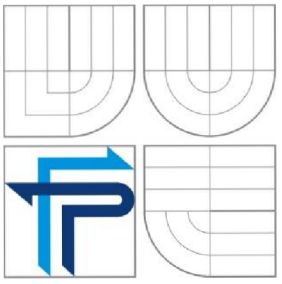
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
DEPARTMENT OF INFORMATICS

OPTIMÁLNÍ MODEL INFORMAČNÍHO SYSTÉMU DATOVÝCH SCHRÁNEK

OPTIMAL MODEL OF THE INFORMATION SYSTEM DATA BOXES

BAKALÁŘSKÁ PRÁCE
BACHELOR THESIS

AUTOR PRÁCE
AUTHOR
MARTIN BALCAR

VEDOUCÍ PRÁCE
SUPERVISOR
prof. Ing. JIŘÍ DVOŘÁK, DrSc.

BRNO 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/10
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Balcar

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Optimální model informačního systému datových schránek

v anglickém jazyce:

Optimal Model of the Information System Data Boxes

Pokyny pro vypracování:

Úvod
Systémové vymezení problému
Cíl práce
Informační zdroje
Současný stav řešené problematiky
Analýza řešeného problému
Návrh řešení problému
Zhodnocení návrhu
Závěr
Seznam použitých informačních zdrojů
Seznam zkratek a pojmů
Přílohy
Rejstřík

Seznam odborné literatury:

SMEJKAL,V. Datové schránky v právním řádu ČR. 1. vyd. Praha: ABF, 2009. 280 s. ISBN 978-80-86284-78-1.
MATES,P., SMEJKAL,V. E-GOVERNMENT v českém právu. 1.vyd. Praha : Linde, 2006. 425 s. ISBN 80-7201-614-8.
BUDIŠ,P. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Praha: ANAG, 2008. 123 s. ISBN 80-7263-465-1.
LIDINSKÝ,V. E-governemnt bezpečně. 1. vyd. Praha: GRADA Publishing, 2008. 360 s. ISBN 978-80-247-2462-1.
JONES,D. Automatizace správy a skriptování MS Windows. 1.vyd. Brno: Computer Press, 2006. 248 s. ISBN 80-251-1261-6.

Vedoucí bakalářské práce: prof. Ing. Jiří Dvořák, DrSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2009/10.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ Fakulta podnikatelská

L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. RNDr. Anna Putnová, Ph.D., MBA
Děkanka

V Brně, dne 7. 2. 2010

Abstrakt

Tato bakalářská práce se zabývá problematikou informačního systému datových schránek. Teoretická část obsahuje vymezení pojmu datových schránek, e-governmentu a nástrojů potřebných k využití datové schránky jako jsou elektronické certifikáty, elektronická konverze dokumentů, elektronická spisová služba a datové úložiště dokumentů. Problematika je zpracována z pohledu potřeb velké organizace typu Krajský úřad Jihomoravského kraje. Praktická část práce zahrnuje charakteristiku organizace a jejího informačního systému. Dále hodnotí začlenění datové schránky v organizaci pomocí provedené analýzy, ze které vyplývají jednotlivé návrhy na řešení problému.

Abstract

This Bachelor thesis deals with problems of information system in data boxes. The theoretical part consists of the concept in data boxes, egovernment and the implementation of data boxes such as electronic certificates, electronic documentation and storage capability. The problems are elaborated according to a large organization, such as a regional authority of South Moravian country. The practical part includes the describtion of the organization and its information system. Furthermore, it evaluates the integration of data boxes in the organization with help of the implementation, which results from the particular proposal to solve the problem.

Klíčová slova:

Informační systém datových schránek, datová schránka, e-government, spisová služba, elektronický certifikát, časové razítko, datové úložiště, optimalizace, model.

Key Words:

Information System Data Boxes, Data Box, Egovernment, Document Record Management System, Electronic Certificate, Time Stamp, Storage Capability, Optimalization, Model.

Bibliografická citace

BALCAR Martin, *Optimální model informačního systému datových schránek*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010, 75 s. Vedoucí bakalářské práce prof. Ing. Jiří Dvořák, DrSc.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 3. června 2010

Podpis

Poděkování

Tímto bych chtěl poděkovat vedoucímu bakalářské práce prof. Ing. Jiřímu Dvořákovi, DrSc. za věnovaný čas, rady a připomínky, které mi poskytl při zpracování této práce.

OBSAH:

1 ÚVOD

Elektronizace veřejné správy zažívá v posledních letech v ČR obrovský rozmach. Co se pod pojmem elektronizace skrývá? V podstatě jde o snahu v maximální míře využít prostředky elektronické komunikace i možnosti informačních a komunikačních technologií mezi veřejnou správou navzájem a širokou veřejností. To vše za podpory platné legislativy. Obecně lze elektronizaci chápat jako snahu o zefektivnění, zrychlení a zjednodušení komunikace mezi úřadem a občanem, a to ve všech oblastech života. Velký důraz je přitom kladen na vytvoření takového právního prostředí, ve kterém bude elektronický dokument na stejné úrovni jako dokument papírový. Tato myšlenka byla jedním ze základních kamenů pro vytvoření, schválení a spuštění projektu „Informační systém datových schránek".

Informační systém veřejné správy zažívá díky datovým schránkám revoluční období. Datové schránky jsou významným počinem elektronizace vnější i vnitřní komunikace organizací, měst, úřadů, ministerstev, a také zvyšují kvalitu a výkon ve vztahu k občanům. Jde o zásadní krok k efektivnosti a transparentnosti veřejné správy, což se promítne do vnitřního chodu všech organizací veřejné správy i těch, které s veřejnou správou komunikují.

Téma datových schránek je dnes aktuální a setkáváme se s ním téměř na každém kroku. Tato problematika je velmi obsáhlá a obtížná, proto byla pro účely této práce zaměřena pozornost zejména na začlenění informačního systému datových schránek do stávajícího prostředí informačního systému Krajského úřadu Jihomoravského kraje.

Uvedená problematika bude popisována z pozice pracovníka Krajského úřadu, podílejícího se na implementaci datových schránek a jejich provozu v této organizaci. Teoretické informace uvedené v této práci budou konfrontovány s praktickými zkušenostmi z běžného provozu.

2 SYSTÉMOVÉ VYMEZENÍ PROBLÉMU

Z hlediska strategie elektronizace veřejné správy v ČR byla vytvořena vize nového prostředku elektronické komunikace, která umožní garantovaný způsob vzájemné komunikace mezi subjekty veřejné, privátní a komerční sféry. Hlavní myšlenkou bylo vytvořit efektivní, rychlou a spolehlivou komunikaci především mezi subjekty veřejné správy a umožnit tím kvalitnější podmínky pro výkon státní moci a poskytování služeb běžným občanům. Velmi důležitým krokem této snahy bylo zrovnoprávnění elektronických dokumentů s papírovými a stanovení zákonné povinnosti využívat elektronickou komunikaci.

Snaha ČR o vytvoření tzv. elektronického úřadu a transformace co možná největšího množství agend do čistě elektronické podoby, tzn. vykonávání veřejné moci bez nutnosti osobní návštěvy úřadu, je plně v souladu se světovým trendem a koresponduje s rozvojem informačních systémů ve světě.

Nový prostředek elektronické komunikace v ČR představuje informační systém datových schránek založený na platné legislativě (více v kap. 5.2) a uvedený do ostrého provozu dne 1. července 2009.

Tato práce obsahuje vymezení problematiky datových schránek, e-governmentu a dalších nástrojů souvisejících s využitím datové schránky jako jsou elektronické certifikáty, elektronická konverze dokumentů, elektronická spisová služba a datové úložiště dokumentů. Smyslem práce je vytvořit optimální model informačního systému datových schránek, na základě kterého bude navržen vhodný způsob začlenění datové schránky do stávajícího prostředí Krajského úřadu Jihomoravského kraje. Pro stanovení potřeb, které má krajský úřad jako typický představitel OVM splňovat, lze doporučit použití SWOT analýzy. Závěry z této analýzy (kap. 6.4) a obecné zhodnocení technického řešení datových schránek (kap. 5) pomohou vymezit oblasti, kterým je vhodné se v modelu optimalizace věnovat (více v kap. 6.4).

3 CÍL PRÁCE

Cílem bakalářské práce je návrh optimálního způsobu začlenění informačního systému datových schránek do stávajícího prostředí IS Jihomoravského kraje.

Dílčí cíle bakalářské práce jsou:

- Systémové vymezení problému a úvod do problematiky elektronizace veřejné správy v ČR (viz kapitola 2)
- Shromáždění informačních zdrojů a jejich soupis (viz kapitola 4)
- Vymezení současného stavu řešené problematiky datových schránek a souvisejících technických řešení z pohledu velké organizace, definice e-governmentu (viz kapitola 5)
- Analýza dané problematiky v prostředí KrÚ JMK, způsob používání datové schránky v organizaci a vytvoření SWOT analýzy hodnotící provoz a využívání ISDS (viz kapitola 6)
- Návrh na zlepšení a odstranění problematických oblastí, tj. návrh na řešení slabých stránek a hrozeb vyplývajících z použité analýzy a obecný návrh na optimální model ISDS (viz kapitola 7)
- Konečné zhodnocení návrhu (viz kapitola 8)

4 INFORMAČNÍ ZDROJE

Mezi hlavní informační zdroje této práce patří odborná literatura z oblasti e-governmentu, datových schránek a informačních technologií. K získání odborné literatury byla využita Moravská zemská knihovna a knihovna VUT. Dalšími důležitými zdroji jsou tematicky zaměřený magazín Egovernment a internetové zdroje, zejména informační weby Ministerstva vnitra ČR.

V teoretické části práce (viz kap. 2 a 5) je čerpáno z literatury, magazínu a internetových zdrojů zaměřených na problematiku e-governmentu, datových schránek a elektronických certifikátů.

V praktické části (kap. 5 a 7) je čerpáno především z literatury a internetových zdrojů zaměřených na problematiku informačních technologií (el. podpis, zabezpečení DS, časové razítko, hromadná instalace). Podnětným zdrojem byla také brožura Typový postup implementace zákona č. 300/2008 Sb., kterou nechal zpracovat Plzeňský kraj (blíže viz kap. 5).

Vzhledem k tomu, že se jedná o složitou problematiku, byla řada otázek konzultována s ostatními kolegy na KrÚ JMK. Jednalo se o konzultace v oblasti informačních technologií - zálohování, archivace a dostupnost dat, konzultace metodické - interní oběh dokumentů s vazbou na spisovou službu a určení vhodné metodiky a konzultace v oblasti právní – v otázkách nutných náležitostí, které musí ISDS a funkčnost spisové služby dle právního výkladu splňovat.

Dalším zdrojem, který přehledným způsobem zpracovává problematiku datových schránek a souvisejících technických řešení a otázek, jsou příspěvky pana Ing. Jiřího Peterky v internetovém zpravodaji www.lupa.cz. Ing. Peterka je publicista, který se od počátku zavedení datových schránek tímto tématem zabývá a publikuje, dle mého názoru, velmi hodnotné články.

Celou problematikou e-governmentu, včetně datových schránek, se také zabývá každoroční dubnová konference ISS[1] konaná v Hradci Králové. Letošní ročník byl věnovaný především tématu základních registrů, ale jeden z dopoledních bloků pojednával o tématu datových schránek. Došlo ke zhodnocení datových schránek po prvním půl roce ostrého provozu a představení plánovaného rozvoje systému.

[1] ISS - Internet ve státní správě.

5 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

V této kapitole bude popsán současný stav řešené problematiky, tj. oblasti datových schránek (viz kap. 5.2), jejich začlenění do e-governmentu (viz kap. 5.1) a další technická řešení přímo související s provozem a funkčností datových schránek. Jedná se o řešení elektronických certifikátů resp. elektronického podepisování dokumentů a časového razítka (viz kap. 5.4), elektronické konverze dokumentů (viz kap. 5.3), oblast spisové služby (viz kap. 5.5) a otázku ukládání elektronických dokumentů (viz kat. 5.6).

Problematika bude popisována z pohledu velké organizace typu krajský úřad, která si nevystačí se základním rozhraním datové schránky přes webový portál a musí proto nutně řešit otázku napojení na vlastní informační systém, tj. otázku integrace ISDS do rozhraní vlastního IS. Tato integrace vychází z potřeby využívat pro příjem, vypravení a evidenci datových zpráv prostředků již používané elektronické spisové služby, z potřeby provádět hromadně konverzi dokumentů do formátu PDF, elektronicky dokumenty podepisovat tj. zaručit jejich autenticitu a nakonec vhodným způsobem zabezpečit uložení, dostupnost a archivaci elektronických dokumentů.

5.1 E-government a datové schránky

Datové schránky a autorizovaná konverze dokumentů tvoří klíčovou součást e-governmentu v ČR. Co to prakticky znamená? Datové schránky a celý legislativní základ na kterém stojí (viz kap. 5.2), jsou významným krokem v elektronizaci veřejné správy a ve zrovnoprávnění papírové a elektronické komunikace, tzn. že naprostou většinu úředních záležitostí bude možné vyřídit elektronicky. Je pravdou, že povinným zavedením datových schránek nastal zlom ve způsobu úřadování a komunikace s veřejnou správou, ale zdaleka se nejedná o jediný krok plánovaný v rámci rozšíření a zavádění e-governmentu v ČR.

Co znamená pojem **e-government**? Existuje celá řada definic, nicméně pro představu postačí jedna z nich, podle níž e-government 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]

V současnosti e-governemnt v ČR propaguje a prezentuje Ministerstvo vnitra ČR.

Určitě je vhodné se zmínit, co vše je součástí e-governmentu, a to buď součástí funkční nebo plánovanou. Jsou to:

- **Czech POINT** (Český Podací Ověřovací a Informační Národní Terminál)
- **KIVS** (Komunikační infrastruktura veřejné správy**)**
- **Zákon o e-governmentu**
- **Základní registry veřejné správy**

Czech POINT - představuje soustavu snadno dostupných kontaktních míst ke kterým se řadí i Krajský úřad JMK. Czech POINT vytváří garantovanou službu pro komunikaci se státem, kde je možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty

[2] LIDINSKÝ, V. (2008). *Egovernment bezpečně.* Praha: GRADA Publishing., s.7.

do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat žádost pro zahájení řízení správních orgánů. Údaje vedené v centrálních registrech[3] jsou vydávány prostřednictvím tzv. ověřených výstupů z informačního systému veřejné správy. (11)

KIVS - Komunikační infrastruktura veřejné správy představuje **sjednocení různých datových linek subjektů veřejné správy do jedné datové sítě.** Pod zkratkou KIVS se skrývá jednotná komunikační struktura, která je základem fungování eGovernmentu. Přínosem KIVS je zefektivnění služeb a výrazné úspory. (11)

Zákon o e-governmentu[4] – jehož cílem je vytvoření optimálních podmínek pro elektronickou komunikaci – a to jak občanů s úřady, tak úřadů mezi sebou. Zákon o e-governmentu stojí na třech hlavních pilířích – zrovnoprávnění elektronických dokumentů s papírovými, povinnost institucí veřejné správy komunikovat mezi sebou elektronicky a vytvoření datových schránek. A to vše při zajištění maximální ochrany osobních dat. (5)

Základní registry veřejné správy - bezpečné a aktuální databáze dat o občanech a státních i nestátních subjektech. Cílem je přeměna současného způsobu sběru a uchovávání údajů a vytvoření tzv. **centrálních registrů veřejné správy**. Registrů, které budou řešit dosavadní potíže související s nejednotností, multiplicitou a neaktuálností klíčových databází. V současné době je nasazení Základních registrů v přípravě. (5)

[3] Typicky např. v Rejstříku trestů.
[4] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

5.2 Informační systém datových schránek

Informační systém datových schránek[5] je informační systém veřejné správy, který obsahuje údaje o datových schránkách, jejich uživatelích, přístupech do schránky a dalších událostech spojených s jejich provozem. Správcem systému je MV ČR, provozovatelem je Česká pošta s.p. jako držitel poštovní licence. Údaje ze systému jsou neveřejné, správce ani provozovatel systému nemají přístup do datových schránek[6] jiných uživatelů. Každé odeslání datové zprávy[7] je potvrzeno doručenkou, která však potvrzuje doručení do DS adresáta, nikoliv její přečtení nebo vyzvednutí.

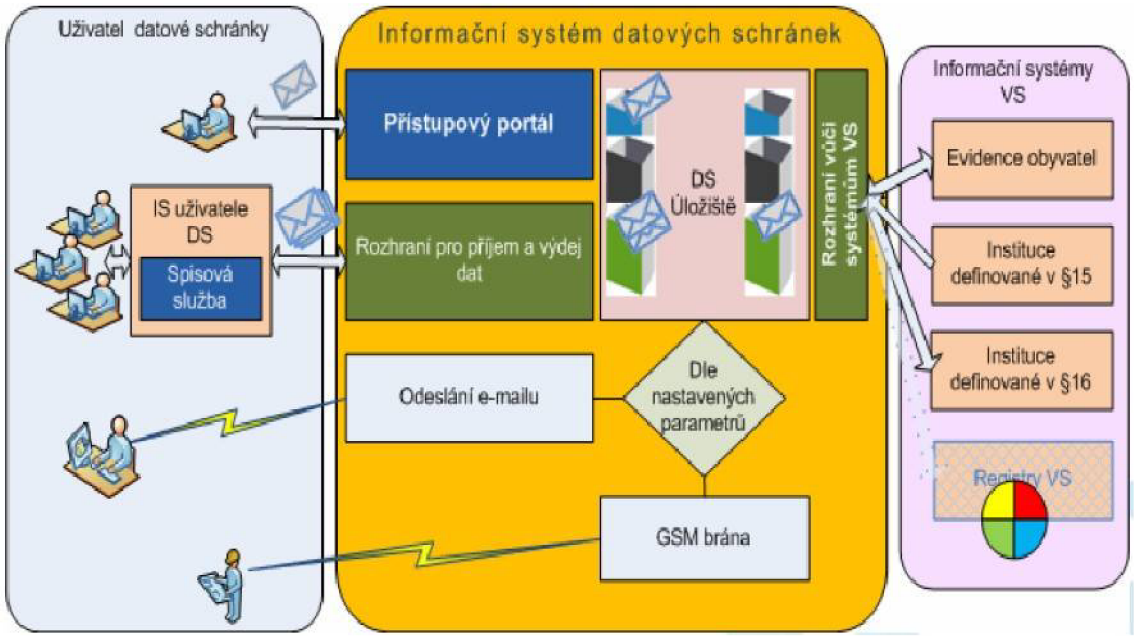
Časová posloupnost nasazení ISDS:

- Od 1. 7. 2009 je umožněno doručování dokumentů mezi:
  - orgány veřejné moci navzájem
  - orgány veřejné moci a právnickými osobami
  - orgány veřejné moci a podnikajícími fyzickými osobami
  - orgány veřejné moci a fyzickými osobami
- Systém je také určen k provádění úkonů od právnických osob, podnikajících fyzických osob nebo fyzických osob směrem k orgánům veřejné moci.
- Od 1. 1. 2010 je umožněna komunikace mezi právnickými osobami, podnikajícími fyzickými osobami a fyzickými osobami navzájem, a navíc je možno dodávat do datových schránek faktury nebo obdobné žádosti o zaplacení.
- Od 1. 7. 2010 bude možné dodávat do datových schránek dokumenty libovolného obsahu. (10)

ISDS disponuje těmito základními vlastnostmi:

- rychlost – datová zpráva je doručena prakticky okamžitě
- spolehlivost – datová zpráva se nemůže ztratit, je garantováno doručení
- průkaznost – je prokazatelné, kdo datovou zprávu podal a komu byla doručena (10)

[5] Dále jen ISDS.
[6] Dále jen DS.
[7] Dále jen DZ.



Obr. 1 – Schéma komunikace s datovou schránkou (ISDS), zdroj: (9)

Legislativní rámec

Problematiku datových schránek v první řadě vymezuje zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů ze dne 17. července 2008, který nabyl účinnosti dne 1. 7. 2009.

Problematika je dále rozpracována vyhláškami, z nichž nejdůležitější je vyhláška č. 194/2009 Sb., o stanovení podrobnosti užívání a provozování informačního systému datových schránek ze dne 23. června 2009. (6a)

S problematikou datových schránek jsou dále spjaty další zákony, z nichž lze považovat za nejdůležitější:

- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

Další právní předpisy upravující komunikaci prostřednictvím datových schránek a úkony s tím související jsou k nahlédnutí v Příloze č. 1.

Ceny za použití ISDS

Provozovateli informačního systému datových schránek náleží odměna, která je hrazena z prostředků státního rozpočtu.

Bezplatné je doručování dokumentů orgánů veřejné moci (OVM) adresovaných jinému OVM, doručování dokumentů OVM adresovaných fyzickým, podnikajícím fyzickým a právnickým osobám, kterým je vůči těmto osobám činěn veřejnoprávní úkon, jakož i činění úkonů vůči OVM fyzickými, podnikajícími fyzickými či právnickými osobami. (11)

Zpoplatněna je „privátní“ komunikace mezi fyzickými, podnikajícími fyzickými či právnickými osobami.

Cena za odeslání datové zprávy je dle aktuálního ceníku České pošty 15,04 Kč.

5.2.1 Datová schránka

Datová schránka je elektronické úložiště, které slouží ke komunikaci v oblasti veřejné správy. Pomocí datových schránek je možné zasílat dokumenty v elektronické podobě orgánům veřejné moci a tímto způsobem je i přijímat. Tento způsob komunikace nahrazuje klasický způsob doručování v listinné podobě, protože zákon zrovnoprávňuje papírovou a elektronickou verzi zasílaného dokumentu. Dokument dodaný prostřednictvím datové schránky, má stejnou váhu jako doporučená zásilka do vlastních rukou. (6a)

Rozlišujeme **čtyři druhy** datových schránek:

1. Datová schránka orgánu veřejné moci
2. Datová schránka právnické osoby
3. Datová schránka fyzické osoby podnikající
4. Datová schránka fyzické osoby

Do datové schránky jsou dodávány úřední listiny v elektronické podobě, které jsou opatřeny elektronickým podpisem odesílatele (OVM). (11)

Datová schránka není e-mailová schránka, ani se nejedná o její náhradu. Není možné s její pomocí komunikovat přímo s jednotlivými úředníky, pouze s celým úřadem či daným subjektem. Výjimku tvoří datové schránky vystavené fyzické osobě.

Datové schránky umožňují:

- odeslání datové zprávy
- příjem datové zprávy
- zjištění stavu odeslaných datových zpráv
- příjem dokladu o dodání a doručení
- ověření, zda má adresát aktivní datovou schránku
- práci s elektronickými formuláři

Pomocí datové schránky se nedoručuje pokud:

- dokument obsahuje utajované informace
- adresát nemá zpřístupněnou datovou schránku
- to neumožňuje povaha dokumentu
- se doručuje na místě (při úkonu)
- z dalších zákonných důvodů (např. doručování veřejnou vyhláškou, jiné pořadí způsobu doručování) (6a)

Zřízení datové schránky

Orgánům veřejné moci a právnickým osobám zapsaným v obchodním rejstříku byly datové schránky zřízeny automaticky ze zákona. Všem ostatním zájemcům jsou zřizovány na základě jejich žádosti (viz obr. 2) prostřednictvím Czech POINTu, podatelny MV ČR nebo www.datoveschranky.info . (6a)

Všechny subjekty obdrží přístupové údaje do systému poštovní zásilkou do vlastních rukou. Přístupové údaje tvoří pouze uživatelské jméno a heslo. Uživatelské jméno je tvořeno náhodně vygenerovaným řetězcem 6 až 12 znaků, bezpečnostní heslo je řetězcem 8 až 32 znaků, nesmí být shodné s uživatelským jménem a uživatel si je může kdykoliv změnit. Uživatelské heslo má automaticky platnost pouze 90 dnů, pak je nutné jej změnit. Po přihlášení do DS je uživatel s dostatečným předstihem na expiraci upozorňován.

Obr. 2 – Schéma zřízení datové schránky, zdroj: (9)

Přístup do datové schránky

Při přístupu k datové schránce rozlišujeme několik rolí – oprávněná osoba, administrátor a pověřená osoba.

Oprávněnou osobou může být fyzická osoba, fyzická osoba podnikající, statutární orgán, člen statutárního orgánu, vedoucí organizační složky nebo vedoucí orgánu veřejné moci.

Administrátor je osoba, určená oprávněnou osobou.

Pověřená osoba je osoba určená oprávněnou osobou nebo administrátorem.

Rozhraní datových schránek - pro přístup do datové schránky lze použít interaktivního webového portálu[8] nebo rozhraní spisových služeb. V obou případech je každé přihlášení oprávněné osoby, administrátora nebo pověřené osoby podrobeno autentizaci.

Spuštění datové schránky

Zákon o elektronických úkonech a autorizované konverzi dokumentů ve znění novely nabyl účinnosti dne 1. července 2009. Od tohoto dne jsou MV ČR zřizovány datové schránky a vydávány k nim přístupové údaje. Dnem spuštění „ostrého“ provozu byl 1. listopad 2009, kdy byly aktivovány i ty datové schránky, do nichž se doposud jejich uživatelé nepřihlásili. (5)

Zasílání dokumentů poštou a datovými schránkami

Pro OVM platí povinnost využívat pro vzájemnou komunikaci s ostatními subjekty[9] datové schránky. Umožňuje-li to povaha dokumentu, musí být zaslán prostřednictvím ISDS. Platí to i v případě, kdy OVM odpovídá na podání v papírové podobě. Zákon ukládá, že komunikace pomoci systému DS se musí upřednostnit. Samotný občan nebo právnická osoba si může zvolit, zda bude podání realizovat v papírové nebo elektronické podobě. Nemá tedy povinnost využít ISDS. (6a)

[8] http://mojedatovaschranka.cz

[9] Jež mají se zákona nebo na vlastní žádost zřízenu DS.

Kapacita datové schránky není omezena a musí být schopna přijímat neustále další zprávy i v případě, že dlouhodobě nedojde k přihlášení a nedochází tak k plynulému odstraňování starých zpráv. Její velikost je tedy pružná a neohraničená. (6a)

V souvislosti s datovou schránkou je třeba zdůraznit pojem „úložiště“. **Datová zpráva je v datové schránce uložena po dobu 90 dnů** ode dne přihlášení nebo dodání zprávy do datové schránky. Po uplynutí 90 dnů je datová zpráva z ISDS automaticky smazána.

Používání datových schránek přináší oproti analogovým dokumentům tyto výhody:

- plné nahrazení obálkového doručování
- snížení ceny za doručování
- bezpečný komunikační kanál
- podporu elektronických formulářů
- přístup z kteréhokoliv místa planety (přes internet)
- úsporu času
- všechny právnické a fyzické osoby komunikují s OVM zdarma
- usnadnění práce zasíláním dokumentů prostřednictvím DS

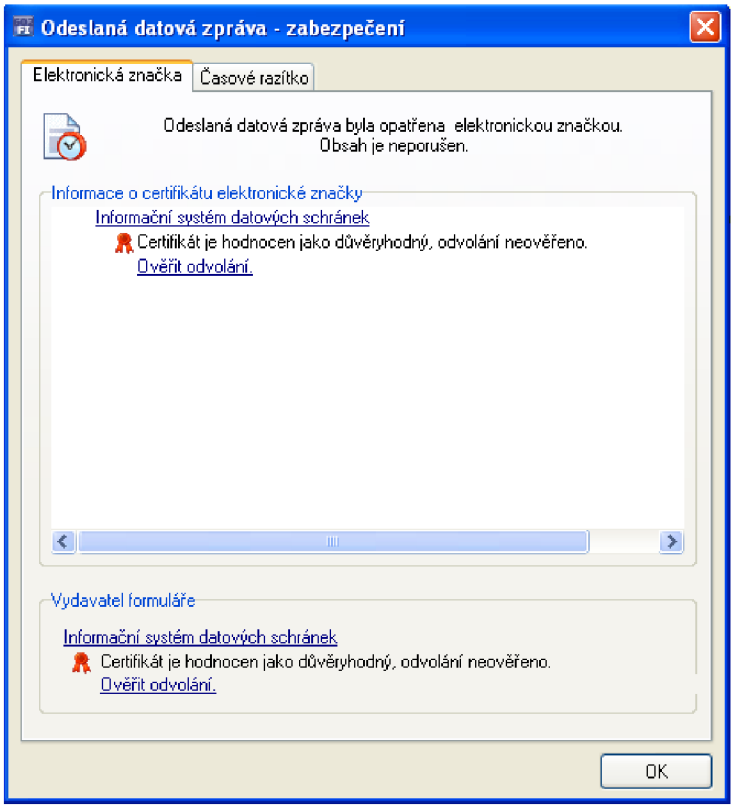
5.2.2 Datová zpráva

Všechny dokumenty zasílané prostřednictvím datové schránky mají formu **datové zprávy**.

Formát datové zprávy - datovou zprávu tvoří obálka a samotný obsah zprávy. Obálka je soubor formátu XML[10], konkrétně označený příponou ZFO[11]. Datová zpráva dále obsahuje elektronickou značku a kvalifikované časové razítko ISDS (viz obr. 3).

[10] XML - Extensible Markup Language (obecný značkovací jazyk)
[11] ZFO - formát elektronického formuláře

Obsahem zprávy může být jedna či více příloh v datových formátech povolených v prováděcím předpisu.[12] Provozovatel má kromě toho právo nepřijmout k odeslání datovou zprávu obsahující škodlivý kód. (10)



Obr. 3 – Datová zpráva – informační okno zobrazující elektronickou značku a časové razítko, zdroj: KrÚ JMK

Maximální velikost datové zprávy je pevně stanovena na 10 MB.

Termín dodání datové zprávy - v systému ISDS je vidět, kdy byla zpráva dodána do datové schránky adresáta. (6a)

Termín doručení datové zprávy - „V ISDS se jedná o datum a čas, od kdy je zpráva považována za doručenou. U OVM je tento termín shodný s termínem dodání. U ostatních subjektů se jedná buď o termín kdy se adresát přihlásil do své datové

[12] Výčet přípustných formátů datových zpráv dodávaných do datové schránky je v Příloze č. 2.

schránky (a mohl si dodané zprávy prohlédnout), nebo termín kdy uplynula lhůta 10 dní od dodání těchto zpráv. V takovém případě se hovoří o doručení fikcí.“ (6a)

„**Fikce doručení“** znamená, že nepřihlásí-li se do datové schránky osoba ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty a začínají platit lhůty plynoucí z obsahu vloženého do dokumentu. V praxi to znamená, že zde máme **systém zaručeného dodání** elektronických dokumentů, kde se předpokládá, že adresát obsah vzal na vědomí. (6a)

5.2.3 Autorizovaná konverze dokumentů

„Je to autorizovaný převod dokumentu z elektronické podoby do papírové nebo naopak. Je tedy možné převést papírový dokument na elektronický, přičemž bude stále považován za stejně hodnotný jako originál (totéž platí i opačně, tzn. je možná konverze z elektronického originálu do papírové podoby).“ (6a)

Novelizovaný zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů dále umožňuje konvertovat již konvertovaný dokument. Je tedy možné dokument opakovaně konvertovat a neomezeně převádět z elektronické podoby do papírové a zpět, aniž by ztratil svoji právní hodnotu.
Novela dále vypouští povinnost konvertovat pouze dokumenty s časovým razítkem. Je tedy možné autorizovaně konvertovat i dokumenty obsažené v datových zprávách, které časové razítko nemají. (6a)

Rozlišujeme autorizovanou konverzi tzv. „**na žádost**“, kdy o konverzi žádá občan či jiný subjekt a konverze je placená (30 Kč/stránku) a konverzi tzv. „**z moci úřední**“, jež je prováděná pro interní potřeby úřadu a je bezplatná.
V rámci CzechPOINTu jsou oba typy konverzí rozlišené a řídí se mírně odlišnými podmínkami.

5.3 Systém spisové služby

Provoz datové schránky úzce souvisí s problematikou evidence datových zpráv, tj. s evidencí doručených a odesílaných dokumentů. V případě velké organizace typu krajský úřad, je potřeba takovou evidenci provádět automatizovaně. Přesně tuto úlohu plní **systém spisové služby**. Krajské úřady, jako OVM mají navíc povinnost ze zákona provozovat evidenci dokumentů pomocí elektronického systému spisové služby[13].

Co vše tedy systém spisové služby umožňuje?

Systém eSSL umožňuje evidenci veškerých údajů o dokumentech i spisech včetně sledování pohybu dokumentů v organizaci. Je určen pro kompletní správu dokumentů v organizaci - pro zapisování, tj. evidenci dokumentů včetně přidělení, převzetí, vyřízení, přípravy k vypravení, případně stornování zápisu. Umožňuje evidovat podání došlých i vlastních dokumentů, kde jako základní evidenční prvek používá prvotní identifikátor dokumentu v podobě čárového kódu.

Systém eSSL eviduje profilové i pomocné údaje o dokumentu (věc, odesílatel, klíčová slova, typ dokumentu, úroveň přístupu), vytváří spis, umožňuje zadání údajů o stornu, ztrátě, nalezení, způsobu vyřízení, přerušení a obnově vyřizování, nabytí právní moci, zadání spisových a skartačních znaků a skartačních lhůt, ukládání dokumentů do operativních úložných míst, zadání údajů o odeslání dokumentu mimo organizaci a následné zpracování dodejek. Pro sledování interního oběhu dokumentu v organizaci slouží důsledné předávání a převzetí včetně sledování osobní zodpovědnosti.

eSSL musí pracovat naprosto rovnocenně s analogovými i elektronickými dokumenty. Tzn. jak s dokumenty v papírové podobě, tak s dokumenty v elektronické podobě jako je mimo jiné obrazový nebo zvukový záznam. Údaje o jednotlivých dokumentech se do systému pořizují ručním zadáváním, elektronickým vstupem (čtečkou) nebo je možné data načítat z jiných programů (systémů), např. ze systému CzechPOINT, ISDS, Yamaco. (12)

[13] Dále jen eSSL.

Jakými pravidly se systém eSSL řídí?

Pravidla pro příjem, evidenci, oběh, odeslání a vůbec celý životní cyklus dokumentů (v analogové i digitální podobě), tj. kompletní správu dokumentů v organizaci řeší tzv. **Spisový a skartační řád**. Jedná se o průběžně aktualizovaný interní dokument závazný pro všechny zaměstnance dané organizace.

Pro úspěšné napojení na ISDS musí eSSL splňovat následující podmínky:

- načítání doručených datových zpráv z datové schránky do modulu elektronické podatelny, jejich kontrola a následné zaevidování do spisové služby
- vyhledávání datových schránek adresátů při přípravě dokumentu na vypravení
- převod připravovaného dokumentu do výstupního formátu (PDF/A) a jeho opatření uznávaným elektronickým podpisem, případně uznávanou elektronickou značkou
- vypravení připravených dokumentů prostřednictvím datové schránky, včetně řešení neočekávaných stavů (datová schránka adresáta byla znepřístupněna, dokument přesáhl povolenou velikost aj.), načítání informací o dodání a doručení vypraveného dokumentu a spárování této informace s dokumentem
- uložení datových zpráv (doručených i vypravených) a dokumentů v nich obsažených do bezpečného úložiště (13)

Typickým příkladem eSSL splňujícím všechny funkční a legislativní požadavky je spisová služba GINIS. Z celkového počtu 14 krajských úřadů provozuje více jak polovina z nich právě eSSL GINIS.

5.4 Elektronické certifikáty

S provozem datových schránek úzce souvisí potřeba elektronických certifikátů, tj. elektronického podpisu, elektronické značky a časového razítka. Legislativa přímo říká, že dokumenty odesílané prostřednictvím datové schránky musí úřad jako OVM podepisovat uznávaným elektronickým podpisem. Dokument musí obsahovat doklad o autentičnosti odesílatele a samotného obsahu dokumentu. Kromě toho je uznávaný elektronický podpis přímo vyžadován některými dalšími právními předpisy, především správním řádem a zákonem o správě daní a poplatků.

V ČR vydávají zaručené elektronické certifikáty[14] tři akreditovaní poskytovatelé certifikačních služeb[15] a sice Česká pošta, s.p. (PostSignum), První certifikační autorita, a.s. (I.CA) a eIdentity, a.s.. Zájemce si tedy může vybrat, u kterého poskytovatele si nechá elektronický podpis vystavit.

Některé Krajské úřady, konkrétně Jihomoravský kraj a kraj Vysočina, řeší problematiku vystavování elektronických certifikátů tím způsobem, že uzavřeli s I.CA smlouvu o poskytování certifikačních služeb a provozují na svém úřadě službu tzv. Veřejné registrační autority (dále jen VRA). Jedná se o pracoviště oprávněné vydávat elektronické certifikáty ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu. Pracoviště VRA je určené pro kontakt s nejširší veřejností. Úkolem tohoto pracoviště je příjem žádostí o vydání certifikátu a ověření totožnosti žadatele. VRA je oprávněna vydávat všechny typy zaručeného elektronického podpisu pro všechny typy uživatelů (fyzické i právnické osoby včetně obcí). KrÚ JMK v hojné míře využívá VRA pro vydávání elektronických certifikátů vlastním zaměstnancům.

V současné době, konkrétně od 1. 1. 2010, jsou v souladu se stanovením MV ČR kvalifikované certifikáty a kvalifikované systémové certifikáty vydávány s podporou algoritmu šifrování SHA-2[16] a minimální délky kryptografického klíče algoritmu RSA 2048 bitů[17].

Koncem května 2010 došlo ke změně ověřování přístupu k serveru datových schránek.

---

[14] Viz zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů.
[15] Certification Service Provider - CSP
[16] SHA-2 -
[17] I.CA podporuje algoritmy SHA-256 a SHA-512

Z tohoto důvodu je nutné mít na všech pracovních stanicích, ze kterých je přistupováno do ISDS, nainstalován nový kořenový certifikát PostSignum založený právě na algoritmu šifrování SHA-2.

5.4.1 Vysvětlení základních pojmů

V následující kapitole považuji za vhodné vysvětlit základní pojmy z oblasti elektronických certifikátů.

Co je elektronický podpis

Elektronický podpis jsou data, která jsou připojena k dokumentu a nahrazují vlastnoruční podpis. Vznikl z potřeby vytvořit nástroj, který by v elektronických dokumentech plnil obdobnou funkci jakou zajišťuje v listinných dokumentech podpis vlastnoruční.

Tento nástroj musí zajistit:

- **Autentičnost zprávy -** tedy jistotu, že zprávu podepsala osoba uvedená v certifikátu.
- **Integritu zprávy** – možnost snadno zjistit jakoukoliv následnou změnu zprávy.
- **Nepopíratelnost odpovědnosti podepsané osoby -** osoba, která zprávu podepsala, nemůže svou činnost popřít.

Pro zajištění těchto požadavků se v ČR využívá tzv. **„zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb“,** který je definován zákonem č. 227/2000 Sb. o elektronickém podpisu. Tento podpis je v zákoně o elektronickém podpisu označován též jako „uznávaný elektronický podpis“.

Elektronický podpis je technologicky založen na kombinaci kryptografických metod, konkrétně na asymetrické kryptografii. Bezpečnost a důvěryhodnost elektronického podpisu je závislá zejména na délce šifrovacích klíčů, typu algoritmů,

kvalitě nosiče a ochrany klíčů[18] a způsobu implementace. Jedná se o velmi složitou technologii, jejíž praktické využití je díky implementaci do standardního programového vybavení velmi jednoduché. (3)

Co je certifikát

Certifikát je digitální dokument, ve kterém jsou uvedeny tyto položky: čísla certifikátu, doba platnosti, ověřovací metody (podle druhu certifikátu) a zejména údaje identifikující příslušnou osobu a její veřejný ověřovací klíč. Tento digitální dokument je pak digitálně podepsán **certifikační autoritou**, což dohromady tvoří podepsaný certifikát. (4)

Kvalifikovaný certifikát

Kvalifikovaný certifikát je certifikát, který byl vydán podle zákona o elektronickém podpisu a který se používá výhradně pro účely elektronického podepisování. Pokud tedy chceme používat elektronický podpis, musíme si pořídit právě tento certifikát.

Nekvalifikovaný (komerční) certifikát

Kromě kvalifikovaných certifikátů existuje řada dalších certifikátů, které se používají například pro autentizaci, šifrování a další procesy. Tyto certifikáty se často nazývají **komerční**. Po technické stránce jsou velmi podobné kvalifikovaným certifikátům, ale liší se způsobem používání a právními účinky. Vydávání těchto certifikátů není upraveno žádným zákonem.

Elektronická značka

Pokud elektronický podpis přirovnáme k vlastnoručnímu podpisu, tak elektronickou značku si můžeme představit jako obdobu otisku razítka. Technologicky jsou elektronický podpis a elektronická značka velmi podobné, hlavní rozdíl je v legislativní stránce. Elektronickou značkou jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené.

[18] Např. použití čipové karty, tokenu.

Elektronická značka je založena na **kvalifikovaném systémovém certifikátu** a může být vydána jak fyzické, tak právnické osobě. Označování elektronickou značkou může probíhat automatizovaně. Například IS elektronické podatelny může automatizovaně označovat doručenky přijatých zpráv. (15)

Časové razítko

Časové razítko je důkazem toho, že konkrétní dokument existoval nejpozději v době, která je v časovém razítku uvedena a potvrzena autoritou, která časová razítka vydává[19]. (1)

Časové razítko je připojeno k digitálnímu dokumentu, podobně jako el. podpis. Platnost časového razítka je 3 roky. Po vypršení platnosti razítka je dokument nadále považován za pravý, není nutné provádět tzv. „přerazítkování“. (7)

Je také pravdou, že názory na zajištění autenticity dokumentů pomocí časového razítka nejsou dosud jednotné a v průběhu času se vyvíjí. Konkrétně názor, zda je nutné dokumenty „přerazítkovávat“ či nikoliv. Nicméně poslední veřejně prezentovaný názor[20] je takový, že dokument stačí opatřit elektronickým podpisem a časovým razítkem jen jednou.

Poskytovatel certifikačních služeb neboli certifikační autorita

Kvalifikované certifikáty vydává tzv. poskytovatel certifikačních služeb. Často se můžeme setkat i s pojmem certifikační autorita. Poskytovatel certifikačních služeb je subjekt, který je důvěryhodný pro uživatele certifikačních služeb, tj. pro podepisující osoby, kterým vydává certifikáty a pro osoby, které se spoléhají na podpisy s nimiž jsou tyto certifikáty spojeny.

Certifikační autorita zejména vydává certifikáty a zajišťuje jejich správu včetně jejich zneplatňování. Vydané certifikáty podepisuje svým elektronickým podpisem, čímž je chrání proti případné modifikaci a je identifikovatelná jako subjekt, který je vydal.

V oblasti orgánů veřejné moci je možné používat pouze kvalifikované certifikáty vydané akreditovaným poskytovatelem certifikačních služeb. (11)

---

[19] TSA - Time Stamp Autority.

[20] Jedná se o názor prezentovaný Odborem archivní správy a spisové služby MV ČR, viz (7).

Kořenové certifikáty poskytovatele certifikačních služeb

Každý poskytovatel certifikačních služeb má kvalifikované certifikáty, které používá k podepisování vydávaných certifikátů. Těmto certifikátům se říká **kořenové certifikáty**.

Tyto certifikáty má vystavené na svých webových stránkách a jsou dostupné i na dalších místech, která jsou popsána v certifikační politice. Všechny kořenové certifikáty ověřuje a publikuje na svých stránkách také MV ČR.

Pokud jsou v počítači nainstalovány kořenové certifikáty certifikační autority, aplikace důvěřují certifikátům vydaným touto certifikační autoritou. (11)

5.4.2 Ověřování platnosti elektronického podpisu

S elektronickým podepisováním dokumentů a vůbec s využíváním elektronického podpisu nutně souvisí otázka **ověření platnosti elektronického podpisu**. Každý podpis je vystaven s omezenou dobou platnosti, obvykle jeden rok. V praxi se proto můžeme setkat s případem, kdy je doručený dokument opatřený podpisem, kterému zbývá do vypršení platnosti několik dnů a nebo byl z nějakého důvodu (např. ztráty, ukončení pracovního poměru) předčasně zneplatněn. Takový dokument se může dostat ke zpracování příjmu resp. na podatelnu ve chvíli, kdy mu již vypršela platnost elektronického podpisu. Pomineme nyní právní výklad, podle kterého lze i dokument s prošlým podpisem považovat za platný a autentický neprokáže-li se opak (blíže v kapitole 7.3) a zaměříme se na **technickou stránku** věci. Tzn. základní proces ověření platnosti podpisu a otázku, **jakým způsobem lze ověření provést a co všechno je vhodné u elektronického podpisu kontrolovat**.

Ověření podpisu

Při ověřování podpisu se ověřuje následující:

- Integrita dokumentu – dokument nebyl od okamžiku podpisu změněn (ověřuje aplikace)
- Vydavatel certifikátu – certifikát, na kterém je založen podpis, vydala certifikační autorita, které důvěřujeme (tj. máme nainstalovány její kořenové

certifikáty v systémovém úložišti kořenových certifikátů důvěryhodných certifikačních autorit)

- Platnost kořenového certifikátu certifikační autority – ověřuje se interval platnosti a to, že certifikát nebyl zneplatněn, pokud je více nadřízených certifikátů, ověřují se takto všechny nadřízené certifikáty
- Platnost certifikátu na kterém je založen podpis – ověřuje se interval platnosti a to, že certifikát nebyl zneplatněn
- Komu byl certifikát vydán (vždy ověřuje uživatel, nikdy aplikace) (1)

Je vhodné upřesnit, že prvotní ověření elektronického podpisu probíhá při zpracování přijaté DZ na podatelně úřadu, tj. v systému eSSL (modul Podatelna). Proces ověření probíhá automatizovaně, a to na základě ověřování podpisu oproti platnému kořenovému certifikátu příslušné CA a tzv. CRL[21] seznamu. Systém elektronické podatelny přijímá každé podání, včetně podání s neplatným podpisem. Na odborném referentovi potom záleží, zda dokument s neplatným podpisem přijme ke zpracování, tj. zda daný podnět ze zákona vyžaduje elektronický podpis či nikoliv. Odlišná situace nastává, pokud ověření platnosti provádí přímo pracovník na svém PC, který ověřuje např. dokument zaslaný elektronickou poštou (typicky podepsané PDF) nebo platnost podpisu e-mailové zprávy. V takovém případě lze doporučit osobní kontrolu platnosti podpisu.[22] V případě kontroly platnosti elektronického podpisu v programu Adobe Reader, je nutné přímo do prohlížeče vložit kořenové certifikáty CA nebo provést změnu nastavení, konkrétně povolit integraci kořenových certifikátů systému Windows do Adobe Reader (viz Příloha č. 4).

[21] CRL – Certification Revocation List - aktualizovaný seznam zneplatněných certifikátů zveřejňovaný příslušnou CA

[22] Postup kontroly platnosti elektronického certifikátu je v Příloze č. 4.

5.5 Převod dokumentů do formátu PDF

V souvislosti s datovou schránkou vyvstala potřeba zajistit převod elektronických dokumentů obvykle z prostředí Microsoft Office[23] do formátu PDF/A[24]. Formát PDF/A je určen legislativou[25] jako jediný vhodný formát pro trvalé uložení a uchování (archivování) obsahu dokumentu, jež má zaručovat jeho neměnnost. Současně má pomocí vkládaných kryptografických prvků, jako je elektronický podpis, elektronická značka a časové razítko zajistit autenticitu dokumentu. O tom ale více v dalším textu.

Organizace typu Krajský úřad (a všechny ostatní) proto stály před otázkou, jakým prostředkem konverzi dokumentů spolehlivě zajistit. Řešení musí splňovat následující podmínky:

- maximální spolehlivost
- možnost současného vložení elektronického podpisu a časového razítka
- začlenění do provozované eSSL úřadu
- dostupnost všem pracovníkům, kteří disponují elektronickým podpisem, nejlépe všem pracovníkům na úřadě
- garance technické podpory řešení dodavatelem
- finanční dostupnost

Existuje velké množství řešení převodu dokumentů do formátu PDF, nicméně na základě předešlých požadavků lze některé ihned vyloučit. Převod řeší např. MS Office 2007, který má v sobě tuto funkci již zakomponovanou, ale nedokáže k vytvářenému PDF přidat elektronický podpis. Dále existují různé volně přístupné řešení typu freeware, např. produkt PDF Creator, který byl odzkoušen, ale nenabízel patřičnou spolehlivost. Na řadu přicházejí komerční produkty u kterých lze po odzkoušení doporučit řešení firmy SW602, konkrétně program Print2PDF.

Print2PDF funguje na principu lokální virtuální tiskárny, nebo je přístupný pomocí webové služby, kterou mohou využívat systémy eSSL.

[23] Zejména soubory formátu *.doc, *.docx, *.rtf, *.xls.
[24] PDF/A - Portable Document Format for the Long-term Archiving.
[25] Viz zákon č. 191/2009, § 20, odst. 2

Print2PDF je v současné době využíván na několika krajských úřadech, kde je provozován jako webová služba a je začleněn do eSSL. Funguje bez zásadních problémů.

5.6 Úložiště elektronických dokumentů

Vzhledem k výraznějšímu nárůstu dokumentů v elektronické podobě, tj. zvýšenému objemu dat, je nutné zajistit dostatečné datové úložiště pro jejich bezpečné uložení. Současně se zvyšuje počet datových zpráv, které musejí organizace typu krajský úřad uchovávat v úložišti elektronické podatelny. Zde musí být ukládány všechny příchozí i odchozí datové zprávy (včetně doručenek), a to po celou dobu životního cyklu spisu, do kterého byly zařazeny, až do ukončení skartačního řízení. (13) Kromě samotného uložení je nutné zajistit i vhodnou dostupnost dat a spolehlivý způsob zálohování. Dokumenty musejí být k dispozici i v případě výpadku některého z disků, minimálně v průběhu pracovní doby, a současně je třeba všechny dokumenty zálohovat pro případ nevratného poškození dat. Dostatečnou kapacitu diskového pole nelze jednoznačně doporučit, je to individuální záležitost v každé organizaci. Můžeme jen uvést příklad KrÚ JMK, kde kapacita elektronického úložiště dokumentů po půl ročním provozu DS tvořila zhruba 70 GB.

Obecně lze doporučit vytvoření tzv. **garantovaného datového úložiště**, které bude sloužit především jako důvěryhodné úložiště datových zpráv a dále jako elektronická spisovna pro uzavřené elektronické spisy[26], případně i uložené dlouhodobě otevřené spisy (13). Standardní úložiště dat (negarantované) primárně slouží k průběžnému a spíše krátkodobému ukládání a zálohování dat, neřeší otázku dlouhodobého ukládání, archivace a hlavně validity dat v podobě elektronických dokumentů. K tomuto účelu by mělo sloužit garantované úložiště, pro které je klíčovou úlohou právě zajištění validity a autorizovaného přístupu k dokumentům[27].

[26] Resp. elektronické části hybridních spisů obsahujících listinné i elektronické dokumenty.
[27] Tj. umožnit přístup k datům jen oprávněným osobám, k datům nesmí být povolen přístup ani správci IS.

Zajištění validity dokumentů znamená, že:

- dokument zůstane uchován po libovolně dlouhou dobu v podobě, v jaké byl uložen a tuto skutečnost bude možné nezpochybnitelně prokázat
- bude možné kdykoliv prokázat původ (autorství) dokumentu
- bude možné kdykoliv prokazatelně určit čas vzniku dokumentu (zdroj-analýza)

Způsob, jakým lze dosáhnout splnění těchto požadavků, je využití elektronické značky a časového razítka. Více tato problematika v práci rozebírána nebude, protože se jedná o oblast velmi širokou a to jak technicky, tak legislativně. Nicméně považuji za důležité otázku garantovaného úložiště zmínit a upozornit v souvislosti se zavedením ISDS. Pro OVM totiž vyplývá zákonná povinnost[28] zajištění datového úložiště elektronických dokumentů. Zákon zcela přenáší odpovědnost za uchovávání dokumentů na původce, přičemž uvedeným zákonným podmínkám[29] plně vyhovuje pouze důvěryhodná archivace tj. důvěryhodné úložiště.

5.7 Optimalizace stávajícího modelu

Stávající model tvoří samotný ISDS a přímo související technická řešení umožňující zasílání DZ (viz předchozí body v kap. 5). Tento model je od počátku nasazení DS určitým způsobem vymezen (legislativou a dostupnými technickými prostředky) a teprve od chvíle ostrého spuštění systému a v průběhu běžného provozu postupně krystalizují problémy, otázky a další požadavky na vhodná řešení celé problematiky ISDS. Můžeme konstatovat, že vzniká potřeba **optimalizace stávajícího modelu**. Z tohoto důvodu bude v následující kapitole (kap. 6.) provedena analýza současného stavu nasazení DS v prostředí konkrétní organizace KrÚ JMK a na základě získaných podkladů proveden návrh optimálního modelu ISDS.

[28] § 64-69 novely zákona č. 499/2004 Sb. o archivnictví a spisové službě a ze zákona 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů.
[29] § 69a, odst. 3 zákona 499/2004 Sb. o archivnictví a spisové službě.

6 ANALÝZA ŘEŠENÉHO PROBLÉMU

Analýza problematiky datových schránek byla konkrétně zaměřena na implementaci a provoz datové schránky v informačním systému Krajského úřadu Jihomoravského kraje[30]. Součástí analýzy je charakteristika organizace KrÚ JMK a jeho informačního systému, postup implementace datové schránky a nakonec zhodnocení celého provozu a využití datových schránek za pomoci SWOT analýzy (viz kap. 6.4).

Jihomoravský kraj přistoupil k aktivaci své datové schránky dne 1. 10. 2009, tj. měsíc před její povinnou aktivací, ještě v průběhu tzv. přechodného období. Během tohoto měsíce bylo aktivováno velmi málo schránek a KrÚ měl možnost komunikovat jen s omezeným množstvím subjektů. Nicméně datová schránka JMK byla připravena k použití a zcela začleněna do IS organizace, zejména eSSL. Nyní je DS denně využívána v rutinním provozu a poskytuje rychlý způsob elektronické komunikace. Přesto se ukazuje, že způsob napojení a využívání DS v rámci IS JMK lze v mnoha ohledech zlepšit a optimalizovat. Především z pohledu zajištění bezpečného přístupu do DS, většího rozšíření funkčnosti eSSL a tím pádem určitého vyššího komfortu pro uživatele, zjednodušení administrace systému a z pohledu bezpečného uchovávání dokumentů.

[30] Dále jen IS KrÚ JMK.

6.1 Charakteristika organizace Jihomoravský kraj

Téma ISDS je v této práci popisováno v prostředí Krajského úřadu Jihomoravského kraje. Organizace spadá do oblasti veřejné správy, kde plní úkoly ve věcech samostatné působnosti při samosprávě kraje a vykonává státní správu v přenesené působnosti.

Jihomoravský kraj je veřejnoprávní korporací s právní subjektivitou, která vlastní majetek, má vlastní příjmy a hospodaří podle vlastního rozpočtu. Kraj je zastupován hejtmanem, který předsedá jednáním zastupitelstva kraje a je členem rady kraje. KrÚ je jedním z orgánů kraje, v jehož čele stojí ředitel, kterého se souhlasem ministerstva vnitra do této funkce jmenuje a odvolává hejtman příslušného kraje.

KrÚ JMK se člení na 17 odborů a 3 útvary, jejichž přesná náplň činnosti je vymezena Organizačním řádem. Ke konci roku 2009 bylo na KrÚ 596 pracovníků. (8)

Jak tedy KrÚ JMK stručně charakterizovat, jaká je jeho úloha, přínos a vůbec hlavní náplň činnosti? Jaký způsob komunikace v organizaci převažuje? KrÚ JMK plní především roli správce rozpočtu, roli zřizovatele a správce příspěvkových organizací (např. škol, sociálních ústavů apod.), roli odvolací instance a roli správce mnoha agend vymezených zákonem (např. v oblasti životního prostředí, sociální, zdravotní, dopravní, kulturní). Klíčovou úlohu úřadu dále tvoří příjem a zpracování žádostí o dotace a přerozdělování finančních prostředků. Pro KrÚ je tedy naprosto zásadní písemná komunikace, ať v podobě papírové nebo elektronické. Pro účely příjmu a vypravení dokumentů KrÚ provozuje dvě podatelny, jednu elektronickou podatelnu[31] a datovou schránku. S rozvojem e-governmentu nabývá stále většího významu komunikace elektronická, a stále více je využíváno doručování pomocí datové schránky (více viz kap. 8).

[31] podání lze zasílat na adresu posta@kr-jihomoravsky.cz nebo přes webový portál http://poe.gordic.cz/KUJM/

6.2 Informační systém Krajského úřadu

Informační systém Krajského úřadu Jihomoravského kraje jako celek tvoří několik autonomních „subsystémů“, správa uživatelů, vhodná síťová infrastruktura a samotné datové úložiště. Jen některé systémy jsou ale vzájemně propojeny. Především z důvodu zajištění bezpečnosti a z důvodu technických možností samotných systémů.

Klíčovou část IS KrÚ tvoří tzv. adresářová služba **Active Directory**, určená především pro definici organizační struktury a správu uživatelských účtů v prostředí Microsoft Windows. Active Directory zajišťuje základní přístupová oprávnění do domény KrÚ pro všechny pracovníky úřadu.

Mezi hlavní informační systémy patří IS GINIS. Jedná se o centralizovaný páteřní IS, který pokrývá všechny klíčové potřeby KrÚ a prostřednictvím specializovaných modulů řeší jednotlivé agendy. Základní rozdělení tvoří agenda ekonomická a agenda spisové služby. Systém využívá jednotného číselníku subjektů (tzv. kartotéku externích subjektů) a pro jednoznačnou dohledatelnost opatřuje každý dokument či subjekt na vstupu jedinečným identifikátorem (tzv. PID). Základní architektura systému je typu klient-server, datová základna je založena na databázovém serveru Oracle 10g. K přístupu do některých modulů je využíván i tzv. tenký klient (.NET). V IS GINIS jsou evidováni všichni zaměstnanci úřadu (bez vazby na Active Directory). Práva pro přístup do IS GINIS má celkem 550 uživatelů, z toho 290 do evidence spisové služby (stav k březnu 2010). Pro účely této práce bude popisována pouze oblast spisové služby.

Krajský úřad využívá tyto komponenty eSSL GINIS:

- USU (universální spisový uzel v těžké i tenké technologii)
- POD (podatelna)
- VYP (výpravna)
- SPI (spisovna)
- webovou službu s vazbou na Czech POINT[32]

[32] Umožňuje evidenci žádostí z Czech POINT do eSSL

6.3 Datová úložiště Krajského úřadu

V této kapitole jsou definována datová úložiště KrÚ určená především pro elektronické dokumenty generované organizací a přijaté datovou schránkou nebo elektronickou podatelnou. Jedná se zejména o dokumenty formátu DOC, PDF a ZFO. Dále je zde definována otázka dostupnosti, zálohování a zabezpečení dat z pohledu autentizace a autorizace přístupu k datům v prostředí eSSL a domény KrÚ.

Datová úložiště elektronických dokumentů

- **Datové úložiště** tvoří diskové pole HP EVA 4400 se šesti diskovými policemi osazenými celkem 72 rychlými „Fiber Channel" disky o celkové hrubé kapacitě 18.985 GB. Z toho pro datové zprávy a spisovou službu je vyčleněna kapacita 385 GB.
- **Dostupnost** dat v případě výpadku některého z disků zajišťuje uspořádání diskového pole RAID 5 (RAID - zkratka Redundant Array of Independent Disks - vícenásobné diskové pole nezávislých disků).
- **Zálohování** dat je řešeno za pomoci týdenních plných a denních rozdílových záloh všech serverů a dat aplikací na diskové pole umístěné v další budově KrÚ. Jedná se o diskové pole HP EVA 4400 s pěti diskovými policemi osazenými celkem 60 pomalejšími „Fiber Channel" disky SAS o celkové hrubé kapacitě 48.418 GB. Obě lokality jsou propojeny dvěma páry optických kabelů. Jeden pár je použit k propojení sítí LAN a druhý pro propojení sítí SAN.
- Veškeré **elektronické dokumenty** přijaté elektronickou podatelnou, datovou schránkou nebo tzv. vlastní dokumenty pořízené pracovníky úřadu, tvoří v eSSL tzv. **elektronický obraz** nebo **přílohy** dokumentu.
- **Přístup k datům v rámci eSSL**, které tvoří elektronický obraz dokumentu nebo příloha, je řešen pomocí autentizace (jméno a heslo uživatele) a autorizace (zvolený typ dokumentu v rámci eSSL).
- **Obecnou úroveň přístupu k dokumentům** v síti KrÚ[33] řeší autentizace uživatele v rámci Active Directory, kde má každý uživatel přidělený limitovaný

[33] doména „kr-jihomoravsky"

datový prostor a na základě definice organizační struktury (svého začlenění) má oprávnění přistupovat jen do vyhrazeného datového prostoru.

- Logování přístupu není v síti KrÚ nastaveno z důvodu nemožnosti vyhodnocení přístupů bez patřičného SW.
- Šifrované ukládání dat není nastaveno.
- IS GINIS ukládá veškeré elektronické dokumenty na tzv. fiktivní „server pro úložiště el. dokumentů“, který se vytváří v administračním modulu ADM. Takto vytvořený server je navázán na reálné (fyzické) elektronické úložiště tvořené diskovým polem.

V současné době dochází k postupnému převodu fyzických serverů na virtuální servery s využitím HP Blade systému C7000 a diskového pole HP Eva 4400. Při určení pořadí virtualizace serverů je přihlíženo jak ke stáří fyzických serverů, tak k důležitosti na nich běžících aplikací.

6.4 Aplikace datové schránky v organizaci

Prvním krokem k aplikaci datové schránky byla implementace ISDS do prostředí IS KrÚ JMK. Celá implementace probíhala převážně ve druhé polovině roku 2009. Jednotlivé kroky musely být vyřešeny nejpozději do 1. 10. 2009, tedy do termínu, který vedení KrÚ stanovilo jako termín pro aktivaci datové schránky. Některé oblasti implementace jsou řešeny stále a průběžně, v závislosti na vývoji ISDS, systému eSSL a nově zveřejňovaných informací z oblasti legislativní a metodické.

Implementace probíhala v několika krocích :

a) napojení spisové služby a ePodatelny na ISDS
b) vystavení elektronických certifikátů
c) instalace kořenových certifikátů CA
d) reinstalace DB klienta Oracle 9i včetně komponenty OLE DB Provider
e) jmenování administrátora a osob pověřených k přístupu do DS
f) metodické a procesní řešení

a) Napojení spisové služby a ePodatelny na ISDS

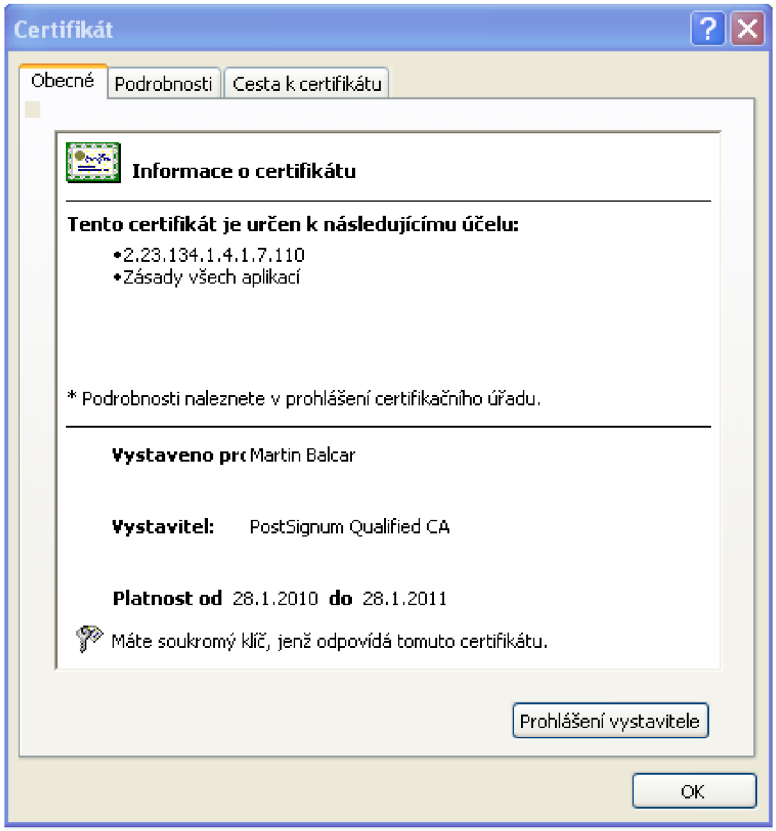
Napojení systému spisové služby a ePodatelny na ISDS předcházela rozsáhlá jednání s dodavatelem eSSL, při kterých se upřesňovala zejména technická specifikace a podmínky, za kterých má propojení obou IS fungovat. Podmínkou bylo vytvoření testovacího prostředí, ve kterém bude možné celou funkčnost propojení vyzkoušet ještě před ostrým spuštěním provozu. V průběhu července 2009 bylo testovací prostředí zprovozněno a první odeslání a příjem datových zpráv úspěšně odzkoušeno. Testovací prostředí tvořila testovací DB GINIS včetně eSSL a napojení na testovací verzi ISDS. Celá funkčnost eSSL a ISDS se ale stále vyvíjela a do doby ostrého spuštění doznala mnoha změn.

b) Vystavení elektronických certifikátů

Jihomoravský kraj přistoupil k rozhodnutí všechny odesílané dokumenty elektronicky podepisovat. Z toho důvodu došlo na jednotlivých odborech k definování **oprávněných osob**, tj. osob které mají podle podpisového řádu pravomoc samostatně podepisovat

rozhodnutí a jiné dokumenty vznikající na úřadě. Těmto osobám byl postupně vystaven zaměstnanecký kvalifikovaný certifikát opravňující k vytváření zaručeného elektronického podpisu.[34] Jednalo se přibližně o 120 zaměstnanců. Ke správě a vydávání těchto certifikátu KrÚ využívá vlastního pracoviště VRA I.CA[35].

S ohledem na bezpečnost jsou kvalifikované certifikáty generovány na kryptografické zařízení, tzv. token. Jedná se o zabezpečené HW zařízení (vizuálně podobné flash disku), na které se importuje soukromý klíč certifikátu, který již nelze exportovat. Použití tohoto soukromého klíče, tedy možnost elektronicky podepisovat, je možné pouze se znalostí bezpečnostního PINu, který si žadatel o certifikát sám definuje a zadává jej při každém použití tokenu. Správná funkčnost tokenu je dále podmíněna instalací korektního ovladače k danému typu tokenu, instalací aplikace SecureStore pro správu samotného tokenu a instalací kořenového certifikátu CA na lokální stanici.



Obr. 4 - Detailové okno kvalifikovaného certifikátu – informace o certifikátu, zdroj: KrÚ JMK

[34] Názvosloví podrobněji vysvětleno v kapitole 5.4
[35] Viz kap. 2.3.3

c) Instalace kořenových certifikátů CA

Kořenové certifikáty CA je nutné instalovat na každou pracovní stanici, kde dochází k použití elektronického certifikátu, tj. elektronickému podepisování dokumentu, DZ, e-mailu, ověřování certifikátu nebo uživatele apod. Stejně tak je zapotřebí kořenového certifikátu při vstupu na webový portál ISDS[36], což platí i pro přístup přes eSSL. Z jakého důvodu? K zabezpečení webového portálu ISDS je použit certifikát akreditovaného poskytovatele certifikačních služeb PostSignum. Vzhledem k tomu, že kořenový certifikát tohoto poskytovatele není obsažen ve standardní instalaci operačních systémů ani internetových prohlížečů mezi důvěryhodnými certifikáty, je zapotřebí jej nainstalovat do úložiště certifikátů. (11)

Zpočátku byly kořenové certifikáty instalovány ručně, jen na vybrané stanice. Instalovány byly kořenové certifikáty všech akreditovaných poskytovatelů certifikačních služeb v ČR, tj. kořenové certifikáty Post Signum, I.CA a eIdentity. Vzhledem k velkému počtu stanic a poměrně zdlouhavé instalaci, byl hledán jednodušší způsob instalace. Počátkem roku 2010 jsme přistoupili k hromadné instalaci certifikátů za pomoci tzv. doménové politiky v rámci Active Directory. Certifikáty jsou automaticky instalovány na každou stanici, která je připojena do domény krajského úřadu. Stačí pouze sledovat platnost certifikátů a průběžně do seznamu doplňovat aktuálně vydané certifikáty. Jedná se i o kořenové certifikáty potvrzující platnost časových razítek.

d) Reinstalace DB klienta Oracle včetně komponenty OLE DB Provider

Požadovaná funkčnost propojení eSSL na ISDS byla podmíněna instalací databázové[37] komponenty OLE DB Provider, jež je volitelnou součástí DB klienta Oracle. Uživatelé přistupují do eSSL za pomoci tzv. těžkého[38] nebo lehkého[39] klienta GINIS, přičemž nutnou podmínkou pro spuštění těžkého klienta eSSL je instalace DB klienta Oracle na daném PC. Nicméně většina těchto stanic neobsahovala před zavedením ISDS komponentu OLE DB. Bylo tedy nutné provést reinstalaci DB klienta a dohrání požadované komponenty. Jednalo se přibližně o 200 stanic.

[36] www.mojedatovaschranka.cz
[37] Dále jen DB.
[38] Těžký klient - lokální instalace klienta na daném PC určená pro vstup do IS GINIS.
[39] Lehký klient - serverová instalace klienta založená na technologii .NET a webové službě, přístupná z lokálního PC pomocí webového prohlížeče.

Současně s tím byla provedena reinstalace velkého množství DB klientů z verze Oracle 8i na verzi Oracle 9g. Což bylo přípravou na plánované povýšení databáze Oracle 8i na verzi Oracle 9g, která proběhla na počátku roku 2010.

e) Určení administrátora a osob pověřených k přístupu do DS

Oprávněnou osobou je v případě KrÚ hejtman Jihomoravského kraje, který jako první obdržel přihlašovací údaje.[40] Úlohou oprávněné osoby je první přihlášení do administračního portálu ISDS, definování role administrátora a nakonec samotná aktivace datové schránky (stiskem tlačítka).

Administrátorem byl určen ředitel KrÚ a jako zástupce vedoucí odboru informatiky. Úlohou administrátora je určení pověřených osob a jejich práv k přístupu do DS, včetně možnosti samotné aktivace DS. Nejedná se tedy o technickou roli, ale především o právo pověřovat další osoby pro přístup do ISDS.

Pověřenými osobami byly určeny pracovnice podatelny, které mají oprávnění pro načítání a vypravení DZ, vyhledávání a ověřování DS adresátů a jejichž účet je využíván pro autorizaci spisové služby do ISDS.

f) Metodické a procesní řešení

V souvislosti se zavedením datové schránky bylo nutné vytvořit metodiku pro práci s DS, jež obsahuje postup pro ověření existence DS adresáta, způsob příjmu, vytvoření a vypravení DZ a definuje v jakém případě opatřovat dokumenty elektronickým podpisem. Hlavním materiálem obsahujícím uvedené postupy je Spisový a skartační řád KrÚ JMK. Další upřesnění jsou uvedena v Organizačním řádu a Podpisovém řádu organizace. Současně se změnou interních dokumentů proběhlo na KrÚ ještě před spuštěním DS hromadné interní školení zaměstnanců na problematiku ISDS, využití elektronického podpisu a právní výklad v oblasti zpracování a využití DZ. Školení bylo vedeno odbornými referenty odpovídajícími za jednotlivé oblasti, tj. oblast archivace a spisové služby, právní a legislativní a oblast informatiky.

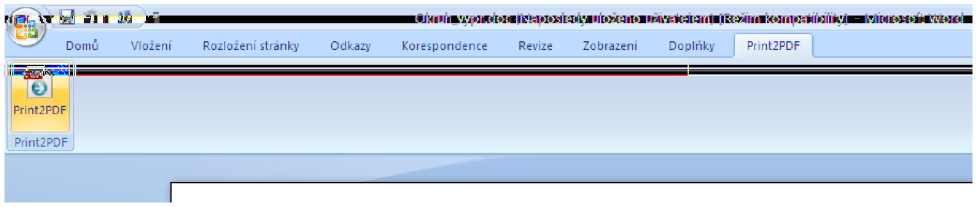
[40] V papírové podobě „do vlastních rukou“.

6.4.1 Převod do PDF a elektronický podpis dokumentů

Pro účely konverze dokumentů do formátu PDF/A je na KrÚ JMK využívána aplikace Print2PDF a sice ve dvou základních režimech. Jako **virtuální tiskárna** instalovaná na pracovní stanici a jako **webová služba** využívána eSSL. V současnosti je plošně využívána forma virtuální tiskárny.

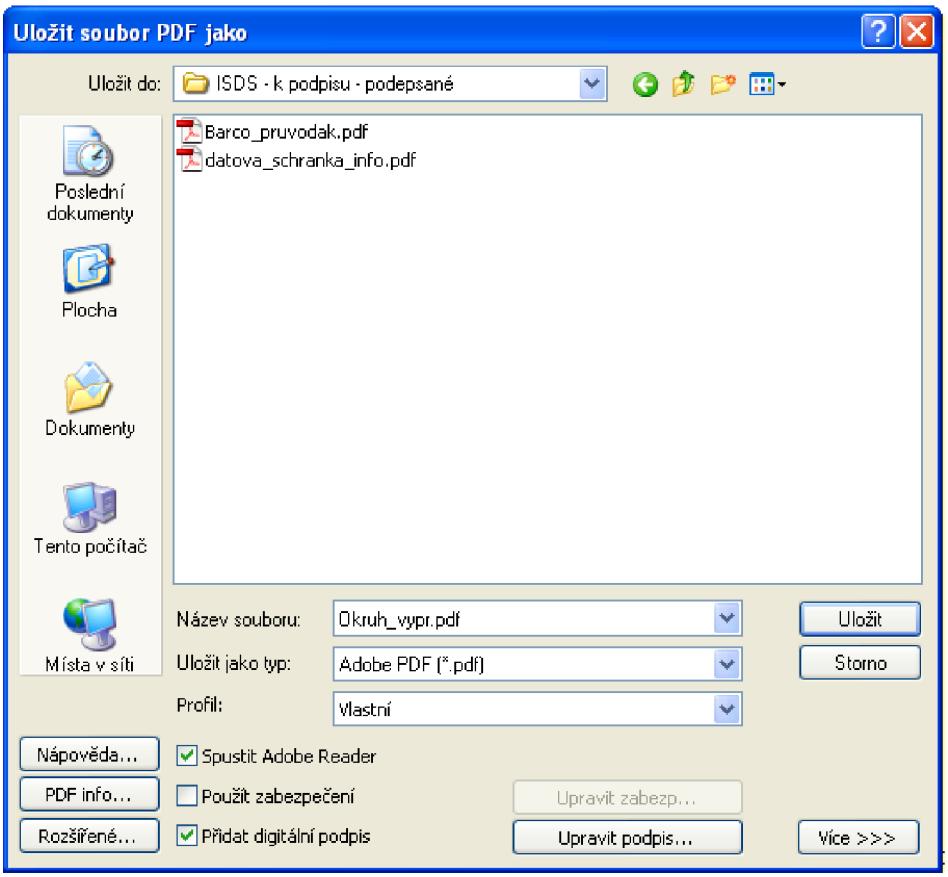
a) Konverze dokumentu a vložení elektronického podpisu v prostředí virtuální tiskárny Print2PDF

Virtuální tiskárna Print2PDF se instaluje na stanici pomocí zástupce sdíleného na aplikačním serveru. Poklikáním na tohoto zástupce dojde k instalaci makra na danou stanici, které se instaluje do prostředí MS Office a obsahuje šablonu s prostředky Print2PDF. Podmínkou úspěšného dokončení instalace je restart PC. V aplikaci MS Word se následně zobrazí nová záložka Print2PDF (obr. 5) pro vyvolání dialogového okna (obr. 6). V tomto okně je potřeba definovat formát PDF/A, vybrat požadovaný podpisový certifikát a cílové umístění nově vytvářeného PDF dokumentu. Po zvolení tlačítka „uložit“ systém vyzve uživatele k zadání bezpečnostního PIN[41] a nový elektronicky podepsaný PDF/A dokument uloží.



Obr. 5 – Ukázka nabídky (záložky) Print2PDF v MS Word 2007; zdroj: KrÚ JMK

[41] PIN – bezpečnostní čtyřmístný kód nutný k použití podpisového certifikátu uloženého na kryptografickém zařízení token.



Obr. 6 – Dialogové okno pro bližší definici konverze, zdroj: KrÚ JMK

b) Konverze dokumentu a vložení elektronického podpisu v prostředí eSSL

Druhým způsobem je konverze a elektronický podpis dokumentu v prostředí eSSL. Jeho velkou předností je, že není nutné nově vytvořený PDF dokument dodatečně vkládat do eSSL. Systém eSSL jej vloží do svého úložiště automaticky sám. Na druhé straně se tato metoda ukázala pro uživatele méně přijatelná.

Oběh elektronických dokumentů k podpisu

Současná praxe je taková, že elektronické dokumenty určené k podpisu nebo již podepsané jsou mezi referentem a vedoucím pracovníkem (oprávněnou osobou) předávány prostřednictvím „odborových složek“. Odborová složka je vyhrazený datový prostor vytvořený na sdíleném síťovém disku, přístupný vždy jen pracovníkům daného odboru na základě organizační struktury úřadu. Tento způsob předávání dokumentů není nejvhodnější a byl zvolen jako určitý kompromis.

V současné době není na KrÚ prostředek, který by dané požadavky splňoval, tj. zajišťoval přijatelné workflow pro oběh dokumentů.

Prohlížení datových zpráv

Datové zprávy lze v IS KrÚ otevírat a prohlížet dvěma způsoby. První způsob nabízí IS GINIS pomocí svého prohlížeče GDZVIEW, druhý způsob je pomocí standardního prohlížeče 602XML Filler. Po otestování obou variant došlo k jednoznačnému rozhodnutí využívat plošně pouze 602XML Filler. Při využití GDZVIEW nastává problém s asociací přípony ZFO, která není využívána jen pro DZ, ale také pro standardní elektronické formuláře, např. v aplikaci Czech POINT. Prohlížeč GDZVIEW nedokáže otevřít jiný formulář než je DZ, a to je z uživatelského pohledu nepřijatelné.

6.4.2 Příjem a odeslání datové zprávy

Příjem DZ je v IS KrÚ řešen centrálně přes elektronickou podatelnu GINIS. Každá přijatá DZ projde procesem zpracování, na závěr kterého pracovnice podatelny přidělí DZ do tzv. spisového uzlu, tj. na sekretariát patřičného odboru.

Odeslání, neboli vypravení DZ probíhá centrálně přes elektronickou výpravnu GINIS, veškeré odesílané dokumenty chystají samotní pracovníci. Tzn. odesílaný dokument zašlou oprávněné osobě k elektronickému podpisu a převodu do PDF (v lepším případě si podpis a konverzi udělají sami), podepsaný dokument PDF/A vloží do své eSSL, vyberou adresáta pomocí tzv. kartotéky externích subjektů, ověří existenci jeho DS případně do systému přidají nebo opraví stávající údaje o DS, vyberou vhodný elektronický obraz či přílohu dokumentu a zvolí odeslat. V tomto okamžiku se DZ objeví v elektronické výpravně a pracovnice výpravny provedou hromadné vypravení.

Na základě získaných hodnot za období leden až duben byl vytvořen **přehled doručených a odeslaných zásilek na KrÚ JMK a jeho možný vývoj do konce roku 2010**. Přehled včetně grafu lze nalézt v Příloze č. 5.

6.5 SWOT analýza

SWOT analýza integrace ISDS v rámci IS KrÚ JMK:

a) Silné stránky (Strenghts)

S1 - rychlost - datová zpráva je doručena prakticky okamžitě

S2 - spolehlivost - datová zpráva se nemůže ztratit, je garantováno doručení

S3 - prokazatelnost - je dokazatelné, kdo datovou zprávu podal a komu byla doručena

S4 - finanční úspora - KrÚ, právnické osoby a fyzické osoby komunikují prostřednictvím ISDS zdarma, datové zprávy odesílané OVM jsou hrazeny ze státního rozpočtu

S5 - KrÚ provozuje tzv. veřejnou registrační autoritu I.CA, tzn. možnost vydávání elektronických certifikátů na počkání přímo v budově úřadu (kvalifikované certifikáty pro zaměstnance)

S6 - přímá vazba ISDS na spisovou službu KrÚ

S7 - možnost elektronického podepisování a konverze dokumentů do formátu PDF/A v prostředí Print2PDF nebo eSSL

S8 – zajištění datového úložiště dokumentů a DZ, včetně dostupnosti a archivace dat je na velmi dobré úrovni

S9 - výpočetní technika na velmi dobré úrovni

S10 - dobrá kvalifikovanost zaměstnanců

S11 - krajský informační webový portál (sdílení informací)

b) Slabé stránky (Weaknesses)

W1 - eSSL neumožňuje hromadné schvalování a podepisování elektronických dokumentů

W2 - řízený oběh elektronických dokumentů

W3 - ISDS garantuje uložení datových zpráv pouze po dobu 90 dnů

W4 - prudký nárůst objemu dat v datovém úložišti, potřeba dostatečné diskové kapacity

W5 – nutnost časté reinstalace SW v rámci sítě KrÚ (602XML Filler)

W6 - autorizovaná konverze, rozpor mezi přípustnými formáty datových zpráv a přípustným formátem pro autorizovanou konverzi dokumentu z elektronické podoby do listinné (jen podepsané PDF)

W7 - placená autorizovaná konverze dokumentů, finanční a časová náročnost pro občana nebo jiný subjekt

W8 - nedostatečné využití spisové služby

W9 - nedostatečná znalost práce s elektronickým podpisem

W10 - problematické vyhledávání příjemců v adresáři, především identifikace fyzických osob

W11 - těžkopádnost ovládání jednotlivých funkcionalit IS spisové služby, nedostatečná uživatelská přívětivost

W12 - uživatelsky složitý proces ověřování platnosti elektronického podpisu ve formátu PDF (tj. v prostředí Adobe Reader)

c) Příležitosti (Opportunities)

O1 - možnost hromadného schvalování a podepisování elektronických dokumentů

O2 - řízený oběh elektronických dokumentů

O3 - rozšíření přístupu do eSSL

O4 - zavedení časového razítka, tj. důvěryhodného dokladu o existenci elektronických dat v daný časový okamžik

O5 - možnost odeslání datové zprávy přímo referentem, nezávisle na e-výpravně, větší operativnost

O6 - zajištění vyššího zabezpečení datové schránky a komunikace s ISDS

O7 - příprava na dlouhodobé uchovávání elektronických dokumentů, vytvoření garantovaného úložiště

O8 - hromadná distribuce SW v rámci sítě KrÚ (602XML Filler, kořenové certifikáty RA)

O9 - změna metodiky, interních norem a procesů v organizaci

O10 - pravidelné tematické školení uživatelů

d) Hrozby (Threats)

T1 – zabezpečení datové schránky a komunikace s ISDS

T2 – dokazování autenticity elektronických dokumentů

T3 – dlouhodobé uchovávání elektronických dokumentů

T4 – lidský faktor v procesu zpracování datových zpráv

T5 – legislativní změny

T6 – změna vedoucí politické strany a politické vůle, změna priorit, ohrožení celého projektu ISDS

Závěry a vyhodnocení SWOT analýzy jsou uvedeny v kapitole 7.

7 NÁVRH ŘEŠENÍ PROBLÉMU

Návrh optimálního způsobu začlenění ISDS do prostředí IS JMK vychází přímo z použité SWOT analýzy, ze které vyplývá poměrně velké množství nedostatků a sporných oblastí. Pro návrh řešení jsem zvolil takové oblasti, u kterých jsem schopný navrhnout nějakou vhodnou a realizovatelnou nápravu.

Návrh se skládá z těchto částí:

- Rozšíření funkčnosti spisové služby (řeší body W1, W2, O1, O2, O3, O5)
- Vyšší zabezpečení datové schránky (řeší body T1, O6)
- Zavedení časového razítka (řeší body T2, O4)
- Hromadná distribuce SW (řeší body W5, O8)
- Vytvoření garantovaného úložiště dat (řeší bod T3, O7)
- Změna metodiky a interních procesů v organizaci (řeší body W5, O9)

Návrh má za cíl řešit lepší využití ISDS v rámci KrÚ, poskytnout zaměstnancům uživatelsky přívětivější prostředí při práci s DS, zjednodušit ovládání, zajistit vyšší bezpečnost při vstupu do systému, zajistit autenticitu dokumentů i po vypršení platnosti elektronického podpisu, navrhnout vhodný způsob aktualizace potřebného SW, zajistit vhodné datové úložiště dokumentů a DZ a v neposlední řadě vytvořit podmínky pro průběžné vzdělávání zaměstnanců, při kterém se seznámí s aktuální problematikou a novými pojmy.

7.1 Optimální model datové schránky

Návrh optimálního modelu ISDS vychází ze zkušeností s provozem DS na KrÚ JMK a z celkového vymezení dané problematiky a v současnosti využívaných technických řešení. Konkrétně tedy z provedené analýzy v kapitole 6.4 a z popisu současného stavu v kapitole 5.

Návrh optimálního modelu ISDS bude obsahovat obecná doporučení, kterými jsou:

- zajištění podmínek pro bezpečnou komunikaci s ISDS – přihlašování do systému pomocí systémového certifikátu, případně vlastními prostředky zajistit vyšší úroveň zabezpečení[42]
- zajištění vhodného prohlížeče datových zpráv – lokální instalace aplikace 602XML Filler nebo instalace zásuvného modulu 602XML Filler do webového prohlížeče např. Mozilla Firefox
- napojení spisové služby a ePodatelny na ISDS
- zajištění vhodného programového vybavení pro konverzi dokumentů do formátu PDF/A a vložení elektronického podpisu do dokumentu
- vystavení zaručených elektronických certifikátů osobám oprávněným podepisovat dokumenty dle tzv. podpisového řádu organizace, tj. dokumenty vedené především dle správního řádu a zákona o správě daní a poplatků (13)
- vybavení pracoviště kvalifikovaným časovým razítkem, které v kombinaci s elektronickým podpisem jednoznačně garantuje pravost odesílaného dokumentu[43]
- zajištění hromadné distribuce kořenových certifikátů všech CA a aktualizací aplikace 602XML Filler
- zajištění vhodného datového úložiště dokumentů a DZ, dostupnost a zálohování dat a příprava na dlouhodobé ukládání a archivaci dokumentů
- vytvoření aktuální metodiky pro využívání datové schránky, tj. aktualizace Spisového a skartačního řádu, Podpisového řádu, Organizačního řádu, případně dalších interních dokumentů

[42] Šifrované spojení pomocí HTTPS, ochranu hesel, ochranu relací, ochranu proti přesměrování - více v příloze 3.
[43] Blíže v kapitole 7.3

7.2 Rozšíření funkčnosti spisové služby

eSSL je jediný prostředek, pomocí kterého jsou referenti napojeni na ISDS, mohou využívat datovou schránku JMK, tj. načítat a odesílat DZ, načítat informace o dodání a doručení DZ[44], vyhledávat a ověřovat existenci adresátů DZ[45], a proto lze doporučit maximální rozšíření eSSL v rámci úřadu. Na základě provedené analýzy (bod O3), lze doporučit, aby **přístup do eSSL měl každý zaměstnanec**, který zpracovává podání a vytváří jakékoliv dokumenty. Již v současné době se pro licencování eSSL využívá tzv. multilicence, takže rozšíření přístupu znamená jen rozšíření licenční smlouvy na požadovaný počet koncových uživatelů. Vzhledem ke zvýšení komfortu evidence a zpracování dokumentů a zrychlení komunikace mezi úřadem a ostatními subjekty se domnívám, že investice do rozšíření počtu licencí eSSL a následné technické podpory je opodstatněná a přinese očekávaný efekt.

Další bod analýzy (O5), který lze doporučit, je **možnost odeslání DZ přímo referentem, nezávisle na e-výpravně**. Současná praxe je taková, že referent v prostředí eSSL k připravované zásilce (obsahující dokument – elektronický obraz nebo elektronickou přílohu) dohledá a připojí identifikaci DS adresáta, jako způsob odeslání zvolí e-výpravnu a potvrdí volbu „odeslat“. Tímto způsobem se připravená zásilka řadí do „fronty“ mezi ostatní, do doby, než pracovnice výpravny všechny zásilky hromadně vypraví, tj. potvrdí v modulu Výpravna odeslání. Pokud referent připraví zásilku k odeslání těsně po hromadném vypravení, může k vypravení jeho zásilky dojít až po 24 hodinách. Domnívám se, že tak dochází ke zbytečnému zdržení (zvláště u rozhodnutí ve správním řízení, kde je nutné dodržovat zákonem dané lhůty), a proto doporučuji možnost odeslání DZ přímo referentem z prostředí jeho eSSL. Navrhovaná funkčnost je v eSSL parametricky nastavitelná. Její využití je podmíněno změnou metodiky odesílání DZ a změnou licenčních podmínek tj. dokoupením funkčnosti.

[44] Tzv. doručenky.
[45] Ostatních subjektů a jejich DS.

Z pohledu fungování úřadu je velmi důležitá otázka řízeného a autorizovaného oběhu elektronických dokumentů. Konkrétně dokumentů určených k podpisu a následně podepsaných dokumentů určených k odeslání do datové schránky. V IS KrÚ není prostředek, který takovou funkci zajišťuje.

Řešení (vycházející z analýzy W1, W2, O1, O2) lze navrhnout v podobě tzv. **Elektronické podpisové knihy (EPK)**. Ta slouží k rychlému a přehlednému zpracování dokumentů určených k podpisu nebo schválení vedoucím pracovníkem, tj. k řízenému oběhu dokumentů mezi referentem a osobou oprávněnou dokument elektronicky podepsat nebo schválit. EPK umožňuje i hromadné zpracování dokumentů. EPK je součástí eSSL GINIS. Předpokládá se využití jak samostatné aplikace typu lehký klient, tak rozšíření funkčnosti v podobě tzv. těžkého klienta USU. EPK je v současné době hotový produkt, který je na KrÚ ve fázi testování.

7.3 Vyšší zabezpečení datové schránky

V souvislosti s používáním datové schránky je vhodné zamyslet se nad hrozbou neoprávněného použití datové schránky. Datová schránka JMK obsahuje množství citlivých údajů, dokumentů a rozhodnutí včetně osobních dat, jejichž zneužití by mohlo mít velmi nepříjemné následky. Včetně finanční sankce, kterou ukládá zákon při zneužití schránky např. formou odcizení, poškození nebo změny dokumentů, případně formou neoprávněného rozesílání spamu.

Zaměstnanci KrÚ přistupují do datové schránky prostřednictvím eSSL. Následně všechny požadavky na komunikaci s ISDS vyřizuje eSSL prostřednictvím přihlašovacího jména a hesla. Z bezpečnostního hlediska je ovšem komunikace a autentizace jen za pomoci přihlašovacího jména a hesla nedostatečná – **přihlašovací jméno a heslo (případně systémový certifikát) nezaručuje dostatečnou bezpečnost datové schránky**[46]. Standardní řešení autentizace do ISDS neřeší otázku ochrany hesel, ochrany relací, šifrované spojení a ochranu přesměrování. (14)

[46] Toto tvrzení se zakládá na modelovém příkladu firmy Kernun - www.kernun.cz , která se zabývá bezpečnou síťovou komunikací a dodává komplexní řešení pro zabezpečení interní sítě.

Z tohoto důvodu lze doporučit **vyšší zabezpečení datové schránky** (analýza T1, O6), konkrétně řešení **Kernun – Bezpečná schránka**[47]. Bezpečná schránka zajišťuje bezpečnost DS pomocí kontroly veškeré komunikace. Má několik unikátních bezpečnostních mechanismů pro odhalení pokusů o odcizení nebo zneužití DS. Řešení je určeno pro bezpečné spojení mezi eSSL a ISDS, který je přístupný přes specializované rozhraní, tzv. XML SOAP zprávy. (14)

Kernun - Bezpečná schránka je HW řešení, které funguje jako aktivní prvek zapojený mezi interní síť (Intranet) a Internet. Řešení se nijak neprojeví na chodu vnitřní počítačové sítě (LAN). Vzhledem k tomu, že JMK již provozuje firewallové řešení Kernun Acces, znamená nasazení Bezpečné schránky pouhé rozšíření stávající funkčnosti, platbu licence a zvýšení servisní podpory. Není třeba pořizovat HW zařízení.

7.4 Zavedení časového razítka

S využíváním ISDS bezprostředně souvisí otázka autenticity elektronických dokumentů, neboli dokazování jejich pravosti a zajištění jejich tzv. „digitální kontinuity“, tj. dlouhodobější časové platnosti dokumentu. Dokumenty zasílané DS jsou opatřeny elektronickým podpisem, ale ten má platnost pouze 12 měsíců od svého vystavení. Jak zacházet s dokumentem, kterému vyprší platnost elektronického podpisu a který je potřeba zkonvertovat do listinné podoby nebo postoupit dál v elektronické podobě a zaručit jeho pravost? Tzn. prokázat, že dokument byl v dané podobě a čase podepsán uvedenou osobou.

Odpověď na tuto otázku poskytuje česká legislativa. Konkrétně zákon č. 499/2004 Sb. uvádí v § 69a, odstavci 8:

„Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán platným uznávaným elektronickým podpisem nebo označen platnou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, osoby odpovědné za převedení z dokumentu v analogové podobě nebo změnu formátu dokumentu v digitální podobě nebo osoby odpovědné za provedení autorizované konverze dokumentu, a opatřen kvalifikovaným časovým razítkem.

[47] Popis řešení a podrobnější vysvětlení principu zabezpečeného přístupu do DS lze nalézt v Příloze 3.

Ustanovení věty první se vztahuje i na dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“[48]

Legislativa tedy jednoznačně určuje, za jakých podmínek lze dokument v digitální podobě považovat za pravý. Musí být splněny oba předpoklady, tj. dokument musí být současně elektronicky podepsán (nebo opatřen elektronickou značkou) a opatřen časovým razítkem. (11)

Na základě výkladu zákona lze tedy jednoznačně doporučit **pořízení, zavedení a využití časového razítka** v co nejbližší době (řeší body T2, O4). V úvahu připadá časové razítko od autority I.CA nebo Post Signum. Vzhledem k porovnání nabídek lze z pohledu KrÚ JMK doporučit časové razítko Post Signum. Zavedení časového razítka prakticky znamená uzavření smlouvy s TSA, získání přístupového jména a hesla (případně certifikátu) pro stahování časového razítka, administrace eSSL pro použití razítka, otestování celé funkčnosti a následně náběh ostrého provozu.

7.5 Hromadná distribuce SW

Pro zobrazení datových zpráv ve formátu ZFO je využíván prohlížeč 602XML Filler. Velkou nevýhodou tohoto prohlížeče je nutnost velmi časté aktualizace a nemožnost otevřít starší DZ v nové verzi a naopak. Od okamžiku spuštění ISDS, tj. za více jak půl roku se jedná přibližně o desátou aktualizaci. Předešlé verze bohužel nepodporují některé nové funkce přidávané do formuláře XML, tj. formuláře DZ nebo Czech POINTu. Filler je lokální instalace „těžkého“ klienta, jehož aktualizaci je nutné provádět pod právy typu „administrátor“. To je velmi nepříjemné pro správu velké sítě[49], kde mají uživatelé na své lokální stanici povolena přístupová práva typu „users“, a tím pádem si sami nemohou potvrdit automatickou aktualizaci aplikace. Automatickou aktualizaci nabízí Filler přímým stažením nové verze ze svých webových stránek.

[48] *Egovernemnt: elektronizace veřejné správy*. C. 1. Praha: info.com s.r.o., 2010. ISSN 1801-9420., s. 8-9.
[49] Síť KrÚ JMK sestává z více než 600 ks PC.

Z tohoto důvodu lze doporučit **řešení hromadné distribuce SW**, konkrétně **hromadnou distribuci nových verzí 602XML Filleru** (řeší body W5, O8). V současnosti je hromadná distribuce Filleru v síti KrÚ řešena za pomoci programu PSExec. Nejedná se ovšem o ideální řešení. Program je spouštěn ručně z příkazové řádky a spuštěná aktualizace Filleru se nahraje jen na aktuálně dostupné stanice. Tzn., že program PSExec je nutné spouštět opakovaně a hlídat podle výpisů (logů) úspěšné nahrání Filleru.

Ideálním řešením je využít tzv. **doménové politiky v rámci služby Active Directory**, a distribuovat nové verze Filleru tímto způsobem. Řešení má jedinou podmínku - vytvořit z dané aktuální verze Filleru tzv. balíček ve formátu MSI, který lze následně distribuovat v síti KrÚ, tj. nahrát ho automatizovaně na každou stanici po jejím přihlášení do domény. Politika sama rozpozná stanice, na které *.msi balíček nebyl nahrán a aktualizaci spustí. (2)

Obdobný problém byl řešen s hromadnou distribucí kořenových certifikátů CA (viz kapitola 5.1). Kořenové certifikáty byly nejprve nahrávány ručně, a nyní je hromadná distribuce řešena za pomoci doménové politiky a funguje bez sebemenších problémů.

7.6 Vytvoření garantovaného úložiště dat

Z analýzy vyplývá (bod T3, O7) potřeba vytvoření, nebo přinejmenším příprava na vybudování garantovaného úložiště dat, do kterého budou postupně ukládány všechny elektronické dokumenty a DZ určené k dlouhodobému a bezpečnému uložení (archivaci). Vzhledem k tomu, že se jedná o finančně velmi nákladnou záležitost, lze doporučit vybudování úložiště v rámci tzv. Technologického centra kraje[50]. KrÚ JMK má v úmyslu využít dotačního titulu z IOP[51] a zapojit se do realizace projektu na vybudování TCK. V rámci TCK bude možné vytvořit jak obecné zálohovací úložiště, tak i důvěryhodné garantované úložiště. Pochopitelně, že se jedná o dlouhodobý projekt na několik let.

[50] Dále jen TCK.
[51] IOP – Integrovaný operační program.

7.7 Metodika využívání datové schránky

V souvislosti s provedenými změnami v předešlých bodech návrhu je nutné doporučit (viz body W5, O9) aktualizaci metodiky využívání datové schránky, tj. aktualizace Spisového a skartačního řádu, Podpisového řádu, Organizačního řádu, případně dalších interních dokumentů. Současně lze doporučit zavedení průběžného školení pracovníků, na kterém si nové postupy osvojí a zdokonalí se např. v problematice elektronického podpisu, terminologii DS, autorizované konverze apod.

8 ZHODNOCENÍ NÁVRHU

Lze předpokládat, že navrhovaná řešení přinesou lepší podmínky pro práci s datovou schránkou na KrÚ a budou znamenat přínos pro zaměstnance, veřejnost i správce výpočetní techniky. Díky realizaci navrhovaných opatření se zvýší uživatelská přívětivost eSSL, zjednoduší se oběh elektronických dokumentů mezi referenty a vedoucími pracovníky a dojde k zabezpečení autenticity vytvářených dokumentů za pomoci časového razítka. To má velký význam jak pro úřad, tak pro občany, kterým i po vypršení platnosti elektronického podpisu zůstane věrohodný dokument, jež lze autorizovaně konvertovat na kterémkoliv místě Czech POINT. S tím úzce souvisí problematika datových úložišť a dlouhodobé archivace dat, která doposud nebyla nijak zásadně řešena a s rozvojem elektronizace státní správy začíná být velmi aktuální. Prudce roste počet elektronických dokumentů, které je nutné vhodným způsobem uchovávat a zabezpečit. Další otázkou je také dostatečně bezpečný přístup do datové schránky. DS je rozhodně víc než běžný e-mail, obsahuje důležité dokumenty a osobní data a proto se spoléhat jen na autentizaci pomocí jména a hesla není příliš bezpečné. Navíc sankce hrozící v případě zneužití DS mohou být pro uživatele schránky velmi nepříjemné.

Smyslem prováděných opatření by měla být také snaha o finanční úsporu. Pokud zhodnotíme počty přijímaných a odesílaných zásilek na KrÚ (viz. Příloha č. 6), dojdeme k závěru, že datové zprávy tvoří maximálně 50% z celkového objemu odesílaných zásilek, přijímaných je ještě méně. Lze tedy konstatovat, že KrÚ a obecně všechny subjekty státní moci mají rezervy ve využití elektronického způsobu komunikace a podle mého názoru by uplatnění modelu optimálního využití ISDS mohlo přinést větší využití tohoto systému a v konečné fázi i finanční úsporu jednotlivým subjektům.

9 ZÁVĚR

Datové schránky jsou významným počinem elektronizace veřejné správy, které bezpochyby řadí Českou republiku mezi pokrokové země a významným způsobem rozšiřují možnosti elektronického prostředí v běžném životě. Jsme celosvětově prvním státem, kde byla komunikace pomocí systému datových schránek uzákoněna. Uvedení datových schránek do provozu sebou neslo přirozeně řadu problémů a nejasností, ale v současné době můžeme konstatovat že systém je plně funkční a úspěšně využíván, zejména mezi OVM. Důkazem je, že za prvních deset měsíců provozu bylo pomocí datové schránky odesláno více jak 10 milionů datových zpráv.

Smyslem práce bylo vytvořit optimální model informačního systému datových schránek, na základě kterého bude navržen optimální způsob začlenění datové schránky do stávajícího prostředí Krajského úřadu Jihomoravského kraje. K dosažení tohoto cíle byla provedena analýza současného začlenění a provozu datových schránek na Krajském úřadě a obecné zhodnocení technického řešení datových schránek. Konkrétním řešením je potom návrh jednotlivých opatření, které pomohou k efektivnějšímu využívání datové schránky, zajistí bezpečnější komunikaci, prokazatelně zabezpečí pravost vytvářených dokumentů a upozorní na potřebu vytvoření garantovaného úložiště dokumentů a datových zpráv.

Lze předpokládat, že provedení změn přispěje k vytvoření stabilnějšího prostředí datových schránek v organizaci a obecně k většímu využití systému a k finančním úsporám. Úsporám jak na straně OVM, které má zasílání datových zpráv zdarma, tak na straně MV ČR, které za odeslané zprávy platí provozovateli systému zhruba poloviční částku oproti standardním doporučeným zásilkám.

Závěrem lze říci, že projekt datových schránek je úspěšný a podle vize MV ČR nebude rozhodně posledním krokem elektronizace veřejné správy. V následujících několika letech je plánováno vytvoření tzv. centrálních registrů veřejné správy, které mají za cíl sjednotit data o občanech do jedné centrální databáze, odstranit tím nejednotnost a roztříštěnost stávajících evidencí a poskytovat všem OVM vždy aktuální a jednotné informace. Realizace této myšlenky bude velmi náročná, především technicky, protože data v současných evidencích jsou často nekompatibilní. Podle mého názoru teprve v okamžiku zavedení centrálních registrů a současně

funkčního systému datových schránek a Czech POINT můžeme hovořit o skutečně komplexním e-governmentu a elektronizaci veřejné správy v ČR.

Na závěr si dovolím krátké zhodnocení. S obecnou snahou rozšiřování elektronické komunikace a celosvětovým trendem elektronizace stále většího množství činností každodenního života nelze jinak než souhlasit. Jedná se o přirozený vývoj společnosti a logický pokrok (nejen v oblasti komunikace), který sebou přináší obrovské možnosti ale současně mění životní styl lidí a vyžaduje od nich vyšší schopnost porozumět tomuto elektronickému prostředí. To je potřeba mít při vytváření elektronického prostředí na paměti a navrhovat elektronizaci procesů takovým způsobem, aby dané „e-prostředí“ lidem práci v první řadě usnadnilo, bylo srozumitelné, přehledné, bezpečné, spolehlivé a vždy dostupné. V tomto ohledu lze konstatovat, že obecná implementace datových schránek jako elektronického prostředí nebyla zvládnuta zrovna nejlépe. Po spuštění ISDS se vyskytovala řada problémů technického rázu, nemluvě o nedořešených metodických a právních otázkách, které udělali na spoustu lidí špatný dojem a zbytečně vrhli na tento ambiciózní projekt stín pochybností.

10 SEZNAM POUŽITÝCH INFORMAČNÍCH ZDROJŮ

1. **BUDIŠ, P.** *Elektronický podpis a jeho aplikace v praxi.* 1. vydání. Praha : Anag, 2008. str. 110. ISBN 978-80-7263-465-1.
2. **JONES, D.** *Automatizace správy a skriptování MS Windows.* Brno : Computer Press, 2006. str. 393. ISBN 80-251-1261-6.
3. **LIDINSKÝ, V.** *Egovernment bezpečně.* 1. vydání . Praha : GRADA Publishing, 2008. str. 144. ISBN 978-80-247-2462-1.
4. **MATES, P. a SMEJKAL, V.** *E-GOVERNMENT v Českém právu.* Praha : Linde Praha, a. s., 2006. str. 244. ISBN 80-7201-614-8.
5. **SMEJKAL, V.** *Datové schránky v právním řádu ČR.* 1. vydání. Praha: ABF, 2009. str. 176. ISBN 978-80-86284-78-1.
6. *Egovernemnt: elektronizace veřejné správy*. C. 2, 3. Praha: info.com s.r.o., 2009. ISSN 1801-9420.
7. *Egovernemnt: elektronizace veřejné správy*. C. 1. Praha: info.com s.r.o., 2010. ISSN 1801-9420.
8. **UHLÍŘOVÁ, K.** Systém hodnocení zaměstnanců a úředníků Krajského úřadu Jihomoravského kraje, 2007. 59 s. Bakalářská práce na Provozně ekonomické fakultě MZLU. Vedoucí bakalářské práce Prof. Ing. Pavel Tomšík, CSc.
9. *eGON NEWS.* **MVČR.** Praha : Ministerstvo vnitra ČR, duben 2009. Speciál ISSS 2009.
10. **Ministerstvo vnitra.** INFORMAČNÍ SYSTÉM DATOVÝCH SCHRÁNEK. *Základní informace.* [brožura]. Praha : Ministerstvo vnitra, 7 2009. Verze 3.0, červenec 2009.
11. **Ministerstvo vnitra.** Oficiální informační web o datových schránkách. *DatoveSchranky.info.* [Online] [Citace: 16. 12 2009.] http://www.datoveschranky.info/o-datovych-schrankach-text/.

12. **GORDIC spol. s.r.o.** SSL - Spisová služba. *GORDIC*. [Online] http://www.gordic.cz/portal/Produkty/GORDICsupsupGINISsupsup/Spisováslužba/tabid/58/language/en-US/Default.aspx.
13. **Plzeňský kraj.** Typový postup implementace zákona č. 300/2008 Sb. *datoveschranky.info*. [Online] verze 3.0, 2009. brožura. www.datoveschranky.info/metodicke-postupy.
14. **Trusted Network Solutions, a.s.** Bezpečná schránka. *Kernun*. [Online] TNS. [Citace: 25. 4 2010.] http://www.kernun.cz/reseni-kernun/bezpecna-schranka/.
15. **První certifikační autorita a. s.** I.CA. [Online] 2010. http://www.ica.cz/cz/menu/2/produkty-a-sluzby/.
16. **Česká pošta s. p.** Post Signum. [Online] 2010. http://www.postsignum.cz/.
17. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů ze dne 17. července 2008.
18. Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.
19. Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

11 SEZNAM ZKRATEK A POJMŮ

ČR	Česká republika
.NET	„dotnet“
CA	Certificate Authority
CRL	Certificate Revocation List - seznam zneplatněných certifikátů
Czech POINT	Český Podací Ověřovací a Informační Národní Terminál
DB	databáze
DNS	Domain Name Systém (systém doménových jmen)
DS	datová schránka
DZ	datová zpráva
EPK	Elektronická podpisová kniha
eSSL	elektronický systém spisové služby
HTTPS	Hypertext Transfer Protocol
HW	hardware
I.CA	První certifikační autorita, a.s.
IS	informační systém
ISDS	informační systém datových schránek
ISSS	konference Internet ve státní správě
KIVS	Komunikační infrastruktura veřejné správy
KrÚ JMK	Krajský úřad Jihomoravského kraje
MSI	Windows Installer Service - instalační služba pro instalaci a správu instalačních balíčků ve formátu MSI v prostředí Microsoft Windows
MV ČR	Ministerstvo vnitra České republiky
OVM	orgán veřejné moci
PDF/A	Portable Document Format for the Long-term Archiving
PIN	Personal Identification Number
RAID	Redundant Array of Independent Disks - vícenásobné diskové pole nezávislých disků
SAN	Storage area network - dedikovaná (oddělená od LAN, WAN) datová síť
SAS	Serial Attached SCSI - sériová sběrnice, která nahrazuje paralelní SCSI sběrnici a slouží k připojení pevných disků a páskových jednotek
SHA-2	kryptografická hašovací funkce
SOAP	Simple Object Access Protocol - protokol pro výměnu zpráv založených na XML přes síť, hlavně pomocí HTTP
SW	software
TSA	Time Stamp Authority
VRA	Veřejná registrační autorita
XML	Extensible Markup Language - obecný značkovací jazyk
ZFO	formát elektronického formuláře

12 PŘÍLOHY

Seznam příloh:

Příloha č. 1 - Základní právní předpisy upravující komunikaci prostřednictvím datových schránek a úkony s tím související

Příloha č. 2 - Přípustné formáty datové zprávy dodávané do datové schránky

Příloha č. 3 - „Kernun – Bezpečná schránka“ zaručuje zabezpečený přístup do datové schránky na základě principu

Příloha č. 4 - Kontrola platnosti elektronického podpisu

Příloha č. 5 - Příklad odeslané datové zprávy zobrazené pomoci aplikace 602XML Filler

Příloha č. 6 - Přehled počtu zásilek na KrÚ JMK a jeho možný vývoj do konce roku 2010

Příloha č. 1:

Základní právní předpisy upravující komunikaci prostřednictvím datových schránek a úkony s tím související

- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění zákona č. 190/2009 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů
- zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
- nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů
- vyhláška č. 496/2004 Sb., o elektronických podatelnách
- vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby (dále jen „spisová vyhláška“)
- vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů
- vyhláška č. 194/2009 Sb., o stanovení podrobností užívání informačního systému datových schránek

Uvedené právní předpisy přinášejí zásadní změny v komunikaci mezi orgány veřejné moci a adresáty veřejné správy a v oblasti nakládání s dokumenty v rámci orgánů veřejné moci.

Příloha č. 2:

Přípustné formáty datové zprávy dodávané do datové schránky:

a) **pdf** (Portable Document Format)
b) **PDF/A** (Portable Document Format for the Long-term Archiving)
c) **xml** (Extensible Markup Language Document)
d) **fo/zfo** (602XML Filler dokument)
e) **html/htm** (Hypertext Markup Language Document)
f) **odt** (Open Document Text)
g) **ods** (Open Document Spreadsheet)
h) **odp** (Open Document Presentation)
i) **txt** (prostý text)
j) **rtf** (Rich Text Format)
k) **doc** (MS Word Document)
l) **xls** (MS Excel Spreadsheet)
m) **ppt** (MS PowerPoint Presentation)
n) **jpg/jpeg/jfif** (Joint Photographic Experts Group File Interchange Format)
o) **png** (Portable Network Graphics)
p) **tiff** (Tagged Image File Format)
q) **gif** (Graphics Interchange Format)
r) **mpeg1/mpeg2** (Moving Picture Experts Group Phase 1/Phase 2)
s) **wav** (Waveform Audio Format)
t) **mp2/mp3** (MPEG-1 Audio Layer 2/Layer 3)
u) **isdoc/isdocx** (Information System Document) verze 5.2 a vyšší

Příloha č. 3:

„Kernun – Bezpečná schránka“ zaručuje zabezpečený přístup do datové schránky na základě principu:

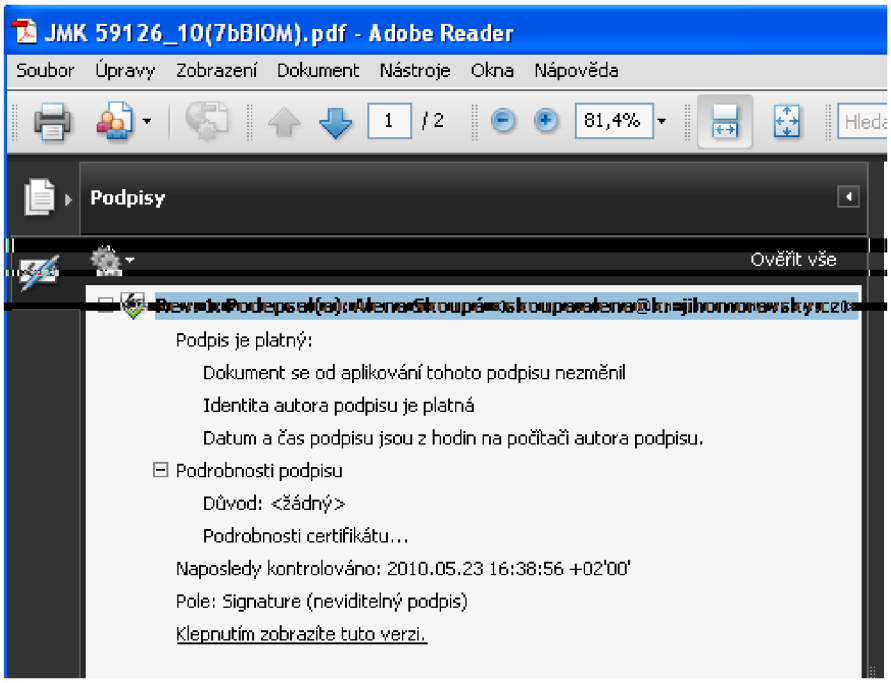
- **Ochrany hesel** - skutečné heslo se zadává pouze při prvním přihlášení k datové schránce. Při dalších přihlášeních se již využívá odlišné heslo. Hesla uložená v bezpečné schránce jsou chráněna pomocí kryptografických metod. Při použití Bezpečné schránky se není třeba obávat odcizení hesla pomocí škodlivého kódu nainstalovaného na počítači, protože nové heslo používané s Bezpečnou schránkou nebude použitelné mimo interní síť.
- **Ochrany relací** - pokud se podaří útočníkovi napadnout internetový prohlížeč a ukrást relaci k datovým schránkám, může se vydávat za uživatele, aniž by znal jeho heslo. Pro převzetí obsluhy nad datovou schránkou oběti mu postačí odcizený identifikátor relace. Kernun Bezpečná schránka chrání data přenášená do datových schránek tím, že přenáší pouze část relace, která je útočníkovi bez znalosti druhé části k ničemu.
- **Šifrování spojení** - spojení mezi datovou schránkou, uživatelem a bezpečnou schránkou je chráněno šifrováním pomocí protokolu HTTPS, stejně jako například u internetového bankovnictví. Bezpečná schránka se sama postará o kontrolu platnosti digitálního certifikátu datových schránek a neumožní tak vstup na podvrženou stránku připravenou útočníkem.
- **Ochrany proti přesměrování** - přístup k datové schránce je chráněn také proti přesměrování na falešné webové stránky potenciálního útočníka. K tomu může dojít při napadení služby DNS poskytovatele připojení k Internetu, tzv. DNS cache poisoning útokem. Bezpečná schránka se postará o správné nasměrování na skutečné servery datových schránek pomocí důvěryhodných kořenových DNS serverů. (14)

Příloha č. 4:

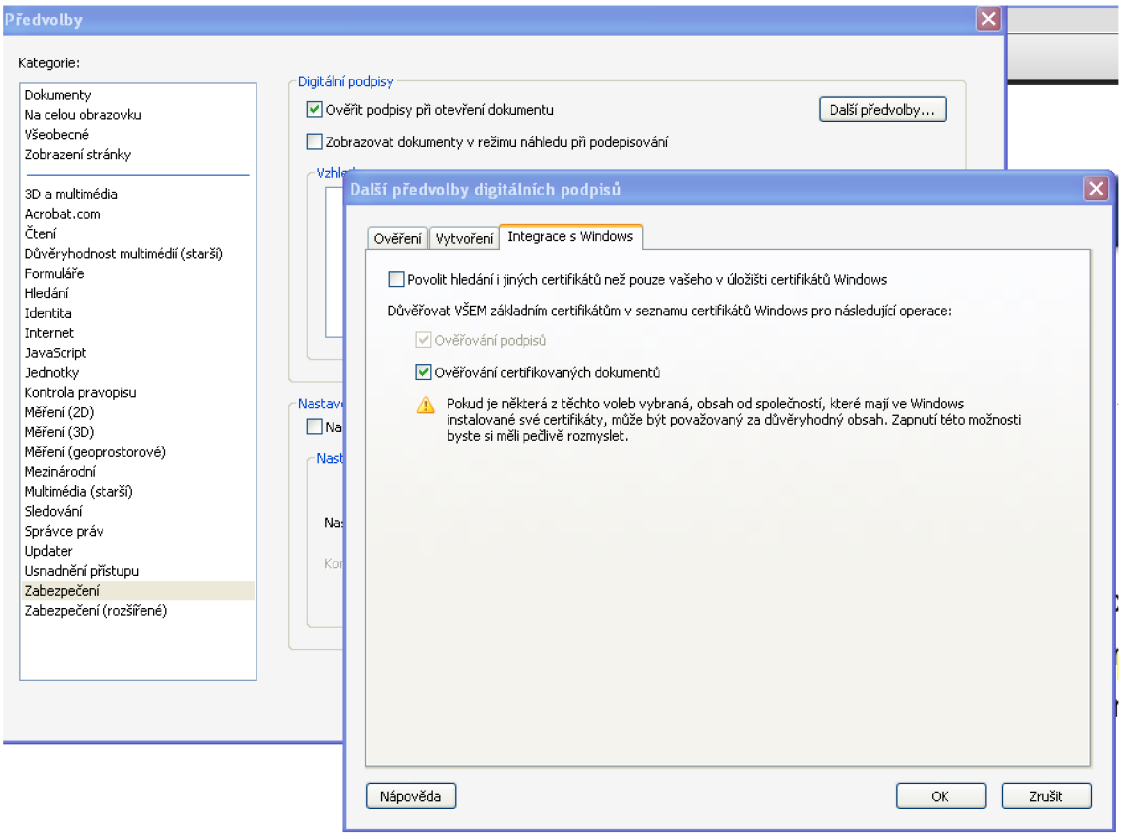
Kontrola platnosti elektronického podpisu

V prostředí programu **Adobe Reader** lze kontrolu platnosti elektronického podpisu provést ze záložky „Podpisy“, kde se daný podpis zobrazí (viz obr. 3) a následně zvolit tlačítko „Ověřit vše“. Pokud kontrola na platnost podpisu proběhne korektně, podpis se označí zeleným zatržítkem. Bližší informace o podpisu, včetně jeho sériového čísla lze získat kliknutím na volbu „Podrobnosti certifikátu“.

Nutnou podmínkou pro úspěšné provedení kontroly je, aby Adobe Reader **obsahoval kořenové certifikáty CA**. To lze provést vložením certifikátů do aplikace, nebo změnou nastavení, konkrétně povolit integraci kořenových certifikátů ze systému Windows do Adobe Reader pomoci záložky „integrace s Windows“ (viz obr. 4).



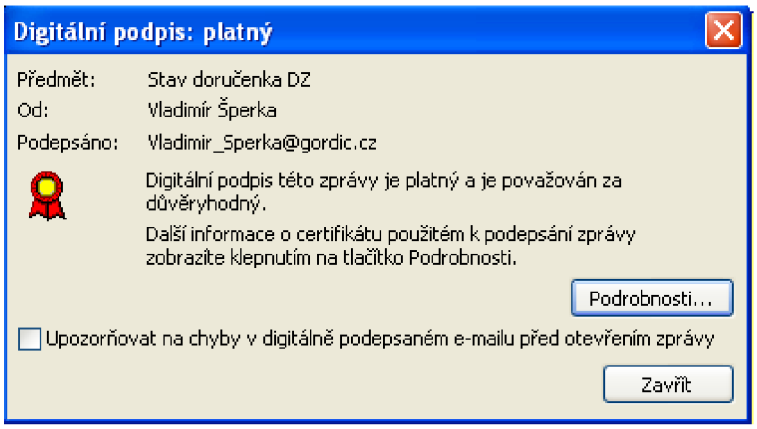
Obr. 7 – Adobe Reader - informační záložka o elektronickém podpisu, zdroj: KrÚ JMK



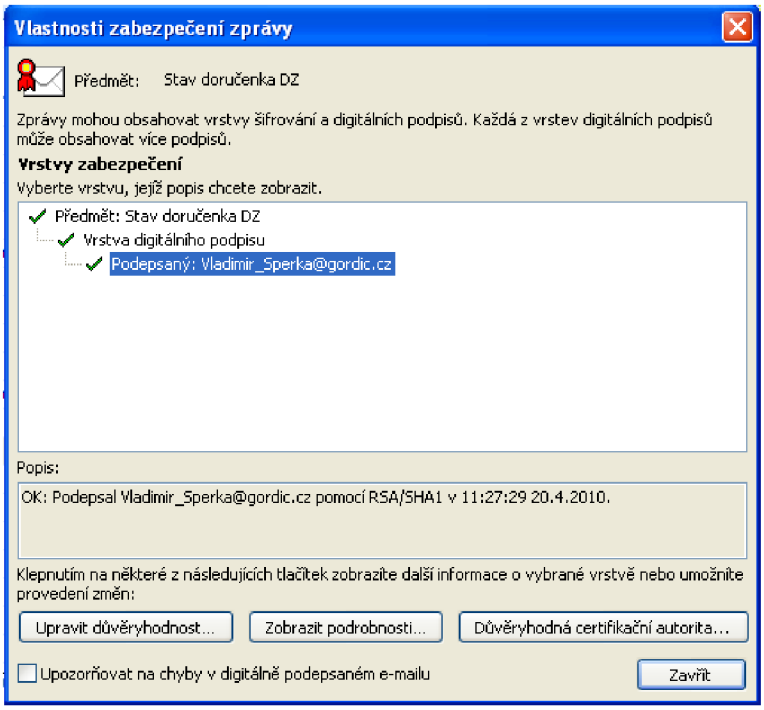
Obr. 8 – Adobe Reader – integrace kořenových certifikátů, zdroj: KrÚ JMK

V prostředí programu **602XML Filler** lze kontrolu certifikátu provést ze záložky „Vlastnosti“. Datové zprávy jsou přímo systémem opatřovány datovou značkou a časovým razítkem. Obojí je k prohlédnutí pomocí ikony „Zabezpečení“ Pro příjemce a pro případnou autorizovanou konverzi dokumentu do listinné podoby (přes kontaktní místo CzechPOINT) je ale podstatný elektronický podpis na samotném dokumentu, tj. příloze DZ.

V prostředí programu **MS Outlook** lze kontrolu provést kliknutím na ikonu se značkou pečeti , která otevře informační okno o platnosti podpisu (viz obr. 5), případně je možné zvolit další „Podrobnosti“ (viz obr. 6).



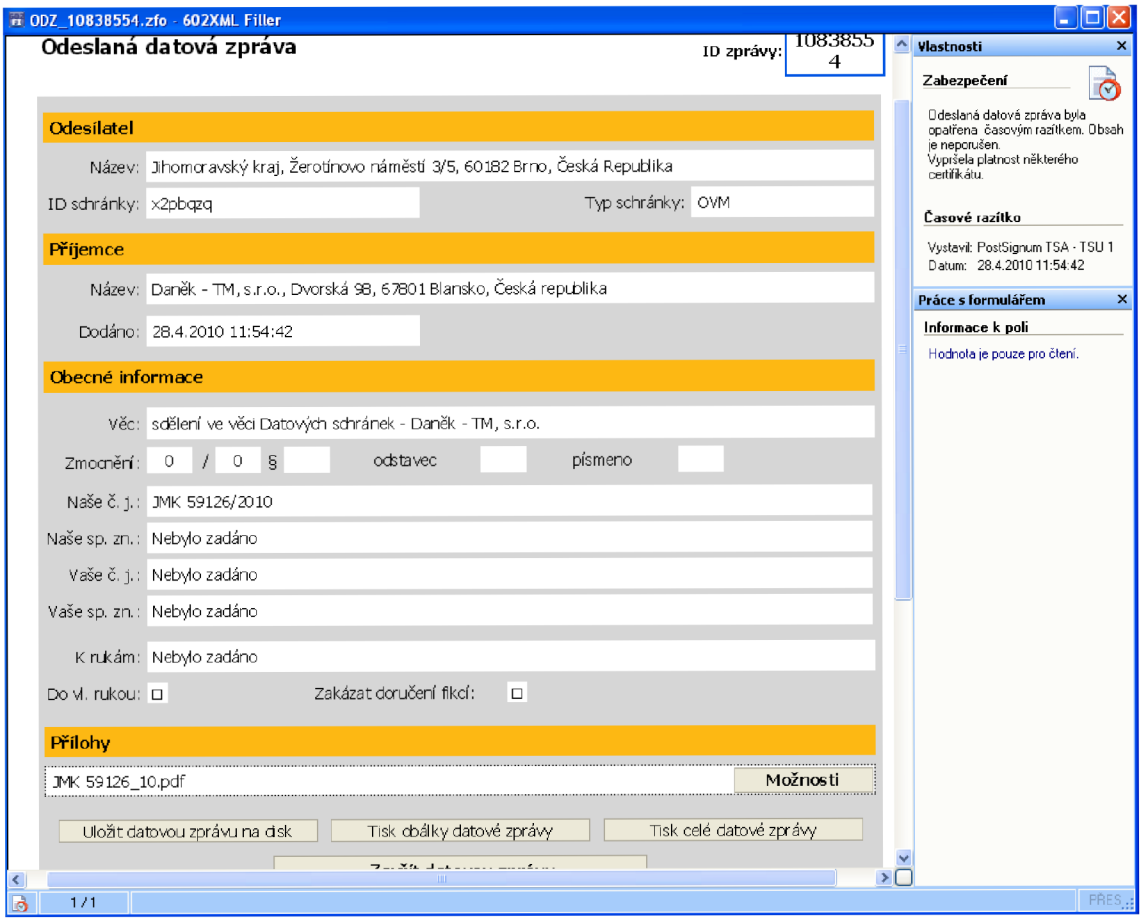
Obr. 9 – Informační okno o platnosti elektronického podpisu, zdroj: KrÚ JMK



Obr. 10 – Informační okno – vlastnosti zabezpečené zprávy, zdroj: KrÚ JMK

Příloha č. 5:

Příklad odeslané datové zprávy zobrazené pomoci aplikace 602XML Filler



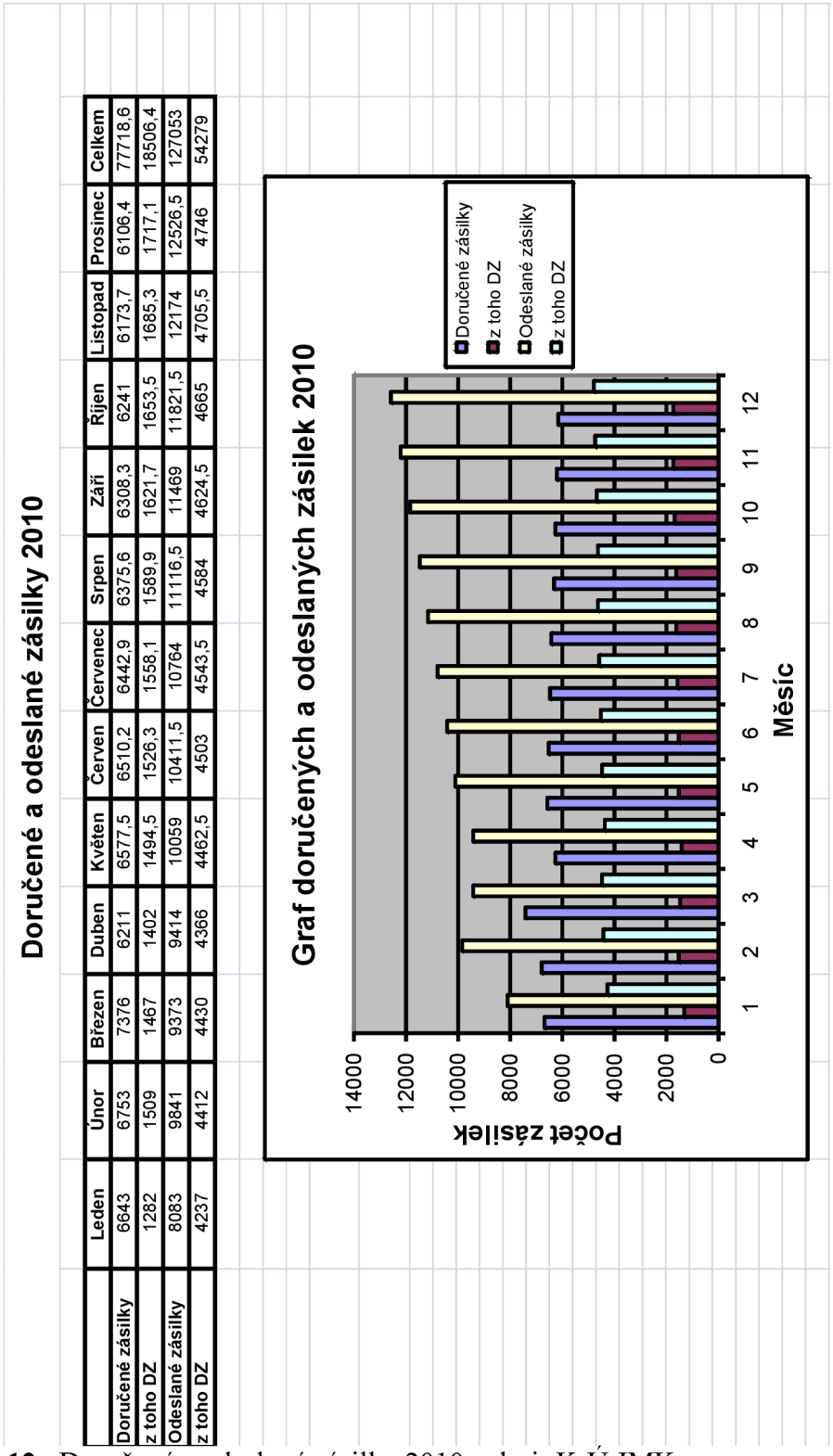
Obr. 11 – Náhled odeslané datové zprávy, zdroj: KrÚ JMK

Příloha č. 6:

Přehled počtu zásilek na KrÚ JMK a jeho možný vývoj do konce roku 2010

Doručené a odeslané zásilky 2010

	Leden	Únor	Březen	Duben	Květen	Červen	Červenec	Srpen	Září	Říjen	Listopad	Prosinec	Celkem
Doručené zásilky	6643	6753	7376	6211	6577,5	6510,2	6442,9	6375,6	6308,3	6241	6173,7	6106,4	77718,6
z toho DZ	1282	1509	1467	1402	1494,5	1526,3	1558,1	1589,9	1621,7	1653,5	1685,3	1717,1	18506,4
Odeslané zásilky	8083	9841	9373	9414	10059	10411,5	10764	111116,5	11469	11821,5	12174	12526,5	127053
z toho DZ	4237	4412	4430	4366	4462,5	4503	4543,5	4584	4624,5	4665	4705,5	4746	54279



Obr. 12 –Doručené a odeslané zásilky 2010, zdroj: KrÚ JMK

13 REJSTŘÍK