj, ale také správu a komunikaci mezi jednotlivými bloky elektronizace státní správy. Typickým příkladem je značkovací jazyk XML.

Speciálním, avšak často skloňovaným výrazem v eGovernmentu je elektronický podpis, který již byl popsán v předchozí kapitole. Jeho technologické aspekty zahrnují nemalou řadu kryptografických technik, hashovacími algoritmy počínaje a certifikáty X.509 konče [11].

### 2.2.1 Hashovací algoritmus

Elektronická podoba státní správy ke své funkci nepochybně potřebuje elektronické dokumenty. Tyto dokumenty mohou být různého charakteru, například lze hovořit o úředním rozhodnutí. Aby bylo zajištěno, že se nejedná o podvrh, je vhodné jej opatřit nějakým jasným a nezfalšovatelným identifikátorem. Tím je právě elektronický podpis, založený na asymetrické kryptografii.

Jenže vytvářet podpis vycházející z dat celého dokumentu by nemuselo být ideální a praktické vzhledem k jeho velikosti. Je tedy na místě užít nějaký způsob, který by značně redukoval množství dat a přesto bylo jasné, že se jedná o daný dokument.

V tomto případě se více než nabízí hashovací algoritmy. Jedná se o funkce, které převádějí vstupní data na relativně malé číslo. Zároveň musí být jednocestné, aby s jejich pomocí nebylo možné zpětně rekonstruovat vstupní data. Taktéž je krajně nepravděpodobné, že by jeden tzv. otisk připadal na více vstupních zpráv, čímž se zaručí jednoznačnost otisku. Typickými představiteli těchto algoritmů jsou například MD5 či SHA-1 [13].

| **Algoritmus** | MD5 | SHA-1 | SHA-224 | SHA-256 | SHA-384 | SHA-512 |
|---|---|---|---|---|---|---|
| **Maximální délka vstupu** | $2^{64}$-1 bitů | $2^{64}$-1 bitů | $2^{64}$-1 bitů | $2^{64}$-1 bitů | $2^{128}$-1 bitů | $2^{128}$-1 bitů |
| **Výsledná délka** | 128 bitů | 160 bitů | 224 bitů | 256 bitů | 384 bitů | 512 bitů |

**Tabulka 1:** porovnání délek výstupů vybraných hashovacích algoritmů [13]

Taková funkce vytvoří krátký otisk, který je jednoznačný pro daný dokument, a tudíž lze zaručit, že utvoření elektronického podpisu na jeho základě je takřka totéž, jako by byl podepisován původní dokument. Stejně tak tyto funkce zaručují, že při změně dokumentu se vypočitatelný otisk změní, tudíž původní vygenerovaný se nebude s ověřovaným výpočtem shodovat, čímž lze dokumenty ochránit proti dodatečným změnám.

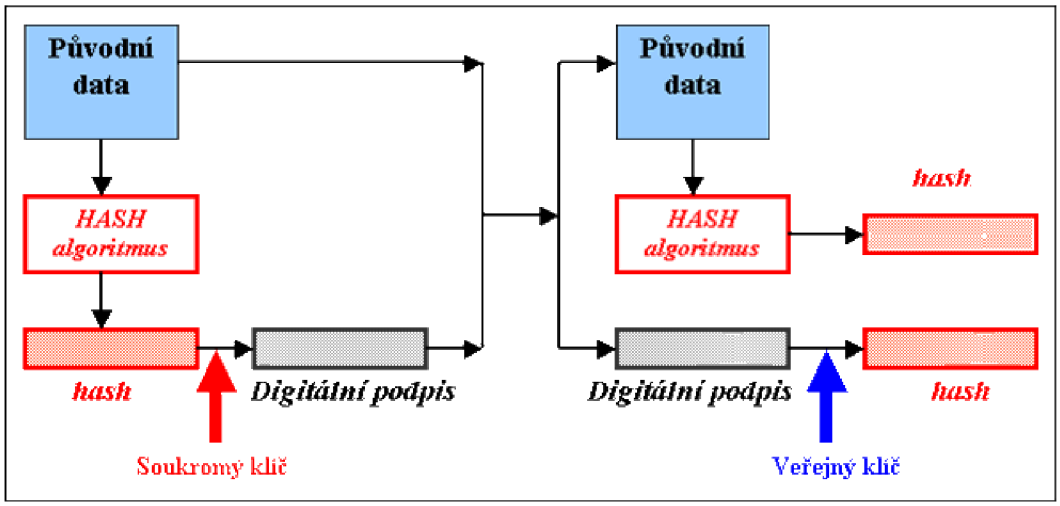
Samozřejmě vzhledem k postupujícímu vývoji v informačních technologiích je možné, že časem vznikne pro daný hash kolizní dokument či někdo algoritmus prolomí. V tomto případě dochází k obměně užívaného algoritmu, přičemž aktuálně používaná je například rodina SHA-2 [14].

### 2.2.2 Asymetrické šifrování

Dalším podstatným nástrojem užívaným nejen v rámci elektronických podpisů je asymetrická kryptografie. Její asymetričnost spočívá v tom, že je použit pár klíčů, kdy jeden z nich je veřejně dostupný a další tajný.

V praxi tento způsob šifrování funguje tak, že se daná zpráva zašifruje pomocí veřejného klíče, ovšem dešifrovat ji jde pouze pomocí privátního klíče, který zná jen příjemce zprávy [15]. Nevýhodou oproti symetrickému šifrování je pomalost, nicméně se jedná o bezpečnější variantu.

V případě elektronického podpisu ovšem princip této metody kryptografie funguje obráceně. Hash dokumentu je zašifrován pomocí soukromého klíče a k ověření slouží klíč veřejně dostupný.




**Obrázek 1:** diagram šifrování v rámci elektronického podpisu [16]

Nejčastěji se pro tyto účely používají algoritmy RSA (podle autorů – Ron Rivest, Adi Shamir a Leonard Adleman) a DSA (Digital Signature Algorithm), přičemž minimální délka prvního zmíněného je stanovena na 2048 bitů [17].

Samotný RSA algoritmus pro vytvoření klíčů je pak následující [18]:

1. zvol 2 prvočísla $p$ a $q$,
2. spočti $n$, kde $n = pq$,
3. najdi takové $e$, pro které platí $3 < e < (p-1)(q-1)$ a zároveň největší společný dělitel $e$ a $(p-1)(q-1)$ je roven 1,
4. najdi takové $d$, pro které platí $ed = 1 \pmod{(p-1)(q-1)}$,
5. veřejný klíč je pak dvojice čísel $e$ a $n$, privátní tvoří dvojice $d$ a $n$.

Při šifrování se zprávy se následně využije rovnice

$$C = M^e \pmod{n},$$

kde $C$ je zašifrovaná zpráva, $M$ je vstupní text, $e$ a $n$ jsou čísla získaná z předchozího algoritmu. Pro dešifrování se uplatní obdobná rovnice:

$$M = C^d \pmod{n}$$

Algoritmus DSA je druhou užívanou variantou. Ke své funkci potřebuje nejprve definovat následující hodnoty [19]:

- prvočíslo $p$, dlouhé $L$ bitů, přičemž platí $512 \le L \le 1024$ a $L \bmod 64 = 0$,
- číslo $q$ o velikosti 160 bitů, který je prvočinitelem čísla $p - 1$,
- číslo $g$, pro které platí $g = h^{(p-1)/q} \bmod p$, přičemž $h < p-1$ a $h$ musí být takové číslo, aby platilo $h^{(p-1)/q} \bmod p > 1$,
- privátní klíč $x$ splňující podmínku $x < q$,
- veřejný klíč $y$ dle rovnice $y = g^x \bmod p$,
- jednocestná hashovací funkce $H(m)$.

K podpisu a verifikaci zprávy pomocí DSA se pak uplatní následující algoritmus [19]:

1. zvolení $k$ takového, aby platilo $0 < k < q$,
2. vypočítaní dvojice čísel $r$ a $s$ tvořící podpis dle rovnic:

$$r = (g^k \bmod p) \bmod q$$
$$s = (k^{-1}(H(m) + xr)) \bmod q$$

3. verifikování podpisu následujícím postupem:

$$w = s^{-1} \bmod q$$
$$u_1 = (H(m) * w) \bmod q$$
$$u_2 = (rw) \bmod q$$
$$v = ((g^{u_1} g^{u_2}) \bmod p) \bmod q$$

přičemž pokud $v = r,$ pak byl podpis verifikován.

### 2.2.3 Certifikáty

Certifikáty jsou nástroji, které hrají významnou roli při ověřování pravosti elektronických podpisů. Při ověřování podpisu můžeme mít sice veřejný klíč k tomuto určený, ovšem kdo zaručí, že tento klíč je autentický a není třeba tvorbou někoho jiného, kdo chce vydávat svůj podpis za náš? Z tohoto důvodu je vhodné, aby nějaká třetí strana zaručila autenticitu daného klíče. Touto třetí stranou může být státem stanovená důvěryhodná certifikační autorita, která vystaví certifikát o daném klíči, čímž se zaručí, že se opravdu jedná o pravý klíč [11].

V rámci českého eGovernmentu se nejčastěji využívají certifikáty definované standardem X.509, který se věnuje certifikaci veřejných klíčů. Struktura takového certifikátu je tvořena atributy obsahující informace o něm a podpis autority, která certifikát vydala.

| Atribut | Atribut (česky) | Význam |
|---|---|---|
| **Version** | Verze | Verze certifikátu X.509, nabývá hodnot 0 až 2, každá z těchto hodnot popisuje specifickou verzi X.509 certifikátu od 1 až 3 |
| **Serial Number** | Sériové číslo | Sériové číslo certifikátu, které je unikátní v rámci vydavatele certifikátu |
| **Signature Algorithm** | Algoritmus podpisu | Identifikátor algoritmu podpisu certifikátu |
| **Issuer** | Vydavatel certifikátu | Identifikační údaje certifikované autority, která certifikát vystavila |
| **Validity** | Platnost | Platnost certifikátu; v rámci tohoto atributu jsou definovány dva atributy - atribut **Not Before** specifikující počátek platnosti a **Not After** specifikující konec platnosti |
| **Subject** | Subjekt | Identifikační údaje subjektu, kterému byl vystaven certifikát |
| **Subject Public Key Info** | Informace o veřejném klíči subjektu | Informace o certifikovaném klíči, obsahuje podatributy specifikující algoritmus a vlastnosti veřejného klíče |
| **Extensions** | Rozšíření | Nepovinný Atribut obsahující informace o dodatečné informace o certifikátu |

**Tabulka 2**: atributy certifikátu X.509 [20]

### 2.2.4 SSL/TLS

Dalším kryptografickým mechanismem na poli eGovernmentu je protokol TLS a jeho předchůdce SSL[9]. Užívá se k zabezpečení internetové komunikace. Může se jednat například o interakci uživatele s webovou stránkou informačního systému, pomocí kterého se přihlašuje, požaduje či zadává data.

Tyto protokoly si lze představit jako vrstvu mezi aplikační a transportní vrstvou TCP/IP, která zajišťuje nejen zabezpečené připojení, ale i odesílání a příjem dat. Používá se ve spolupráci s aplikačními protokoly jako FTP, SMTP či XMPP, avšak nejčastěji se spojuje s HTTP protokolem pro vytvoření nadstavby HTTPS. SSL a TLS poskytují pět následujících subprotokolů [21].

- **Record Protocol** sloužící k obalení dat vyšší vrstvy.
- **Handshake Protocol** určený k vytváření spojení, s jehož pomocí se obě strany na začátku spojení domluví na způsobu komunikace (fragmentace, šifrování, komprimace).
- **Change Cipher Spec Protocol** je protokol, sloužící k signalizaci změny způsobu šifrování.
- **Alert Protocol** sloužící k zasílání výstrah. Tyto výstrahy se dělí do dvou skupin – varovné a fatální. Zprávy z druhé skupiny mají za následek ukončení spojení.
- **Application Data Protocol** určený k výměně dat mezi oběma stranami dle smluveného formátu komunikace.

### 2.2.5 XML

XML[10] je značkovací jazyk, který slouží k přenosu a ukládání dat. Jeho výhodou je otevřenost a široká uplatnitelnost. Uživatel může sám definovat vlastní značky, které bude užívat, což činí XML užitelným v podstatě kdekoliv.

XML soubory mají stromovou strukturu. První značku tvoří XML deklarace. Následuje otevírací značka tzv. kořenového elementu, který obsahuje data celého dokumentu. V rámci dokumentu může existovat pouze jediný kořenový element. Všechny ostatní elementy jsou jeho potomky. Konec dokumentu je uzavřen koncovou značkou kořenového elementu. Dané elementy v sobě mohou zapouzdřovat další podelementy a obsahovat data. Také mohou být blíže specifikovány atributy zapsanými ve formátu `atribut="data"` [22].

Příkladem XML dat jsou následující řádky:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<koren>
   <element atribut="hodnota">zprava</element>
   <dalsi_element>text</dalsi_element>
</koren>
```

[9] Transport Layer Security, resp. Secure Sockets Layer

[10] Extensible Markup Language

V rámci eGovernmentu se XML užívá například pro předávání dat mezi informačními systémy, pro elektronické formuláře či dokumenty spisových služeb. Je v podstatě jedním ze stavebních bloků elektronické státní správy.

### 2.2.6 Webové služby

Mimo přístup k informačním systémům veřejné správy pomocí webových stránek existují i různé desktopové aplikace. Často se jedná o aplikace vyvinuté třetími stranami, jejichž účelem je poskytnout zákazníkovi alternativu oproti webovému rozhraní. Tyto programy však k datům na vzdálených serverech také nějakým způsobem přistupují a prostředky, které k tomu využívají, se nazývají webové služby [23].

Dle W3C[11] jsou definovány takto: „*Webová služba je softwarová aplikace identifikovaná URI, jejíž rozhraní je možno definovat, popsat a prozkoumat pomocí XML a podporuje přímé interakce s jinými aplikacemi za užití XML zpráv prostřednictvím internetových protokolů.*“ [24]

Jedná se v podstatě o služby poskytované na určité webové adrese, které aplikace využívají. Mají rozhraní, pomocí kterého k nim lze přistupovat a které je ve většině případů poskytovatelem dokumentováno.

Výhodami webových služeb je jejich interoperabilita [25], která zaručuje, že spolu jejich prostřednictvím mohou komunikovat i různé operační rodiny operačních systémů jako například Windows či Linux.

Jejich současný vývoj směřuje k užívání jednodušších architektur [26], přičemž typický představitel je REST[12]. Nicméně dnes na poli webových služeb stále převládá trojice následujících součástí vycházejících z XML [27].

- **Protokol SOAP** (Simple Object Access Protocol), který slouží k výměně dat po síti, typicky s pomocí protokolu HTTP.
- **Jazyk WSDL** (Web Service Description Language), který popisuje funkcionalitu služeb a jejich způsob volání, očekávané vstupní parametry a výstupy.
- **Jazyk UDDI** (Universal Description Discovery and Integration), který popisuje dostupné služby.

V souvislosti s eGovernmentem jsou webové služby užívány v různých odvětvích státní správy. Jsou k dispozici například pro katastr nemovitostí, územně identifikační registr adres či základní registry.

---

[11] World Wide Web Consortium, organizace vytvářející internetové standardy

[12] Representational State Transfer, architektura rozhraní navržená Roy Fieldingem v roce 2000

## 2.3 Analýza datových schránek

Jak již bylo řečeno, datové schránky slouží jako datové úložiště pro elektronické dokumenty. Jedná se o službu provozovanou Českou poštou, která je velmi podobná emailu. Existují však jisté rozdíly. Na rozdíl od elektronické pošty datová zpráva postrádá tělo. Obsahuje tedy jen hlavičku, která určuje od koho zpráva pochází a komu je určena, a přílohu, například formulář ve formátu PDF. Velikost všech příloh datové zprávy je limitována na 10 MB [28].

Cílem datových schránek je zefektivnění státní správy, což se projevuje zejména díky elektronickému zpracování původně fyzické pošty. Odpadá tak časová prodleva způsobená přepravou dopisů, čekání ve frontách, vedení formulářů v kartotékách apod. Datové schránky spadají pod informační systém datových schránek ISDS, který obsahuje nejen je, ale i údaje o uživatelích.

Původně byly datové schránky určeny pro doručování zpráv mezi orgánem veřejné moci a fyzickou či právnickou osobou. Ovšem dnes již se komunikace může odehrávat i mezi firmami či soukromými osobami, i když je tato funkčnost zpoplatněna [29].

Ze zákona[13] je zřízena datová schránka každé právnické osobě zapsané v obchodním rejstříku automaticky. Ostatní subjekty mohou bezplatně zažádat o její zřízení například podáním patřičného formuláře na úředním místě Czech POINT.

Z pohledu vlastníka se pak rozlišují čtyři typy datových schránek [30], které mají na funkcionalitu marginální vliv:

- orgánu veřejné moci,
- fyzické osoby,
- podnikající fyzické osoby,
- právnické osoby.

Každá datová schránka má svůj vlastní identifikátor podobně jako email. Tento identifikátor je krátký alfanumerický řetězec, který je jednoznačně asociován s vlastníkem schránky. Díky němu je možné vyhledat jejího vlastníka a zjistit tak číslo datové schránky například za účelem odeslání zprávy.

K přihlašování do datové schránky se však spíše používá uživatelské jméno, což je opět alfanumerický řetězec. Uživatele dané datové schránky lze přidávat, měnit jim pravomoci či je smazat. Datová schránka tedy může mít různý počet uživatelů reflektující kupříkladu určitou obchodní společnost.

Způsoby přístupu k datové schránce jsou v podstatě dvojí. Buď může uživatel využít dostupné webové rozhraní informačního systému datových schránek ISDS, nebo má možnost použít aplikace třetích stran.

---

[13] zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi ze dne 17. července 2008

V prvním případě se lze přihlašovat hned několika možnostmi:

- uživatelským jménem a heslem,
- certifikátem (X.509) ,
- uživatelským jménem, heslem a SMS kódem,
- uživatelským jménem, heslem a bezpečnostním kódem.

Webové rozhraní je stavěno na HTTP protokolu se šifrováním dle TLS. Kromě tohoto přístupu lze použít taktéž aplikací třetích stran, které ke komunikaci s ISDS využívají aplikační rozhraní datových schránek.

API je založeno na technologiích webových služeb, konkrétně protokolu SOAP ke komunikaci a WSDL pro popis funkcí. Tyto funkce pokrývají většinu možností webového rozhraní. Lze s jejich pomocí manipulovat s datovými zprávami, spravovat datové schránky a vyhledávat jiné. Funkčnost API dokáže nahradit původní webové rozhraní datových schránek.

### 2.3.1 Dostupné aplikace

Byť jsou datové schránky projektem státní správy a tudíž mají webovou aplikaci, s jejíž pomocí je lze ovládat, existují i aplikace třetích stran, které využívají aplikační rozhraní datových schránek.

Důvody, proč existují tyto programy, jsou různé. Původní rozhraní poskytuje pouze základní funkcionalitu, například neumožňuje shlukovat zprávy dle skupin či složek. Taktéž významným omezením je lhůta 90 dnů, která určuje životnost datové zprávy. Po uplynutí této doby se datová zpráva maže ze schránky.

Dostupné aplikace jsou buď webové, desktopové, nebo jsou to konektory pro jiné programy (např. MS SharePoint). Ve většině případů se jedná o komerční produkty vhodné svou cenou spíše pro větší firmy.

| Aplikace | Typ aplikace | Funkcionalita |
|---|---|---|
| **Evolio**[14] | desktopová, komerční | převod zpráv do PDF, uchovávání zpráv i po 90 dnech, práce s více DS i uživateli |
| **Ixtent**[15] | konektor, komerční | podpora více datových schránek, lze spojit s MS Outlook, Sharepoint, SAP |
| **postregistr.cz**[16] | webová, komerční | propracované filtry dle různých kritérií, např. podle určení uživatelským účtům |

**Tabulka 3:** srovnání některých dostupných aplikací

[14] dostupné na http://www.datoveschranky.com

[15] dostupné na http://www.jaknadatoveschranky.info/

[16] dostupné na http://www.postregistr.cz/index.php?option=com_content&view=article&id=11&Itemid=12

# 3 Legislativa a eGovernment

Spolu s elektronizací státní správy přichází také otázka, jak eGovernment zajistit po stránce právní. Je mnoho aspektů, se kterými je spjatý, a aby byly dostatečně zabezpečeny, musí být jasně vymezeny legislativou.

Například datové schránky jsou popsány zákonem č.300/2008 Sb.[17] Informační systémy státní správy popisuje zákon č. 365/2000 Sb.[18] I pro elektronický podpis byl vytvořen zákon, specificky č. 227/2000 Sb.[19]

## 3.1 Elektronický dokument

V rámci elektronické komunikace vzniká mnoho dokumentů, ať už se jedná o obyčejné dopisy či úřední usnesení. Nemálo z nich pak vzhledem k dnešní technické úrovni substituuje původní fyzické listiny. Elektronická podoba státní správy například umožňuje občanům podávat daňové přiznání přes digitální formuláře, či úřadům vydávat rozhodnutí s pomocí datových zpráv.

Tyto dokumenty lze podepsat elektronickým podpisem, čímž vlastník podpisu stvrzuje svou vůli stejně jako v klasické podobě ručního podpisu. Teoreticky by se tak měla zajistit platnost dokumentu a mělo zabránit zneužití nepověřenou osobou. Ovšem jak již bylo zmíněno dříve, ne vždy tomu tak musí být.

V soudnictví odjakživa byly používány důkazy v podobě papírových listin, nicméně v dnešní době lze době užívat i elektronických dokumentů ke stejnému účelu [31]. Je kupříkladu možné použít zmíněné daňové přiznání jako důkazní materiál dosvědčující, že daný člověk zatajil příjmy a dopustil se krácení daní. Samozřejmě platí, že důkaz musí být věrohodný, což může být zaručeno právě kvalifikovaným elektronickým podpisem.

Ze zákona je dané, že digitální dokument podepsaný platným uznávaným elektronickým podpisem či elektronickou značkou osoby je pravý, pokud se neprokáže opak[20]. V případě, že je dokument opatřen platným elektronickým podpisem (tedy nedošlo k žádnému podvržení, například dodatečným změnám), je vše v pořádku.

Ovšem pokud je podpis ve skutečnosti podvrh či již není platný, může nastat problém [11]. Takový dokument může být použit u soudu jako důkazní materiál a v případě, že nikdo nezpochybní jeho platnost, není vyloučeno, že tím neprávem vzniknou škody určité straně zúčastněné v soudním řízení.

---

[17] zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi ze dne 17. července 2008

[18] zákon č. 365/2000 Sb., o informačních systémech veřejné správy ze dne 23. října 2000

[19] zákon č. 227/2000 Sb., o elektronickém podpisu ze dne 29. června 2000

[20] zákon č. 499/2004 Sb., o archivnictví a spisové službě ze dne 30. června 2004

Z tohoto hlediska zákon[21] stanovuje několik úprav, které přinášejí odpovědnost jak vlastníkovi soukromého klíče podpisu, tak straně, která se na platnost daného elektronického podpisu spoléhá [11]. Stejně tak ukládá povinnosti certifikačním autoritám, jejichž certifikáty stvrzují elektronické podpisy.

Podepisující osoba dle práva musí zacházet s elektronickým podpisem tak, aby nedošlo k jeho zneužití, a v případě nebezpečí je povinna neprodleně informovat certifikační autoritu, která certifikát vystavila.

Avšak pokud tato osoba prokáže, že ten, komu vznikla škoda, nepodnikl všechny potřebné kroky k ověření určitého digitálního dokumentu, zůstává škoda na něm a odpovědnosti je podpisovatel zproštěn.

V případě, že certifikační autorita nezajistí dostatečné prostředky umožňující potvrzení identity podpisovatele a pravosti dokumentu, zákon sice nestanovuje, kdo zodpovídá za vzniklé škody, nicméně ukládá této autoritě pokutu.

Dalším aspektem v rámci elektronických dokumentů a jejich platnosti je bezpochyby technická realizace elektronického podpisu. Jak již bylo zmíněno dříve, uznávaný elektronický podpis je založen na asymetrické kryptografii a hashovacích algoritmech.

Postupem času se však informační technologie vyvíjí a výpočetní technika tak může snáze prolomit algoritmy, které dříve byly považovány za bezpečné. Z tohoto důvodu je ve vyhlášce č. 378/2006 Sb. definováno, že kryptografické algoritmy používané v této oblasti zveřejňuje ministerstvo na své úřední desce. Aktuálně platí, že pro kvalifikované certifikáty vydávané certifikačními autoritami je užívána rodina hashovacích algoritmů SHA-2 a minimální přípustná délka kryptografického klíče dle algoritmu RSA je 2048 bitů [17].

## 3.2 Informační systémy

Elektronická správa disponuje počtem informačních systémů, které slouží rozličným účelům. Namátkou lze vyjmenovat informační systém datových schránek či informační systém o datových prvcích.

Obecně z hlediska bezpečnosti, která je v této oblasti eGovernmentu klíčová, platí, že pokud existuje povinnost jejího zajištění z právního předpisu a tato povinnost není dodržena, jedná se o správní delikt [31].

Specificky vyhláška č. 529/2006 Sb.[22] definuje požadavky bezpečnosti na orgán veřejné správy. Ukládá povinnost v informační koncepci uvést dlouhodobé cíle, kterých chce dosáhnout

[21] zákon č. 227/2000 Sb., o elektronickém podpisu ze dne 29. června 2000

[22] vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy ze dne 6. prosince 2006

v oblasti řízení bezpečnosti informačních systémů veřejné správy. Pod tyto cíle vždy spadá bezpečnost zpracovávaných dat, technických a programových prostředků a služeb, které poskytují.

Dané orgány jsou povinny stanovit plán řízení bezpečnosti, který bude obsahovat popis činností vykonávaných za cílem dosažení požadavků na bezpečnost informačního systému a časový harmonogram jejich plnění.

Z dané vyhlášky také vychází požadavky na strukturu provozní dokumentace, jejíž součástí je bezpečnostní dokumentace informačního systému. Jejími složkami jsou bezpečnostní politika a směrnice. První obsahuje popis opatření, které orgán uplatňuje při zajištění bezpečnosti systému, druhá podrobný popis bezpečnostních funkcí, které správce používá pro provádění určených činností v informačním systému, a návod jejich použití.

Zákon č. 365/2000 Sb.[23] stanovuje nutnost provedení atestace dlouhodobého řízení informačních systémů veřejné správy a nutnost prokázat splnění povinností, které byly zmíněny výše. Právo tedy definuje obecné bezpečnostní požadavky, ovšem nijak konkrétně nezmiňuje, jak by měla bezpečnost informačních systémů veřejné správy (ISVS) být implementována. Nestanovuje ani, na jaké úrovni by měla bezpečnost být, jaké funkce by měly být užity a jaké nástroje uplatněny [31].

V praxi je tedy možné realizovat plán řízení bezpečnosti různými způsoby. Atestaci pak provádí atestační středisko pověřené Ministerstvem vnitra České republiky, ovšem ani tím nejsou stanovena kritéria pro bezpečnost ISVS.

Zákon č. 101/2000 Sb.[24] definuje v tomto ohledu přesnější požadavky na bezpečnost. Ukládá správci a zpracovateli povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě. Dle zákona je na správci či zpracovateli, aby posoudil rizika zneužití. V oblasti automatizovaného zpracování osobních údajů má za úkol zajistit, aby informační systém použily pouze oprávněné osoby, uchovávat záznamy o tom, kdo a kdy dané údaje zaznamenal či jinak zpracoval, a zabránit neoprávněnému přístupu k datovým nosičům.

Byť tedy tato právní norma blíže určuje, co je v informačních systémech, které uchovávají osobní údaje, zapotřebí v rámci bezpečnosti, opět není přímo specifikováno, jaké technologie nebo nástroje mají být používány. Nicméně stanovisko soudu v tomto případě je řídit se technickými normami, které jsou při užívání daných technologií považované za standard (například české technické normy ISO/IEC TR 13335) [31].

---

[23] zákon č. 365/2000 Sb., o informačních systémech veřejné správy ze dne 23. října 2000

[24] zákon č. 101/2000 Sb., o ochraně osobních údajů ze dne 4. dubna 2000

## 3.3 Datové schránky

Datové schránky a jejich informační systém v sobě zahrnuje velký počet aspektů, které jsou podchyceny v patřičných zákonech a úpravách. Jedná se o zákon č. 300/2008 Sb.[25] a řadu vyhlášek, zejména pak vyhlášku č. 194/2009 Sb.[26] Datové schránky jako takové na rozdíl od emailu představují důvěryhodné úložiště datových zpráv umožňující zabezpečené doručování.

Jak již bylo dříve řečeno, datové zprávy sestávají z hlavičky a těla, které tvoří příloha (či více příloh). Za účelem zamezení šíření škodlivých dat s pomocí těchto zpráv stanovuje dříve zmíněná vyhláška použitelné formáty příloh. Mezi ně se řadí PDF, DOC, ODT a další. Soubory ve formátu EXE či archivy jako ZIP nelze prostřednictvím datových správ zasílat.

Samotné omezení ovšem nutně nezaručuje, že se škodlivá data nebudou prostřednictvím datových zpráv šířit. Možností, jak zapouzdřit virus do souborů podporovaných formátů je mnoho, například pomocí maker v dokumentech Microsoft Word [32].

Zákon č. 300/2008 Sb. nicméně uvádí, že se fyzická osoba dopouští přestupku tím, když použije datovou schránku k šíření nevyžádaných sdělení nebo počítačového programu, který může poškodit ISDS a jeho údaje, či výpočetní techniku držitele datové schránky. Přestupek je možno sankcionovat pokutou až 20000 Kč. V případě, že by se stejného přečinu dopustila podnikající fyzická či právnická osoba, jednalo by se o správní delikt, který je v tomto případě postižitelný pokutou až 20 milionů Kč.

Další neodmyslitelnou součástí datových zpráv je elektronický podpis a certifikáty s ním spjaté. Z tohoto důvodu stanovuje provozní řád ISDS umožnění doručovat certifikáty X.509 (formáty CER, CRT, DER, PK7) a certifikáty a elektronické podpisy dle PKCS#7 (formáty P7B, P7C, P7F, P7M, P7S) [31].

Jinou stránkou užívání datových schránek je bezpečnost přistupování k nim. Způsoby přístupu, které již byly dříve zmíněny, jsou ustanoveny ve vyhlášce č. 194/2009 Sb. Taktéž je v ní uvedena délka uživatelského jména (6 až 12 znaků), délka bezpečnostního hesla (8 až 32 znaků) a vymezeny přípustné znaky.

Aby byla zaručena bezpečnost už při zřizování datové schránky a předávání přístupových údajů, je ze zákona o elektronických úkonech dáno, že Ministerstvo vnitra zašle tyto údaje neprodleně do vlastních rukou osoby oprávněné k přístupu do datové schránky. Dále je specifikováno, že tato osoba musí zacházet s údaji tak, aby nedošlo k jejich zneužití.

---

[25] zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi ze dne 17. července 2008

[26] vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek ze dne 23. června 2009

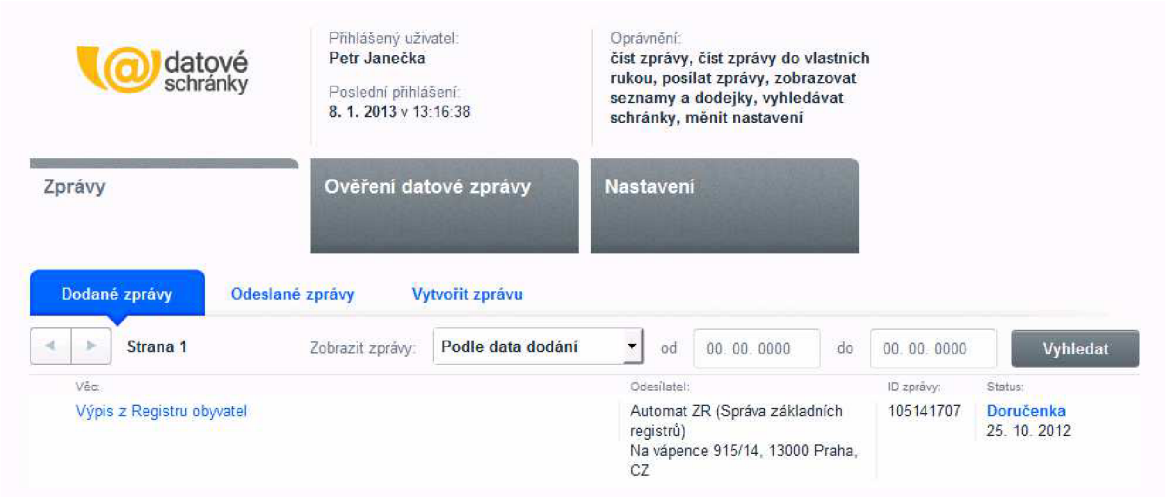
V případě, že by došlo k odcizení přístupových údajů, by měl jejich vlastník oznámit neprodleně ministerstvu tuto skutečnost. Dle zákona má ministerstvo povinnost údaje zneplatnit a zároveň zaslat vlastníkovi nové.

Tento zákon platí i pro pověřené osoby, kterým může vlastník zřídit uživatelský účet ve své datové schránce. Pokud by osoba ztratila pověření a došlo by k oznámení této skutečnosti, má ministerstvo povinnost přístupové údaje okamžitě zneplatit a informovat o tomto kroku jak pověřenou osobu, tak tu, která o zneplatnění zažádala.

Podobně právo reaguje i na další situace týkající se zajištění bezpečnosti datových schránek. Pokud by například došlo k úmrtí osoby vlastnící datovou schránku, či by nastoupila výkon trestu, ministerstvo je povinno tuto datovou schránku neprodleně znepřístupnit.

# 4 Návrh aplikace

Aplikace vytvořená v rámci bakalářské práce vychází z funkcionality původního webového rozhraní datových schránek. Jejím cílem je pokrýt většinu poskytovaných funkcí a k tomu přidat i rozšíření, která nejsou součástí původního rozhraní, jako například uchovávání zpráv v datové schránce déle než 90 dní či práce s více datovými schránkami.




**Obrázek 2:** webové rozhraní datových schránek

## 4.1 Uživatelské rozhraní

Jelikož se jedná o desktopovou aplikaci, je její rozhraní od původního webového patrně odlišné, nicméně i tak je jejím cílem jednoduchost a přehlednost. Protože je svým zaměřením orientována spíše mezi kancelářské aplikace, odpovídá tomu i rozložení hlavního okna, které je navrženo ve stylu MS Outlook. Toto rozložení je mezi uživateli známé a považováno za intuitivní.


**Obrázek 3:** schéma rozhraní aplikace

Dle schématu na obrázku 3 je rozhraní rozděleno na čtyři základní bloky. Horní blok obsahuje ovládací prvky, které se týkají všech aspektů aplikace. Umožňuje vytvářet nové zprávy, spravovat účty, prohlížet kontakty atd.

Nejlevější panel obsahuje složky, do kterých jsou jednotlivé datové zprávy roztříděny. Obdobně jako u klasického emailu, i zde se zprávy dělí standardně na přijaté a odeslané, navíc je možné třídit i dle uživatelem definovaných složek. Tento panel také obsahuje možnost filtrování, například podle data.

Seznam zpráv potom obsahuje všechny zprávy, které odpovídají aktuálnímu filtru. Položky jsou seřazeny pod sebou a zobrazují základní informace o zprávách, konkrétně předmět, jméno odesílatele či příjemce a čas. Pravým tlačítkem myši je možné zobrazit kontextové menu k dané datové zprávě, které obsahuje běžné úkony jako odstranění zprávy nebo odpovědět.

Poslední, nejpravější blok je určen pro zobrazení zprávy zvýrazněné v seznamu zpráv. Tento blok obsahuje detaily o aktuální zprávě. Podobně jako v emailových klientech lze s touto zprávou pracovat pomocí příslušných tlačítek v horní liště (např. odpovědět či přeposlat).

Vytváření nové zprávy obstarává samostatné okno, které sestává z lišty obsahující patřičné ovládací prvky (odeslat, přidat příjemce, přidat přílohu apod.) a těla, jehož obsahem je samotná zpráva.

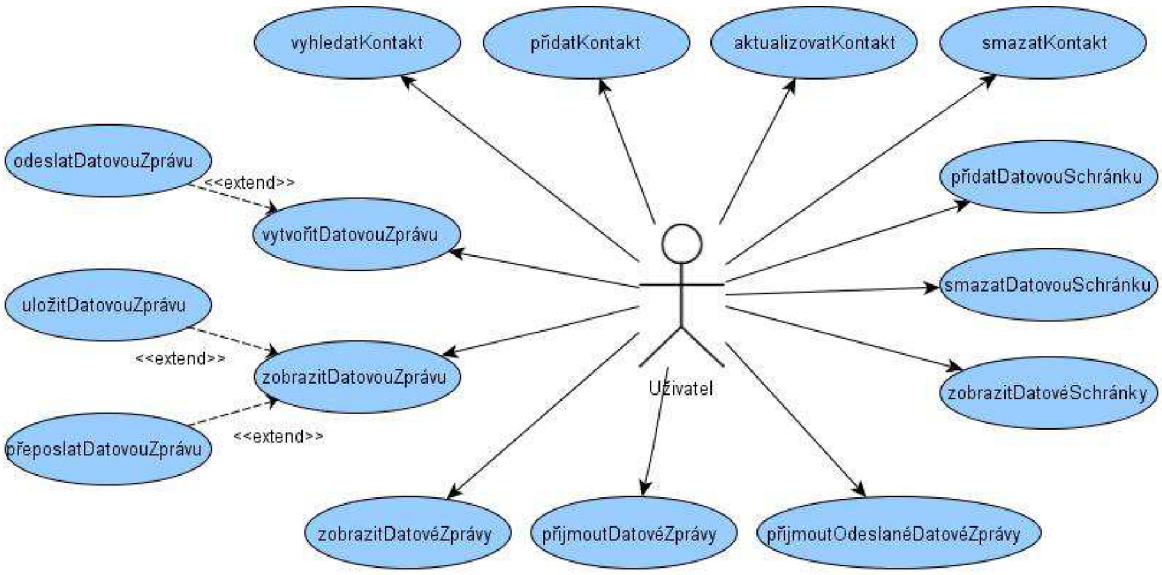
Pro správu kontaktů je taktéž vyčleněno vlastní okno, kde lze kontakty vyhledávat a přidávat. Při psaní zprávy je pak možné z tohoto seznamu jednoduše přidávat adresáty.

## 4.2 Funkcionalita aplikace

Funkcionalita aplikace se zakládá na funkcích poskytovaných API datových schránek a dá se shrnout do čtyř základních bloků:

- komunikace s ISDS,
- správa datových schránek,
- manipulace s datovými zprávami,
- vyhledávání datových schránek a správa kontaktů.

Z pohledu uživatele program poskytuje širokou škálu funkcí, přičemž základní z nich zachycuje následující diagram užití na obrázku 4.




**Obrázek 4:** diagram užití základních funkcí aplikace

### 4.2.1 Komunikace s ISDS

Tato část funkcionality je až na výjimky uživateli skryta. Jejím cílem je navázat spojení s informačním systémem datových schránek a komunikovat s ním. V podstatě se jedná o podpůrné funkce, které dle akcí uživatele zasílají požadavky ISDS, přijímají odpovědi a postupují je k dalšímu zpracování.

V případě synchronizace zpráv tedy aplikace prostřednictvím webových služeb zažádá ISDS o seznam nových zpráv a dle odpovědi se pak rozhoduje, které zprávy ještě nejsou v databázi a je třeba je stáhnout.

Jednou ze zmíněných výjimek je například situace, kdy dojde k problému v komunikaci, například uživatel není připojen k internetu, a tudíž nelze navázat spojení. V takové situaci program informuje o nastalé situaci chybovým hlášením.

### 4.2.2 Správa datových schránek

Tento blok zahrnuje veškerou činnost ohledně správy datových schránek. Jedná se zejména o přidávání datových schránek, jejich mazání, zobrazení údajů o schránce a o uživateli nebo změnu údajů.

Zmíněná možnost přidání datové schránky je dostupná kdykoliv a zachycuje ji následující případ užití.

| přidatDatovouSchránku |
|---|
| **ID: UC1** |
| **Uživatelé:** Uživatel |
| **Tok událostí:**<br>1. Uživatel zvolí možnost přidat datovou schránku.<br>2. Program zobrazí okno pro přidání nové datové schránky.<br>3. Uživatel specifikuje identifikační a přístupové údaje datové schránky.<br>4. Uživatel potvrdí volbu.<br>5a. Program se pokusí ověřit platnost vstupních údajů, pokud je v pořádku, přidá datovou schránku do databáze.<br>5b. Když vstupní údaje nejsou platné, uživatel je požádán o úpravu údajů (krok 3). |
| **Následné podmínky:**<br>V databázi datových schránek programu přibyla nová datová schránka a program je připraven s ní pracovat. |
| **Alternativní tok událostí:**<br>1. – 3. Uživatel může kdykoliv opustit dialog. |

Na podobném principu pak fungují i ostatní uživatelské úkony, ať už se jedná o smazání datové schránky či změnu údajů. Každý požadavek lze vyvolat pomocí příslušné položky v menu nebo ovládacího prvku.

### 4.2.3 Manipulace s datovými zprávami

Stejně jako lze spravovat datové schránky, je také možné manipulovat s jednotlivými datovými zprávami. Ty lze sestavovat, ukládat pro pozdější zpracování, odesílat, přijímat atd. Aplikace průběžně dotazuje informační systém datových schránek za účelem synchronizace zpráv.

Mimo základní funkcionalitu program umožňuje třídit jednotlivé zprávy dle uživatelem definovaných složek či zobrazovat pouze zprávy vyhovující specifikovanému filtru. Samozřejmostí je neomezená doba, po kterou zprávy zůstávají uloženy v databázi.

V rámci vytváření datové zprávy lze adresáty vybírat ze seznamu kontaktů či je dle kritérií vyhledávat. V případě, že program obsahuje více účtů datových schránek, si uživatel si může zvolit, který z nich bude použit jako odesílatel. Aplikace podporuje přidávání všech ze zákona povolených formátů příloh.

### 4.2.4 Vyhledávání datových schránek a správa kontaktů

Součástí aplikace je také databáze kontaktů, kterou uživatel může využít za účelem jednodušší komunikace. Jednotlivé kontakty odpovídají daným datovým schránkám v ISDS. Možnost přidat kontakt do databáze ukazuje následující diagram užití.

| **přidatKontakt** |
|---|
| **ID: UC2** |
| **Uživatelé:** Uživatel |
| **Tok událostí:**<br>1. Uživatel zvolí možnost přidat kontakt.<br>2. Program zobrazí dialog pro přidání nového kontaktu.<br>3. Uživatel specifikuje údaje, na základě kterých chce danou datovou schránku vyhledat.<br>4a. Program zkontaktuje ISDS a získá seznam odpovídajících datových schránek dle specifikovaných údajů, který následně Uživateli prezentuje.<br>4b. KDYŽ se nepodaří zkontaktovat ISDS, program zobrazí chybové hlášení a dotáže se uživatele, zda chce provést pokus znovu.<br>5a. Uživatel zvolí danou datovou schránku a potvrdí výběr.<br>5b. Uživatel změní údaje o vyhledávání a případ užití se vrací na krok 4. |
| **Následné podmínky:**<br>V databázi kontaktů programu přibyl nový kontakt. |
| **Alternativní tok událostí:**<br>1. – 5. Uživatel může kdykoliv opustit dialog. |

Jiný způsob ukládání kontaktů představuje přidání kontaktů z přijaté datové zprávy, kdy se přeskakuje celý proces vyhledávání datové schránky. Proces vyhledávání lze využít i při vytváření datové zprávy, když adresát není v seznamu kontaktů a uživatel jej potřebuje nejprve najít.

# 5 Implementace aplikace

V této kapitole je popsána implementace aplikace. Zejména jsou zmíněny jednotlivé technologie, které program ke své funkčnosti využívá.

## 5.1 Technologie aplikace

Aplikace je stavěna na technologii .NET a byla vytvářena ve vývojovém prostředí Visual Studio 2010. Jako programovací jazyk byl zvolen C# a pro ukládání dat byla použita databáze Microsoft SQL Express.

Taktéž byly užity různé knihovny a algoritmy pro šifrování, zejména standard PKCS#7[27] a X.509. Pro zpracování XML souborů byly použity vestavěné knihovny .NET. Pro komunikaci s informačním systémem datových schránek slouží knihovny pro webové služby.

### 5.1.1 Microsoft .NET Framework

.NET Framework je platforma pro vývoj, nasazení a běh aplikací, ať už desktopových či webových. Podporuje mnoho jazyků a poskytuje širokou škálu služeb, například správu paměti. Framework v sobě obsahuje velký počet knihoven, které jsou v rámci aplikace hojně využity, zejména pro webové služby.

V rámci aplikace tedy .NET Framework zaštituje veškerou funkcionalitu.

### 5.1.2 C#

Jak již bylo zmíněno, celá aplikace byla naprogramována v jazyce C#. Jedná se o objektově orientovaný jazyk, který vychází z jazyků Java a C++. Je zaštítěn platformou .NET Framework a poskytuje znatelné množství podpůrných knihoven, zejména od verze 4.0 obsahuje podporu pro webové služby.

### 5.1.3 SQL Express

Microsoft SQL Server Express 2008 je odlehčená varianta SQL Server. Je to volně dostupná verze určená pro menší a střední aplikace. Díky své kompaktnosti umožňuje lehčí přenositelnost a exportování databáze.

V rámci aplikace zajišťuje databázovou vrstvu, uchovává všechna data od zpráv až po kontakty.

---

[27] Standard pro podepisování a šifrování zpráv pomocí asymetrické kryptografie PKI

### 5.1.4 XML a LINQ

Knihovny pro práci s XML aplikace využívá kvůli XML formátu datových zpráv. Pro tyto účely používá program kromě vestavěných knihoven pro zpracovávání XML také LINQ[28]. Integrovaný jazyk LINQ ovšem umožňuje i další funkcionalitu, například dotazování nad daty v polích, kolekcích a relačních databázích. Zaměřuje se zejména na zpracovávání hromadných dat. Aplikace si nicméně vystačí pouze s užitím jeho XML aspektů.

### 5.1.5 Kryptografie

V rámci aplikace bylo využito množství kryptografických technologií, přičemž mnohé z nich zajišťují webové služby informačního systému datových schránek. Ty, které však řeší přímo aplikace, jsou certifikáty X.509 (knihovna `X509Certificates`) a algoritmus RSA (knihovna `Pkcs`), obojí popsané v kapitole 2. První zmíněné se používá jako možnost přihlašování, druhé pak k ověřování datových zpráv a šifrování citlivých údajů.

### 5.1.6 API datových schránek

API datových schránek představuje komunikační bod mezi aplikací a informačním systémem datových schránek. Sestává z webových služeb, které do větší míry kopírují původní webové rozhraní. Tyto webové služby aplikace používá k veškeré práci s ISDS (například příjem a odesílání zpráv či vyhledávání datových schránek).

### 5.1.7 Web Services Description Language Tool

Web Services Description Language Tool je program, který dokáže generovat z webových služeb popsaných v daných XML souborech a XSD[29] schématech funkce použitelné v rámci .NET Framework. Umožňuje tak webové služby poskytované API informačního systému datových schránek jednoduše integrovat do aplikace.

## 5.2 Třídy aplikace

Aplikace je tvořena mnoha třídami, které by se daly vzhledem k jejich odlišnosti rozdělit do několika skupin – formuláře a jejich funkčnost, datová schránka a webové služby.

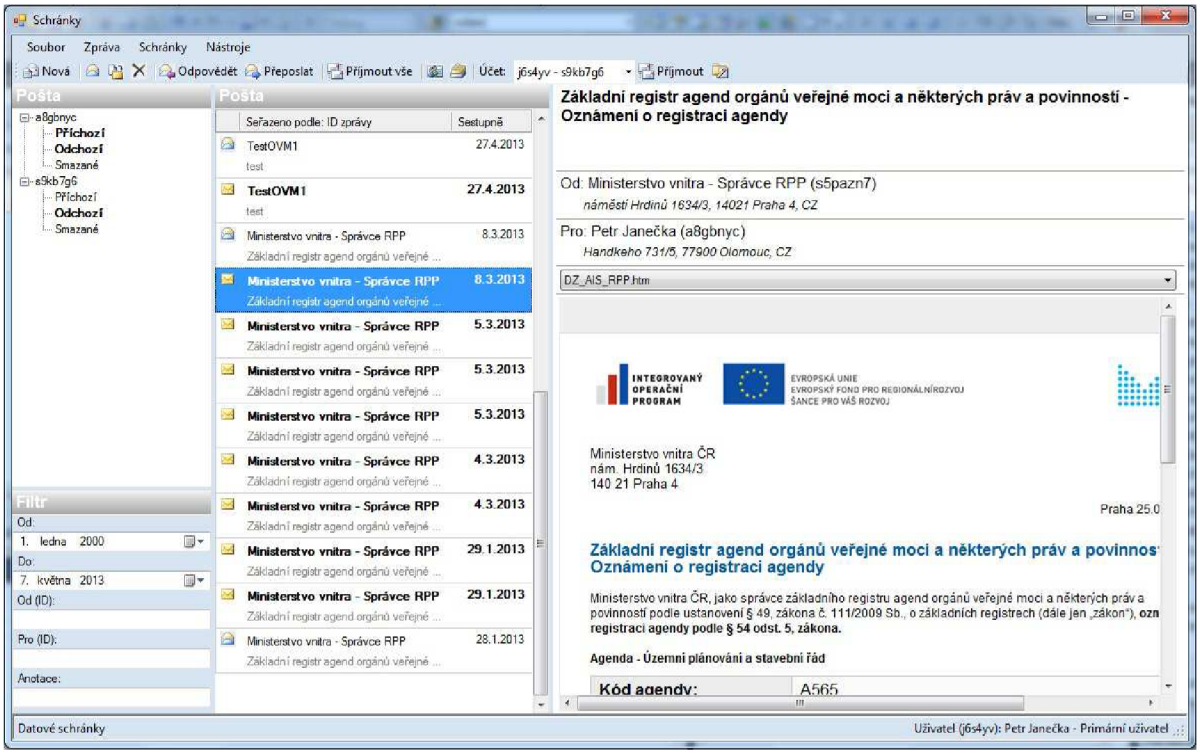
První skupina obsahuje třídy, které působí zejména jako uživatelské rozhraní a jeho funkcionalita. Zahrnuje všechny formuláře a podtřídy, které se k nim vážou. Následující seznam obsahuje základní z nich.

---

[28] Language Integrated Query – integrovaný jazyk pro dotazování

[29] XML Schema Definition, schémata definující strukturu XML dokumentu

- `AddAccount`, formulář pro přidávání a úpravu účtů.
- `Contacts`, formulář na správu kontaktů.
- `FindContact`, formulář vyhledávání kontaktů.
- `ManageAccounts`, formulář pro správu účtů.
- `MainWindow`, formulář hlavního okna (viz obrázek 5).
- `MessageForm`, formulář pro sestavování datových zpráv.
- `ViewMessage`, formulář pro detailní zobrazení datové zprávy.




**Obrázek 5:** hlavní obrazovka

Druhou skupinu tvoří samostatná třída datové schránky `Databox`. Z této třídy se vytvářejí instance účtů datových schránek používaných v aplikaci. Jednotlivé objekty pak komunikují s ISDS pomocí webových služeb.

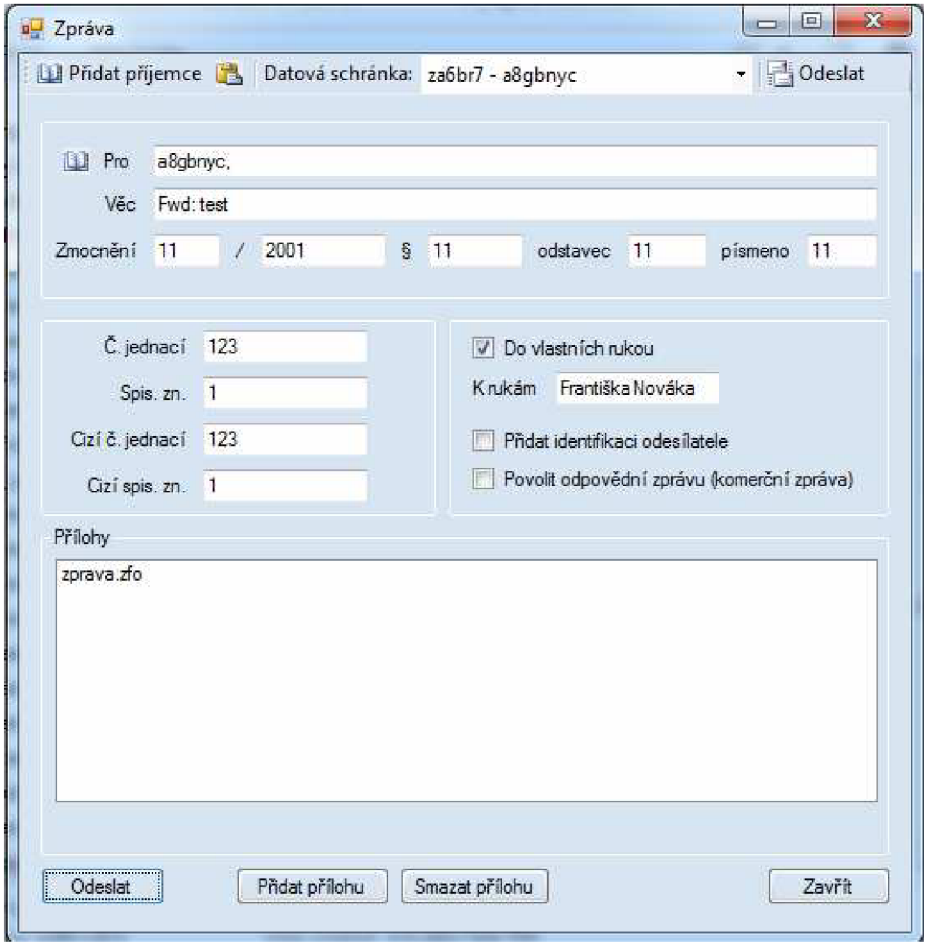
Poslední skupinou jsou třídy webových služeb implementované ze XML souborů a XSD schémat API datových schránek. Jejich seznam je následující.

- `DataboxAccess`, třída pro přístup k datovým schránkám.
- `DataboxManipulation`, třída pro manipulaci s datovou schránkou.
- `DataboxSearch`, třída určená pro vyhledávání datových schránek.
- `DmInfoWebService`, třída určená pro práci se seznamy datových zpráv.
- `DmOperationsWebService`, třída pro stahování a odesílání datových zpráv.

## 5.3 Testování

Vývoj a následné testování funkčnosti aplikace probíhalo na operačních systémech Windows 7 a Windows XP s pomocí dvou testovacích datových schránek, jedné typu *fyzická osoba* a druhé typu *orgán veřejné moci*. Schránky poskytly možnost komunikovat s informačním systémem datových schránek a ověřit si požadovanou funkčnost aplikace.

Díky kombinaci dvou schránek bylo možné ověřit zejména i funkcionalitu odesílání zpráv (zda zpráva skutečně dojde v očekávané podobě), což by s jednou schránkou nebylo možné, neboť ISDS neumožňuje zasílat zprávu sám sobě.




**Obrázek 6:** formulář zprávy – odeslání na identickou datovou schránku (s ID `a8gbnyc`) by vyvolalo chybu

Vzhledem k rozmanitosti funkcí webových služeb byl program podroben různým testům. Například bylo zjišťována funkčnost různých nestandardních zpráv, zejména pak hromadných zpráv. V případě odesílání hromadné zprávy tak bylo zjištěno, že webová služba nepodporuje odesílání hromadných zpráv uživatelům, kteří nejsou orgány veřejné moci. Program tak sám zajišťuje rozesílání více adresátům a využívá při tom základní webovou službu pro odesílání zpráv jednotlivě.

Dále byl brán v potaz obsáhlý seznam příloh a jejich správné ověřování, což je zajištěno pomocí zadaného MIME[30] typu příloh. Nikdy nebylo docíleno stavu, že by byla přijata nepodporovaná příloha od serveru ISDS kvůli antivirové kontrole, kterou ISDS provádí. Stejně tak program nepřijímá neplatné přílohy, aby nedošlo k případným problémům ze strany ISDS.

Celkově byla zkoušena komunikace programu a ISDS, díky čemuž bylo možné odladit různé problematické stavy v případě chyby, výpadku spojení či například nevyhovujícímu zadání vyhledávání datových schránek.

Jednotliví uživatelé datových schránek mají definována práva, například mohou či nemohou posílat datové zprávy. Jedním cílem testování tak bylo ověřit, zda práva program kontroluje a v případě, že uživatel nemá určitou akci povolenou, přístup zamítne.

Aspektem aplikace je taktéž dvojí způsob přihlašování – heslem nebo certifikátem. V případě hesla nebylo třeba klást takový důraz jako u certifikátů, u nichž bylo nutné mimo jiné zajistit výběr z patřičného certifikačního úložiště a také způsob, jakým si bude program pamatovat správný certifikát. Vzhledem k bezpečnosti nepřipadalo v úvahu, aby byl ukládán do databáze.

V souvislosti s bezpečností bylo ověřeno, zda dané zprávy nejsou podvržené, což umožňuje k tomu uzpůsobená webová služba. Program tak poskytuje možnost ujistit se, že je zpráva validní a nedošlo ke změně zvenčí.

Dalším aspektem bezpečnosti je samotný příjem zpráv. Jelikož užívaná webová služba k příjmu zpráv vrací zašifrovaná data opatřená podpisem, je nutné je nejprve dešifrovat. Bylo tedy nutné ověřit, zda je podpis platný a daná data dešifrovat.

Neméně důležitou součástí k testování byla kromě webových služeb i zmíněná databáze programu, která si klade za cíl zvládat užívat zároveň více datových schránek. Stěžejní část testování v tomto případě sestávala z ověření, že se datové schránky nebudou plést navzájem a bude jednoznačně rozlišeno, jaké zprávy patří dané datové schránce.

V rámci této funkčnosti bylo potřeba brát v potaz i uživatelské rozhraní, které umožňuje zprávy přetahovat z jednotlivých složek do jiných. Aby se předešlo nesrovnalostem, aplikace neumožňuje zprávu přesunout ze složek jedné datové schránky do druhé.

U uživatelského rozhraní bylo taktéž nutno ověřit, zda splňuje očekávanou funkcionalitu. Zvláště v případě přidávání, ukládání souborů, či uložení zprávy ve správném formulářovém formátu ZFO[31], který se používá v jiných aplikacích pro další zpracování.

---

[30] Multipurpose Internet Mail Extensions, někdy také Internet Media Type, identifikátor určený k formátu souboru na internetu

[31] XML formát formuláře pro aplikaci 602XML Filler zmíněný v 2. kapitole

# 6 Závěr

Cílem bakalářské práce bylo vytvořit software pro obsluhu datových schránek, který by implementoval vybrané funkce původního rozhraní datových schránek. Toho bylo v rámci programu dosaženo a vytvořená aplikace dokáže nahradit webové rozhraní.

Program taktéž disponuje dalšími možnostmi, které původní rozhraní neposkytuje, například schopnost ukládat zprávy po déle než 90 dní. Taktéž je možné pracovat s více datovými schránkami zároveň, či třeba třídit zprávy do složek, řadit je dle specifických vlastností, filtrovat je a další.

I přes různá rozšíření se však naskýtá mnoho způsobů, jak aplikaci vylepšit, neboť problematika datových schránek je velice obsáhlá. Koneckonců, existují podnikové aplikace, které se datovým schránkám věnují a pracují na nich celé týmy.

Jako budoucí rozšíření lze uvažovat zobrazování PDF souborů v rámci aplikace, přidání více funkcí nacházejících se v klasickém poštovním klientovi jako třeba kalendář a úkoly, či možnost vyplňování formulářů ve formátu ZFO, které jsou dnes v rámci elektronické státní správy hojně používané.

# Literatura


[1] MATES, Pavel a Vladimír SMEJKAL. *E-government v českém právu.* Praha: Linde, 2006, 244 s. ISBN 80-720-1614-8.

[2] LIDINSKÝ, Vít et al. *eGovernment bezpečně.* 1. vyd. Praha: Grada, 2008, 145 s. ISBN 978-80-247-2462-1.

[3] Základní registry veřejné správy. *Ministerstvo vnitra České republiky* [online]. 2010 [cit. 2013-05-07]. Dostupné z: http://www.mvcr.cz/clanek/zakladni-registry-verejne-spravy.aspx

[4] ŠPAČEK, David. *eGovernment: cíle, trendy a přístupy k jeho hodnocení.* Praha: C.H. Beck, 2012, xix, 258 s. Beckova edice ekonomie. ISBN 978-807-4002-618.

[5] MARTINEK, Lukáš. Hradecký magistrát upozorňuje na problémy se spuštěním základních registrů. *Hradec Králové* [online]. 2012 [cit. 2013-05-07]. Dostupné z: http://www.hradeckralove.org/noviny-a-novinky/hradecky-magistrat-upozornuje-na-problemy-se-spustenim

[6] DOLEŽALOVÁ, Magdaléna. Základní registry veřejné správy jsou spuštěny, náš úřad je ale zatím nemůže používat. *Jičín* [online]. 2012 [cit. 2013-05-07]. Dostupné z: http://www.mujicin.cz/zakladni-registry-verejne-spravy-jsou-spusteny-nas-urad-je-ale-zatim-nemuze-pouzivat/d-1278391

[7] LEDVINKA, Robert. Vyjádření Ministerstva vnitra k mediálním komentářům k tématu uvedení základních registrů do ostrého provozu. *Ministerstvo vnitra České republiky* [online]. 2012 [cit. 2013-05-07]. Dostupné z: http://www.mvcr.cz/clanek/zpravodajstvi-vyjadreni-ministerstva-vnitra-k-medialnim-komentarum-k-tematu-uvedeni-zakladnich-registru-do-ostreho-provozu.aspx

[8] PETERKA, Jiří. Základní registry pod lupou: vaši banku či operátora na změny (zatím) neupozorní. *Lupa.cz* [online]. 2012 [cit. 2013-05-07]. Dostupné z: http://www.lupa.cz/clanky/zakladni-registry-pod-lupou-vasi-banku-ci-operatora-na-zmeny-zatim-neupozorni/

[9] PETERKA, Jiří. Základní registry pod lupou: Hlášení změn vašich údajů třetím osobám? Zmatek a chaos. *Lupa.cz* [online]. 2012 [cit. 2013-05-07]. Dostupné z: http://www.lupa.cz/clanky/zakladni-registry-pod-lupou-hlaseni-zmen-vasich-udaju-tretim-osobam-zmatek-a-chaos/

[10] Nový registr vozidel plně v provozu od 9. července 2012. *Ministerstvo dopravy* [online]. 2012 [cit. 2013-05-07]. Dostupné z: http://www.mdcr.cz/cs/Media/Tiskove_zpravy/Novy_centralni_registr_vozidel_plne_v_provozu_od_9_cervence_2012.htm

[11] PETERKA, Jiří. *Báječný svět elektronického podpisu.* Praha: CZ.NIC, c2011, 430 s. CZ.NIC. ISBN 978-80-904248-3-8.

[12] PAVLÍK, Roman. Běžné chování uživatelů datových schránek znamená bezpečnostní problém. *Magazin Egoverment* [online]. 2009 [cit. 2013-05-07]. Dostupné z: http://www.egovernment.cz/archiv/PDF%204-09/6.pdf

[13] DELFS, Hans a Helmut KNEBL. *Introduction to cryptography: principles and applications.* 2nd ed. New York: Springer, 2007, xvi, 367 p. ISBN 35-404-9243-7.

[14] Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu. *Ministerstvo vnitra České republiky* [online]. 2010 [cit. 2013-05-07]. Dostupné z: http://www.mvcr.cz/clanek/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmum-v-oblasti-elektronickeho-podpisu.aspx

[15] KAHATE, Atul. *Cryptography and network security.* 2nd ed. New Delhi: Tata McGraw-Hill, 2008. ISBN 978-007-0648-234.

[16] Elektronický podpis, správa veřejných klíčů. KUNDEROVÁ, Ludmila. *Bezpečnost IS/IT* [online]. 2010 [cit. 2013-05-07]. Dostupné z: https://akela.mendelu.cz/~lidak/bis/9pki.htm

[17] Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu. *Ministerstvo vnitra České republiky* [online]. 2008, 2009 [cit. 2013-05-07]. Dostupné z: http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvareni-elektronickeho-podpisu.aspx

[18] LUBBE, J. *Basic methods of cryptography.* New York: Cambridge University Press, 1998, xiv, 229 p. ISBN 05-215-5559-0.

[19] SCHNEIER, Bruce. *Applied cryptography: protocols, algorithms, and source code in C.* 2nd ed. New York: Wiley, c1996, xxiii, 758 p. ISBN 04-711-1709-9.

[20] CIAMPA, Mark D. *Security guide to network security fundamentals.* 4th ed. Boston, MA: Course Technology, Cengage Learning, c2012, xxvi, 628 p. ISBN 11-116-4012-2.

[21] OPPLIGER, *Rolf. SSL and TLS: theory and practice.* Boston: Artech House, c2009, xxi, 257 p. Artech House information security and privacy series. ISBN 15-969-3447-6.

[22] GOLDBERG, Kevin Howard a Elizabeth CASTRO. *XML.* 2nd ed. Berkeley, CA: Peachpit Press, c2009, xviii, 269 p. Visual quickstart guide. ISBN 03-215-5967-3.

[23] WEERAWARANA, Sanjiva et al. *Web services platform architecture: SOAP, WSDL, WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging, and more.* Upper Saddle River, NJ: Prentice Hall PTR, c2005, xxxix, 416 p. ISBN 01-314-8874-0.

[24] AUSTION, Daniel, Abbie BARBIR a Sharad GARG. Web Services Architecture Requirements. W3C [online]. 2002 [cit. 2013-05-07]. Dostupné z: http://www.w3.org/TR/2002/WD-wsa-reqs-20020429

[25] KUMAR, B. V. a S. V. SUBRAHMANYA. *Web Services: An Introduction.* New Delhi: Tata McGraw-Hill Education, 2004. ISBN 978-0-07-059378-7.

[26] BENSLIMANE, Djamal, Schahram DUSTDAR a Amit SHETH. Services Mashups: The New Generation of Web Applications. In: *IEEE Internet Computing* [online]. 2008 [cit. 2013-05-07]. Volume 12, Issue 5, s 13-15. DOI: 10.1109/MIC.2008.110. Dostupné z: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4620089&isnumber=4620081

[27] ALONSO, Gustavo et al. Web services: concepts, architectures, and applications. New York: Springer, 2004, xx, 354 p. ISBN 35-404-4008-9.

[28] TESAŘ, Pavel. Provozní řád ISDS. *Datové schránky* [online]. 2013 [cit. 2013-05-07]. Dostupné z: http://www.datoveschranky.info/assets/ke-stazeni/provozni_rad_isds.pdf

[29] Poštovní datová zpráva. *Česká pošta* [online]. 2011 [cit. 2013-05-07]. Dostupné z: http://www.ceskaposta.cz/cz/sluzby/datove-schranky/postovni-datova-zprava-id29096/

[30] BUDIŠ, Petr a Iva HŘEBÍKOVÁ. *Datové schránky: fungování, doručování, bezpečnost, návody.* 1. vyd. Olomouc: ANAG, 2010, 287 p. ISBN 80-726-3617-0.

[31] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty.* 2. podstatně přeprac. a rozš. vyd. Praha: Leges, 2012, 464 s. Teoretik. ISBN 978-808-7576-366.

[32] TIWANA, Amrit. *Web security.* Boston: Digital Press, c1999, xvi, 425 p. ISBN 15-555-8210-9.

# Seznam příloh

**Příloha A**: Obsah CD

# **Příloha A:** Obsah CD

- složka `src` – soubory zdrojového kódu programu
- složka `manual` – uživatelský manuál k programu
- složka `install` – instalační soubory programu
- složka `technicka_zprava` – soubory technické zprávy