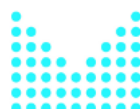




Informační systém datových schránek II.



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

**PODPORUJEME
VAŠI BUDOUCNOST**
www.esfcr.cz

Rozsah:

16 hodin

Anotace:

V tomto kurzu se seznámíme s Informačním systémem datových schránek, prací s datovými schránkami, detailně rozebranou teorií z oblasti datových schránek a aktuálními možnostmi v rámci Informačního systému datových schránek. Abychom vše správně pochopili a zařadili do souvislostí, budeme se z počátku zabývat aktuální legislativou.

Průvodce kurzem:

V první části kurzu si vysvětlíme používanou terminologii, vyspecifikujeme, co jsou a co nejsou datové schránky, jak fungují a kdo a jakým způsobem datové schránky používá.

Druhá část kurzu se zabývá praktickou prací s datovými schránkami. Získáte přehled o praktickém používání datové schránky orgánu veřejné moci společně s informacemi o propojení s elektronickou spisovou službou, datové schránky fyzické osoby a datové schránky právnické osoby.

Seznam modulů:

- ISDS II - Legislativa a obecné informace
- ISDS II - Praktické zkušenosti s užitím DS OVM, PO, FO

Přílohy ke kurzu:

- ISDS brožura základní informace
- Informace ke Správnímu řádu a ISDS
- Správní poplatky v ISVS
- Zákon č.300-2008
- Zákon č.301-2008
- Zákon č.365-2000
- Zákon č.499-2004
- Zákon č.500-2004
- Vyhláška č.193-2009
- Vyhláška č.194/2009

Obsah modulu ISDS II - Legislativa a obecné informace

1	Úvod.....	5
2	Definice pojmů a používaná terminologie	5
3	Legislativa.....	7
4	Druhy datových schránek	11
5	Statistické údaje ISDS.....	22
6	Datové schránky a Czech POINT	22
7	Archivace a dlouhodobé ukládání elektronických dokumentů	25
8	Spisová služba a její další rozvoj v souvislosti se zavedením datových schránek	27
9	Autorizovaná konverze dokumentů podle zákona 300/2008 Sb.....	28
10	Informační zdroje.....	31
11	Závěr.....	32

Obsah modulu ISDS II - Legislativa a obecné informace

1	Úvod.....	34
2	Praktická obsluha DS z pohledu úřadu, orgánu veřejné moci (OVM)	34
3	DS z pohledu Právnícké osoby.....	57
4	DS z pohledu FO a PFO.....	59
5	Závěr	61

MODUL: ISDS II - Legislativa a obecné informace

V tomto modulu se seznámíme s Informačním systémem datových schránek a s ním spojenou legislativou, kterou probereme v úvodu. Protože v minulosti docházelo k řadě změn v legislativní oblasti, je modul aktualizován v návaznosti na schválené legislativní dokumenty, především na novelizaci zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně dalších zákonů. Získáte také informace o obsahu prováděcích vyhlášek k zákonu č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Cílem tohoto modulu je uvést studenta do problematiky Informačního systému datových stránek v teoretické rovině tak, aby se v následném modulu bezproblémově orientoval v praktické obsluze systému.

1 Úvod



Projekt je spolufinancován z ESF z OP LZZ Vzdělávání úředníků a zaměstnanců veřejné správy, metodiků a školitelů a politiků v oblasti zavádění eGovernmentu do veřejné správy,

reg. č. CZ.1.04/4.1.00/38.00001

V této první části kurzu si vysvětlíme používanou terminologii, vyspecifikujeme, co jsou a co nejsou datové schránky, jak fungují a kdo a jakým způsobem datové schránky používá. Rovněž se seznámíme s aktuální legislativou.

2 Definice pojmů a používaná terminologie

eGovernment

Vládní pojetí (e-Česko 2006) - transformace vnitřních a vnějších vztahů veřejné správy pomocí moderních informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým zákazníkům. Totéž se očekává i od samosprávy.

Definice Evropské unie - využívání informačních a komunikačních technologií ve veřejné správě, které provází změna organizace a osvojení nových dovedností s cílem zlepšit služby veřejnosti, posílit demokratické procesy a podpořit veřejný zájem.

Autentizace - ověření totožnosti, že skutečně ten, kdo je identifikován, podepsal (*svědci, podpisový vzor, úředně ověřený podpis apod.*)

Identifikace - určení osoby, která učinila určitý úkon, tedy rozpoznání subjektu na základě identifikátorů, spojených s jeho osobou a může být znám dalším osobám (jméno, příjmení popř. rodné číslo apod.) Zjištění, kdo je pod zprávou podepsán.

Listina - písemnost zachycená na papírovém nosiči, tedy papírový dokument nebo doklad

Elektronický dokument (datová zpráva) - elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou (vznikne buď jako původní nebo převodem z listinné podoby)

Elektronický podpis - údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě. Za elektronický podpis se v širším významu považuje i prosté nešifrované uvedení identifikačních údajů (např. jména, IČ) na konci textu v elektronické podobě, které zaručuje identifikaci (tedy jednoznačné určení) označené osoby.

Zaručený elektronický podpis - údaje, které jsou připojeny k obsahu elektronického dokumentu a které jsou vytvořeny zvláštním postupem s využitím kryptografie - je jednoznačně spojen

s podepisující osobou, umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, byl vytvořen a připojen k datové zprávě pomocí prostředků, které má podepisující osoba výhradně pod svojí kontrolou, je ke zprávě připojen takovým způsobem, že lze zjistit jakoukoliv následnou změnu zprávy.

Komerční certifikát - ověření totožnosti uživatele při přihlašování do uzavřeného systému.

Kvalifikovaný certifikát - má náležitosti uvedené zákonem o elektronickém podpisu a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky stanovené zákonem pro poskytovatele certifikačních služeb vydávajících kvalifikované certifikáty.

Elektronická značka - je technicky (nikoliv právně) elektronický podpis, který byl vytvořen technickým zařízením - je jednoznačně spojena s označující osobou a umožňuje její identifikaci prostřednictvím kvalifikovaného systémového certifikátu, byla vytvořena a připojena k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou, je k datové zprávě, ke které se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Kvalifikované časové razítko - je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem (*náležitosti časového razítka viz §12b zákona o elektronickém podpisu*).

Elektronická veřejná listina - je veřejná listina vydaná soudy ČR nebo jinými státními orgány v mezích jejich pravomoci, popř. listina, kterou zvláštní právní předpis prohlašuje za veřejnou a k její verifikaci je použit zaručený elektronický podpis na bázi kvalifikovaného certifikátu nebo elektronická značka na bázi kvalifikovaného systémového certifikátu (*podrobněji o veřejných listinách viz Občanský řád soudní*).

Orgány veřejné moci (OVM) - zejména státní orgány a instituce, vč. orgánů státní správy, orgány územních samosprávných celků, územní samosprávné celky, veškeré státní fondy České republiky, zejména včetně Pozemkového fondu České republiky, zdravotní pojišťovny, Český rozhlas, Česká televize, všechny samosprávné komory zřízené zákonem, notáři a soudní exekutoři, soudy, všechny složky Policie České republiky a Armády České republiky, všechny organizační složky státu a jiných veřejnoprávních korporací, veřejnoprávní korporace a všechny státní příspěvkové organizace.

2.1 Používané zkratky

V kurzu budeme používat zkratky, proto si vysvětlíme jejich význam.

DS - datová schránka

ISDS - Informační systém datových schránek

KIVS - komunikační infrastruktura veřejné správy

MV ČR - Ministerstvo vnitra České republiky

ORP - obec s rozšířenou působností

OVM - orgán veřejné moci

SpS - spisová služba

ESS - elektronická spisová služba

ÚOOÚ - Úřad pro ochranu osobních údajů

TC - technologické centrum

OSVČ - osoba samostatně výdělečně činná

PO - právnická osoba

FO - fyzická osoba

PFO - podnikající fyzická osoba

DT - datový trezor

PDS - poštovní datová zpráva

3 Legislativa

Základními legislativními dokumenty, které upravují problematiku informačního systému datových schránek, jsou:

- **zákon č. 300/2008 Sb.**, o elektronických úkonech a autorizované konverzi dokumentu
- **zákon č. 301/2008 Sb.**, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentu

Další související právní předpisy, které upravují oblast elektronizace veřejné správy, jsou:

- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a změně dalších zákonů
- zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně dalších zákonů
- vyhláška o stanovení podrobností užívání a provozování informačního systému datových schránek (č.194/2009)
- vyhláška o stanovení podrobností provádění autorizované konverze dokumentů (č.193/2009)
- vyhláška o podrobnostech výkonu spisové služby (č. 191/2009)
- národní standard pro elektronické systémy spisové služby

3.1 Zákon o eGovernmentu

Strategie aneb eGON ožívá

eGON – personifikovaný zákon o eGovernmentu, představovaný jako organismus, který je schopen existovat pouze tehdy, spojí-li se všechny jeho potřebné orgány a funkce dohromady.

Oživení eGONa umožnil **Zákon o eGovernmentu**, tedy zákon o elektronických úkonech a autorizované konverzi dokumentů č. 300/2008 Sb., který vstoupil v účinnost **1. července 2009**

Zákon o eGovernmentu zavádí

- Povinnou formu elektronické komunikace mezi orgány veřejné moci prostřednictvím datových schránek
- Povinnou formu elektronického doručování dokumentů orgánů veřejné moci fyzickým a právnickým osobám, které mají zřízenu a zpřístupněnu datovou schránku
- Dobrovolnou formu činění úkonů fyzických a právnických osob, které mají zřízenu a zpřístupněnu datovou schránku vůči orgánům veřejné moci
- Autorizovanou konverzi dokumentů

Východiskem pro vznik zákona o eGovernmentu je digitalizace dokumentů. Digitalizace přináší řadu problémů, které je třeba řešit, např.

- Chybné, nebo nejasné chápání takových pojmů jako je listina, písemnost, dokument apod.
- Technologicky závislá legislativa – tzn. použití takových pojmů v zákoně, které nelze rozšířit ani výkladem, př. kniha opiátů, znalecký deník apod.
- Přílohy, které nelze v elektronické podobě doručovat (od předmětů doličných až po výkresy velkých rozměrů)
- Negativní přístup k zákonu o archivnictví a spisové službě
- Obecná touha lidstva mít v ruce papír, tedy pocit, že mám nad procesem (byť fiktivní) kontrolu

Základní pojmy, které je třeba znát pro správné uchopení zákona o eGovernmentu:

Dokument (dříve písemnost)

- je každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či digitální, který vznikl z činnosti původce dokument
- je jakýkoliv objekt obsahující zaznamenané informace, které lze zpřístupnit jiné osobě
- nemusí být pouze na papíře

Listina (= listinná podoba dokumentu) je písemnost zachycena na papírovém nosiči, tedy papírový dokument nebo doklad

Datová zpráva (= elektronická podoba dokumentu) je písemnost zachycená na nosiči, který umožňuje provést záznam elektronicky, optoelektronicky nebo jiným obdobným způsobem; jde o elektronický dokument (dokument vznikne buď jako původní nebo převodem z listinné podoby)

KAŽDÁ LISTINA JE DOKUMENTEM, ALE NE KAŽDÝ DOKUMENT JE LISTINOU

3.2 Vyhlášky

Vyhláška o stanovení podrobností užívání a provozování informačního systému datových schránek (194/2009)

- přístupové údaje do datové schránky (uživatelské jméno a bezpečnostní heslo)
- elektronické prostředky pro přihlášení do datové schránky (webové rozhraní, spisová služba)
- technické podmínky a bezpečnostní zásady pro přístup do datové schránky (vyšší zabezpečení - komerční certifikát na tokenu)

- způsob tvorby identifikátoru datové schránky (není to žádný ze stávajících identifikátorů – IČ, DIČ, RČ, ...)

Vyhláška o stanovení podrobností provádění autorizované konverze dokumentů (193/2009)

- technické náležitosti provádění autorizované konverze dokumentu (konverze)
- technické náležitosti dokumentu, který provedením konverze vznikl (výstup)
- technické náležitosti dokumentu, jehož provedením výstup při konverzi vznikl (vstup)
- vzor osvědčení o vykonání zkoušky zaměstnance provádějícího konverzi na žádost
- výstupní datové formáty

Vyhláška o podrobnostech výkonu spisové služby (191/2009)

- příjem dokumentu
- označování a evidence dokumentu
- číslo jednacích a tvorba spisu
- rozdělování, oběh a vyřizování dokumentu
- spisový znak, skartační znak a skartační lhůta, skartační řízení
- výstupní datové formáty

Národní standard pro elektronické systémy spisové služby

- přehled požadavků na elektronické spisové systémy pro vedení spisové služby
- spisový plán a organizace spisu
- kontrola a bezpečnost
- uchovávání a vyřazování (skartační operace)
- příjem dokumentu, atd....

3.3 Vazba na Správní řád

Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů a zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů se dotýkají zejména ve dvou oblastech:

- doručování dokumentu
- vydávání rozhodnutí v elektronické podobě

Doručování dokumentu mezi orgány veřejné moci navzájem:

- se řídí §17 odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu

Umožňuje-li to povaha dokumentu, orgán veřejné moci jej doručuje jinému orgánu veřejné moci prostřednictvím datové schránky, pokud se nedoručuje na místě. Umožňuje-li to povaha dokumentu a má-li fyzická osoba, podnikající fyzická osoba nebo právnická osoba zpřístupněnu svou datovou schránku, orgán veřejné moci doručuje dokument této osobě prostřednictvím datové schránky, pokud se nedoručuje veřejnou vyhláškou nebo na místě. Doručuje-li se způsobem podle tohoto zákona, ustanovení jiných právních předpisů upravující způsob doručení se nepoužijí.

Doručování dokumentu orgány veřejné moci jiným subjektům:

se podle §17 odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu uskuteční, pokud

- to umožňuje povaha dokumentu
- se nedoručuje na místě (při provádění úkonu) nebo veřejnou vyhláškou
- má adresát zpřístupněnou datovou schránku

Provádění úkonů jiných subjektů vůči orgánům veřejné moci:

se řídí §18 odst. 1 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu

Fyzická osoba, podnikající fyzická osoba a právnická osoba může provádět úkon vůči orgánu veřejné moci, má-li zpřístupněnu svou datovou schránku a umožňuje-li to povaha tohoto úkonu, prostřednictvím datové schránky.

Jiné subjekty provádí úkony vůči orgánům veřejné moci pokud:

- to umožňuje povaha dokumentu
- subjekt má zpřístupněnou datovou schránku
- subjekt chce využít systém datových schránek

Vydávání správního rozhodnutí v elektronické podobě:

§ 69 odst. 3 zákona č. 500/2004, Správní řád

(Pokud se na žádost účastníka má rozhodnutí doručit elektronicky, vyhotoví úřední osoba, která za písemné vyhotovení rozhodnutí odpovídá, jeho elektronickou verzi s tím, že na místě otisku úředního razítka vyjádří tuto skutečnost slovy "otisk úředního razítka" a dokument podepíše svým zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném)

Postup pro vydání elektronické podoby rozhodnutí:

- rozhodnutí je schváleno a podepsáno oprávněnou úřední osobou (např. pomocí vnitřní certifikační autority)
- osoba odpovědná za písemné vyhotovení rozhodnutí podepíše svým zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb
- rozhodnutí je vloženo do datové schránky příjemce

3.3.1 Co se pomocí datové schránky nedoručuje

Pomocí datové schránky se nedoručuje

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

3.4 Zákon č. 300/2008 po zkušenostech z praxe

- 10 let eGovernmentu v ČR (respektive 18 let, první kroky byly učiněny v roce 1992)
- ČR je jedinou zemí na světě, která má eGovernment v tak širokém rozsahu
- Po spuštění ISDS se nekonalo jeho zhroucení
- Do současnosti nebyly v ISDS odhaleny podvodné zprávy a spamy
- Byl pročištěn obchodní rejstřík, došlo zejména k:
 - odhalení nefunkčních společností
 - aktualizaci údajů o společnostech
 - zjednodušení způsobu jednání za společnost

3.4.1 Naplnění cílů

Následujícími informacemi zjistíme, zda byly naplněny předem vytyčené cíle:

- Povinná forma komunikace: **ANO**
- Povinné doručování DS OVM, PO, FO, PFO, které mají zřízenu a zpřístupněnu DS: **ANO**
- Dobrovolné doručování FO a PO: **ANO** (ale ISDS dokáže vyhledat v adresáři pouze ten subjekt u kterého je zadán přesný název ve vyhledávači)
- Vzájemná komunikace mezi FO a PO: **NE** (od 1. 1. 2010 bylo dodáno pouze 480 DZ tímto způsobem)
- Autorizovaná konverze dokumentů: **ANO** (přetrvává problém s geometrickými plány, kterých je mnoho. Dala by se tímto způsobem řešit veškerá stavební řízení).

4 Druhy datových schránek

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

Kdo je orgánem veřejné moci si můžeme ověřit na <http://www.datoveschranky.info/ovm.php>

4.1 Typy datových schránek podle zřízení

Následující schéma uvádí, jak se od sebe jednotlivé typy DS liší z pohledu jejich zřízení.



4.1.1 Funkce, které datová schránka plní

Pomocí datové schránky můžeme:

- odesílat zprávy
- přijímat zprávy
- zjišťovat stavy odeslaných zpráv
- přijímat doklady o dodání a doručení
- ověřovat, zda adresát má datovou schránku
- pracovat s elektronickými formuláři
- dlouhodobě uchovávat zprávy pomocí DT - jedná se o komerční funkcionalitu poskytovanou Českou poštou, s. p.

4.1.2 DS jako úložiště

- DS není koncipována jako e-mail! Jedná se o krátkodobé (90 denní) úložiště zpráv.
- DS vysoce přesahují obvyklé stávající bezpečnostní protokoly pro přenos zpráv. Máme na mysli zejména http, POP3 a další...

4.2 Doručování do DS

Doručování přes informační systém datových schránek bylo primárně zamýšleno pro zásilky určené doručením do vlastních rukou, kdy nelze doručit jinými způsoby.

Do budoucna by neměl existovat důvod, aby přes systém datových schránek bylo automaticky doručováno i za předpokladu, kdy je náhradní doručení vyloučeno. Jedná se například o platební rozkazy.

4.2.1 Doručování do DS

Časová osa odeslání až smazání datové zprávy

Datová zpráva je doručena okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na svá oprávnění přístup k dodanému dokumentu



Časová osa fikce doručení

Jestliže se oprávněná osoba nepřihlásí ve lhůtě 10 dnů do datové schránky, je dokument doručen posledním dnem této lhůty. Pokud jiný právní předpis vylučuje náhradní doručení, NENÍ možno doručit fikcí.



4.2.2 Doručení datové zprávy

Dokument dodaný do datové schránky je doručen:

- okamžikem, kdy se do datové schránky přihlásí osoba mající dle svého oprávnění přístup k dodanému dokumentu
- nepřihlásí-li se do datové schránky oprávněná osoba ve lhůtě 10 dnů ode dne dodání do datové schránky, považuje se dokument za doručený posledním dnem této lhůty (fikce doručení)

4.2.3 motně právní úkony účastníků

OSŘ umožňuje provádět procesní úkony účastníků řízení vůči soudům přes ISDS

OSŘ umožňuje i hmotně právní úkony, například žádat vymáhání pohledávky nebo výpověď z bytu. Z pohledu podpisu stačí, že byla z DS osoby s přístupovými právy taková žaloba zaslána.

V případě hmotně právních úkonů musí mít tyto úkony náležitosti platné i pro povinnost použití podpisu v hmotně právních žalobách.

Za oprávněnost nároku vůči žalovanému ručí soud, nikoli podavatel žaloby.

4.2.4 Hmotně právní účinky doručení do DS

Poprvé v historii doručování je sjednocena jeho právní úprava ve veřejné správě a resortu justice.

§17 – procesní doručování ve veřejném právu se týká oblasti:

- zasílání písemností od OVM směrem k PO, FO, PFO
- součinnosti OVM navzájem

§18 – řeší provádění úkonů PO, FO, PFO vůči OVM

4.2.5 Soukromoprávní účinky doručení

Soukromoprávní účinky doručení s významem pro hmotné právo:

- podání návrhu
- přijetí návrhu
- jednostranné úkony (výpověď, odstoupení od smlouvy, ...)

Okamžikem doručení v soukromoprávním styku přes DS je: §18a odstavec 2. Na tento dokument se nevztahuje §17 odst. 3 a 4 (fikce doručení).

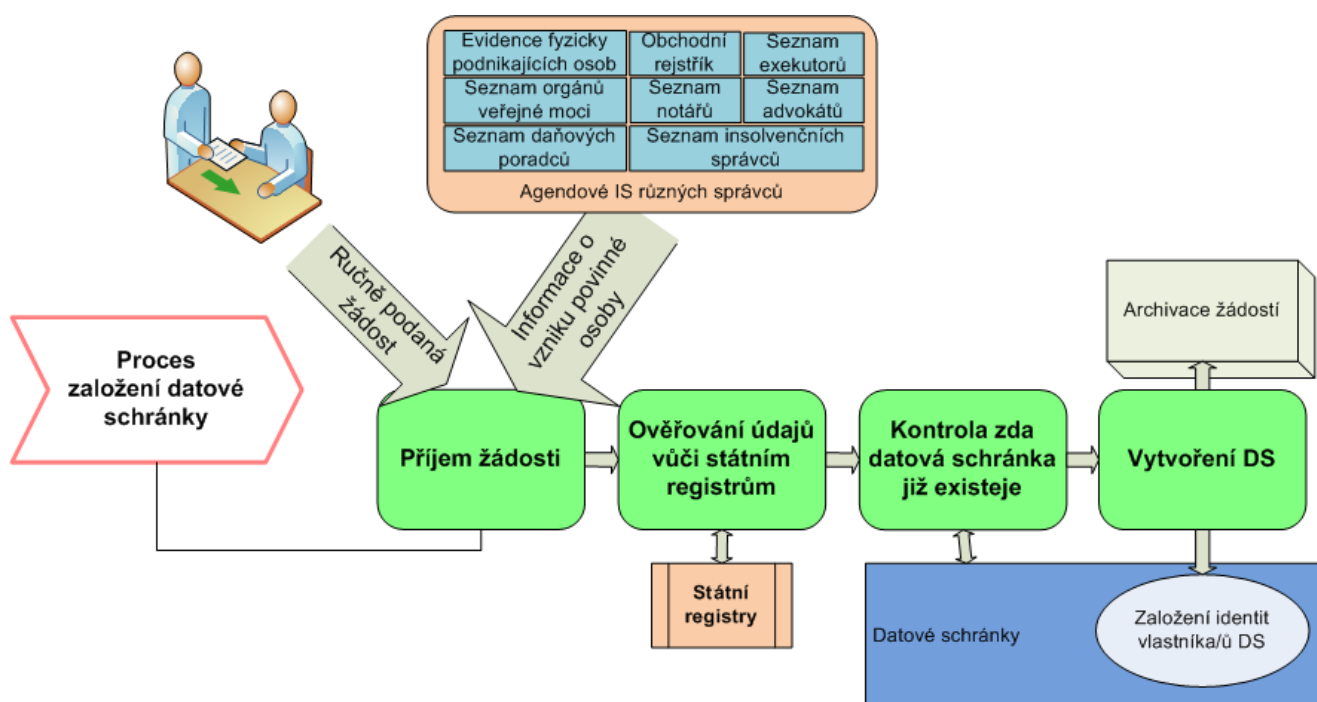
4.3 Zřízení datové schránky

Orgánům veřejné moci, právníkům osobám zapsaným v obchodním rejstříku a právníkům osobám zřízeným ze zákona je Datová schránka zřizována automaticky ze zákona. O zřízení datové schránky mohou správce požádat fyzické osoby, podnikající fyzické osoby a právníké osoby nezapsané v obchodním rejstříku.

Náležitosti žádosti definuje zákon v §3 odst. 3 a 4 (fyzické osoby), §4 odst. 4 a 5 (podnikající fyzické osoby) a §5 odst. 4 a 5 (právníké osoby nezapsané v obchodním rejstříku).

Po zřízení datové schránky ze zákona obdrží vedoucí orgánu, resp. statutární zástupce zásilku do vlastních rukou, která obsahuje přístupové údaje a návod k používání.

Fyzické osoby a ostatní subjekty si mohou o zřízení datové schránky požádat od 1. 7. 2009 na kontaktním místě Czech POINT nebo na MV ČR.



4.3.1 Způsoby žádosti o zřízení datové schránky

Žádost o zřízení Datové schránky lze podat následujícími způsoby:

- Na kontaktním místě veřejné správy (pracoviště Czech POINT). V tomto případě není nutné žádost opatřovat úředně ověřeným podpisem (viz §27 odst. 2).
- Vyplněním elektronického formuláře žádosti, jeho podepsáním zaručeným elektronickým podpisem a následným odesláním na e-podatelnu správce (posta@mvcz.cz). Formulář žádosti naleznete na webu www.datoveschranky.info.
- Vyplněním formuláře žádosti, jeho vytištěním, opatřením ověřeným podpisem a zasláním na poštovní adresu správce.

Pokud žádost obsahuje všechny zákonné náležitosti a zároveň (v případě FO a PFO) byla osoba žadatele jednoznačně identifikována v databázi evidence obyvatel, správce zřídí datovou schránku do

3 pracovních dnů od přijetí žádosti. Přístupové údaje jsou následně žadateli zaslány poštovní zásilkou do vlastních rukou.

V případě žádosti o zřízení datové schránky právnické osoby nezapsané v obchodním rejstříku, je nutné, aby bylo doloženo, že žadatel je oprávněn za tuto právnickou osobu jednat. Tento doklad není správcem vyžadován, pokud je osoba žadatele uvedena ve veřejném rejstříku dostupném dálkově (např. RES, ARES apod.).

V opačném případě vyzve správce žadatele k zaslání kompletně vyplněné žádosti, případně k doplnění údajů.

4.3.2 Zřízení další datové schránky OVM dle § 6 zákona

Žádost o zřízení další datové schránky organizace se statutem OVM lze podat následujícími způsoby:

- a) Na kontaktním místě veřejné správy (pracoviště Czech POINT).
- b) Odesláním žádosti na e-podatelnu správce (posta@mvcz.cz)
- c) Odesláním žádosti na poštovní adresu správce.
- d) Odesláním žádosti do datové schránky správce.

Ve všech výše uvedených případech platí, že k podání žádosti je oprávněna osoba, která je k primární datové schránce vedena v roli oprávněné osoby nebo administrátora.

Pro zřízení další datové schránky je kromě podání žádosti správci nutné též zadat následujícím způsobem všechny vyžadované údaje:

- a) Pokud organizace žadatele spadá do oblasti územní samosprávy (obce, kraje apod.), garant dat se přihlásí na portále <https://www.epusa.cz>. V prostředí tohoto portálu zadá sadu povinných údajů. Pokud žadatel nedisponuje přihlašovacími údaji pro portál ePusa, kontaktuje helpdesk na emailové adrese help@epusa.cz.
- b) Pokud organizace žadatele je jiný typ OVM než dle bodu a), garant dat se přihlásí na portále OVM <https://ovm.smartadministration.cz>. V prostředí tohoto portálu zadá sadu povinných údajů. Pokud žadatel nedisponuje přihlašovacími údaji pro portál OVM, kontaktuje helpdesk na emailové adrese ovm@smartadministration.cz.
- c) Postup dle bodu b) se vztahuje i na další datové schránky právnických osob či fyzických osob, kterým byl přiznán statut OVM dle §5a zákona č. 300/2008 Sb. Přístupové údaje jsou odeslány poštou na adresu sídla organizační složky do vlastních rukou osoby uvedené v žádosti.

4.3.3 Žádost o funkčnost schránky v režimu OVM dle §5a zákona

Vykonává-li fyzická nebo právnická osoba působnost v oblasti veřejné správy, ministerstvo jí na žádost umožní, aby její datová schránka plnila rovněž funkci datové schránky v režimu OVM.

Žádost lze podat následujícími způsoby:

- a) Na kontaktním místě veřejné správy (pracoviště Czech POINT).

- b) Odesláním žádosti na e-podatelnu správce (posta@mvcr.cz)
- c) Odesláním žádosti na poštovní adresu správce.
- d) Odesláním žádosti do datové schránky správce.

Nutnou náležitostí žádosti je doklad či prohlášení žadatele, osvědčující jakou působnost v oblasti veřejné správy subjekt vykonává.

4.3.4 Zpřístupnění datové schránky

Dle §10 odst. 2 je datová schránka zpřístupněna (aktivována) prvním přihlášením osoby uvedené v § 8 odst. 1 až 4 do datové schránky, nejpozději však patnáctým dnem po dni doručení přístupových údajů. Toto přihlášení je možné pouze prostřednictvím webového portálu datových schránek.

4.3.5 Znepřístupnění datové schránky

Subjekty, kterým byla datová schránka zřízena na žádost, mohou také požádat o její znepřístupnění. Žádost o znepřístupnění datové schránky lze podat následujícími způsoby:

- a) Na kontaktním místě veřejné správy (pracoviště Czech POINT). V tomto případě není nutné žádost opatřovat úředně ověřeným podpisem (viz §27 odst. 2).
- b) Odesláním žádosti podepsané zaručeným elektronickým podpisem na e-podatelnu správce (posta@mvcr.cz).
- c) Odesláním žádosti opatřené ověřeným podpisem na poštovní adresu správce.
- d) Odesláním žádosti do datové schránky správce.

Správce znepřístupní datovou schránku do 3 pracovních dnů od přijetí žádosti.

4.3.6 Zrušení datové schránky

Datovou schránku zruší správce 3 roky po zániku subjektu, pro který byla zřízena, viz §13. Záznamy o přenesených zprávách (obálky těchto zpráv bez příloh) uchovává ISDS trvale.

4.3.7 Žádost o povolení příjmu Poštovních datových zpráv

Žádost o umožnění dodávání datových zpráv dle §18a, odst. 1 zákona lze podat následujícími způsoby:

- a) Zaškrtnutím příslušné volby v prostředí administrativní části webového portálu ISDS . Po odeslání žádosti je dodávání poštovních datových zpráv povoleno ihned, bez dalšího schvalování správcem.
- b) Na kontaktním místě veřejné správy (pracoviště Czech POINT).

4.3.8 Žádost o ukončení povolení příjmu Poštovních datových zpráv

Žádost o ukončení povolení dodávání datových zpráv dle §18a, odst. 1 zákona lze podat následujícími způsoby:

- a) Zaškrtnutím příslušné volby v prostředí administrativní části webového portálu ISDS. Po odeslání žádosti je dodávání Poštovních datových zpráv ukončeno ihned, bez dalšího schvalování správcem.
- b) Na kontaktním místě veřejné správy (pracoviště Czech POINT).

4.3.9 Odesílání Poštovních datových zpráv

Odesílání datových zpráv je službou České pošty, s. p.

Zájemce o tuto službu musí kontaktovat Českou poštu, s. p., například pomocí klientské zóny na www.cpost.cz.

4.4 Přístupy do datové schránky

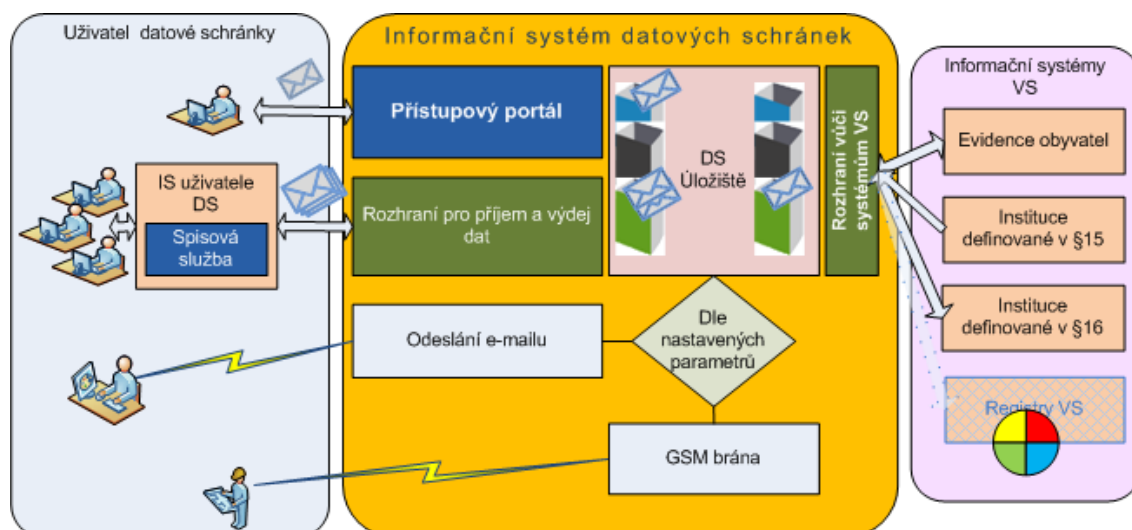
Při přístupu k datové schránce rozlišujeme několik rolí.

Oprávněná osoba je:

- Fyzická osoba
- Fyzická osoba podnikající (OSVČ)
- Statutární orgán
- Člen statutárního orgánu
- Vedoucí organizační složky
- Vedoucí orgánu veřejné moci

Administrátor je osoba, určená oprávněnou osobou

Pověřená osoba je osoba určená oprávněnou osobou nebo administrátorem



4.4.1 Přístupové údaje

Přístupové údaje pro oprávněné osoby datových schránek:

Subjektům, kterým správce vytvoří datové schránky, budou zaslány přístupové údaje poštou, a to do vlastních rukou oprávněné osoby adresáta.

Používání přístupových údajů:

Přístupové údaje vydané správcem při zřízení datové schránky i ve všech dalších případech jsou platné pouze pro určitý počet přihlášení. Jakmile nastane okamžik pro změnu uživatelského hesla, systém si takovou změnu vynutí, přičemž počet zbývajících přihlášení uživateli vždy oznámí. Pokud nedojde ke změně uživatelského hesla ani při posledním možném přihlášení, systém přístupové údaje zablokuje a nebude je možné znovu použít. Systém může kdykoliv, v závislosti na nastavení, omezit uživateli počet možných přihlášení s aktuálně používanými přístupovými údaji a znovu jej požádat o změnu přístupového hesla. Princip změny hesla je poté stejný, jako v případě použití prvních přístupových údajů.

Dojde-li k zablokování přístupových údajů, je jediným způsobem, jak znovu přistoupit do datové schránky, zažádat o jejich opětovné vydání na kontaktním místě veřejné správy nebo odeslat požadavek podepsaný elektronickým podpisem nebo notářsky ověřeným podpisem správci. V případě, že uživatel používá k přístupu do datové schránky jiný technický prostředek (aplikaci), zajistí systém ISDS, aby nedošlo k vyčerpání všech pokusů pro změnu hesla a uživatel tak mohl heslo změnit prostřednictvím webového rozhraní.

V hesle musí být obsaženo jedno velké a jedno malé písmeno a jedna číslice. Heslo nesmí být žádným z předchozích hesel.

4.4.2 Přístupové údaje pro FO a PFO

Fyzickým osobám a fyzickým osobám podnikajícím budou přístupové údaje zaslány na adresu, kterou uvedou v žádosti o zřízení datové schránky. Pokud adresu pro doručení nevyplní, použije se adresa získaná z evidence obyvatel.

Žadatel může zvolit pro doručení i zahraniční adresu, pokud se tato nachází v některé ze zemí, do kterých lze prostřednictvím provozovatele doručovat v režimu „do vlastních rukou“. Seznam těchto zemí je zveřejňován na informačním webu datových schránek.

4.4.3 Přístupové údaje pro OVM

Vedoucím orgánů veřejné moci budou přístupové údaje odeslány na adresu jejich úřadu.

4.4.4 Přístupové údaje pro PO

Statutárním zástupcům právnických osob budou přístupové údaje zaslány na adresu sídla společnosti. Pokud si adresát zásilku nepřebere, je na rozhodnutí správce, zda pošle nové přístupové údaje na adresu trvalého pobytu, tak jak je uvedena v obchodním rejstříku.

4.5 Rozhraní datových schránek

Pro přístup do datové schránky můžeme použít webového rozhraní nebo rozhraní spisových služeb. V obou případech musí být každý přístup autorizován oprávněnou osobou, administrátorem nebo pověřenou osobou.

Použití webového rozhraní je postačující pro jednotlivce a malé organizace. Je to jednoduchá aplikace dostupná přes internet a umožňuje odesílání a příjem datových zpráv.

Charakteristika webového portálu:

- slouží k využívání služeb ISDS fyzickými osobami, ale rovněž administrátory úřadů
- není třeba instalovat žádný software
- stačí jen běžný počítač, webový prohlížeč a přístup k internetu
- uživatel vybere formulář a adresáta, systém předvyplní potřebné údaje
- uživatel vloží zprávu (vlastní data), případně připojí přílohu
- zprávu bude možné i elektronicky podepsat
- bude možné prohlížet seznamy odeslaných zpráv, přijatých zpráv, historii včetně doručenek
- portál mohou využívat i úřady

Rozhraní spisových služeb umožní přímé propojení se spisovou službou či jinou aplikací.

Charakteristika rozhraní spisových služeb:

- MV ČR ve spolupráci s vybranými dodavateli spisových služeb připravilo jednotný standard komunikace.

19. 12. 2008 bylo podepsáno memorandum o spolupráci mezi Ministerstvem Vnitra ČR a zástupců výrobců elektronických spisových služeb <http://www.mvcr.cz/datove-schranky.aspx>.

Univerzální rozhraní datových schránek na bázi web services:

- slouží k využívání služeb ISDS spisovými službami
- je umožněno automatizovaně přijímat a odesílat zprávy včetně elektronicky podepsaných doručenek
- kromě odesílání a přijímání datových zpráv je možné stahovat seznamy odeslaných zpráv, přijatých zpráv, historii včetně doručenek
- odpadá nutnost listinné evidence, vše bude ve spisové službě, resp. podatelně
- spisová služba musí ovšem být na uvedené připravena

4.6 Povinnosti správce ISDS

Správce Informačního systému datových schránek:

- zajistí připojení kvalifikovaného časového razítka k odeslané datové zprávě
- dodá odesílanou datovou zprávu do datové schránky adresáta
- vyrozumí adresáta o dodání zprávy
- oznámí odesílateli, že
 - zpráva byla doručena (označenou elektronickou značkou)
 - datová schránka příjemce byla zpřístupněna, zrušena, neexistuje
- o těchto událostech vede bezpečnou evidenci

Z hlediska bezpečnosti garantuje:

dostupnost systému – 99,9%

integritu systému a dat – kryptografické komponenty

důvěrnost – provozovatel nemá přístup k datům

průkaznost – evidence veškerých událostí spojených s provozem

zálohování systému

omezení formátů příloh – zakázané *.exe a spustitelné soubory, komprimované

Autentifikace a autorizace uživatelů je stanovena vyhláškou MV ČR (možnost použití el. podpisu a certifikátů)

V oblasti auditu a dohledu zajišťuje:

- dohled 24 x 7 x 365
- pravidelné (plánované) bezpečnostní audity – každý rok
- atest jako ISVS
- dohled MV, ÚOOÚ (úřadu pro ochranu osobních údajů)

4.7 Harmonogram změn v datových schránkách

1. 7. 2009	-	31. 12. 2009	OVM	⇔	OVM, PO, FO, PFO
1. 1. 2010	-	30. 6. 2010	OVM, PO, FO, PFO	⇔	OVM, PO, FO, PFO
1. 7. 2010	-	X	OVM, PO, FO, PFO	⇔	OVM, PO, FO, PFO

5 Statistické údaje ISDS

Celkové počty v ČR:

- Počet obcí: 6249
- Počet OVM: 8227
- Kontaktní místa Czech POINT: 6255

Níže uváděná data jsou platná k 31. srpnu 2010

- 392 505 aktivních DS
- Denně je odesláno přes 100 000 DZ
- Do současnosti bylo datovými schránkami přeneseno více než 20 000 000 datových zpráv.
- 26. 11. 2009 byl ISDS přenesen první milion DZ

6 Datové schránky a Czech POINT

S Informačním systémem datových schránek spolupracují i kontaktní místa Czech POINT. Na kontaktním místě je možné zažádat o zřízení datové schránky nebo o autorizovanou konverzi dokumentu.

Ukažme si modelový příklad **žádosti o autorizovanou konverzi**.

1. Příjemce se přihlásí do své datové schránky, přečte si přijatou zprávu a z nabízených funkcionalit si vybere *Odeslat ke konverzi do listinné podoby*. Tím odešle přílohu do centrálního úložiště dokumentů.
2. Uživateli je vystaven lístek s kódem, pod kterým je dokument v úložišti uložen.
3. S lístkem si půjde uživatel na kterékoli pracoviště Czech POINT, kde mu na základě předloženého lístku provedou autorizovanou konverzi dokumentu.

Konverze je zpoplatněna částkou 30 Kč za každou načatou stránku A4.

6.1 Konverze dokumentů na pracovišti Czech POINT

Konverze z listinné podoby do elektronické (konverze na žádost)

Na pracovišti Czech POINT dokument převedou do elektronické podoby a dokument uloží a opatří ho:

- časovým razítkem
- podpisem úředníka
- ověřovací doložkou (doložka je uložena do centrální evidence)

Dokument je odeslán:

- do datové schránky občana, pokud ji má

- do úschovny elektronických dokumentů a občanovi předají vytištěné jednorázové přístupové údaje do úschovny, kde si přes web svůj dokument vyzvedne
- na CD nebo DVD

Konverze z elektronické podoby do listinné (konverze na žádost)

Občan na pracovišti Czech POINT předloží jednorázové přístupové údaje k úložišti, odkud si obsluha vyzvedne elektronickou zprávu a převede do listinné podoby, kterou si žadatel převezme.

Asistent kontaktního místa Czech POINT:

- provede kontrolu:
 - časového razítka
 - podpisu úředníka nebo elektronické značky úřadu
 - platnost podpisu nebo elektronické značky
- vygeneruje a vytiskne ověřovací doložku a jedinečný hash (údaje o konverzi), které se ukládají do centrální evidence ověřovacích doložek pro možnost ověření shody v centrální evidenci

Ověřovací doložka - konverze do elektronické podoby

Ověřovací doložka konverze z **listinné do elektronické podoby** je součástí výstupu a obsahuje:

- název subjektu, který konverzi provedl,
- pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí,
- údaj o věření toho, že obsah výstupu odpovídá obsahu vstupu,
- údaj o tom, z kolika listů se skládá vstup,
- údaj o tom, zda vstup obsahuje vodoznak, reliéfní tisk nebo embossing, suchou pečeť nebo reliéfní ražbu, opticky variabilní prvek nebo jiný zajišťovací prvek,
- datum vyhotovení ověřovací doložky,
- jméno, případně jména, a příjmení osoby, která konverzi provedla.

Ověřovací doložka - konverze do listinné podoby

Ověřovací doložka konverze **do dokumentu v listinné podobě** je součástí výstupu a obsahuje:

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


- datum a čas uvedené v kvalifikovaném časovém razítku, číslo kvalifikovaného časového razítka a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal,
- otisk úředního razítka, jméno, popřípadě jména, příjmení a podpis osoby, která konverzi provedla

Tyto údaje jsou v evidenci provedených konverzí uchovávány po dobu 10 let od provedení konverze.

6.2 Technické vybavení pracoviště Czech POINT

Technické vybavení pracoviště Czech POINT

1. PC – dvoujádrový procesor, min. 2 GB RAM, grafická karta
2. alespoň 2 připojitelné monitory (min. rozlišení 1280 x 1024, 1440 x 900)
3. pevný disk min. 160 GB
4. optická mechanika DVD±RW
5. integrovaná síťová karta min. 100 Mb/sec
6. USB 2.0, klávesnice, myš
7. multifunkční zařízení (barevná laserová tiskárna, RAM min. 128 MB, rozlišení tiskárny min. 600 x 600 dpi, rychlost tisku min. 8 str./min. černobíle, 4 str./min. barevně, skener s podavačem, rozlišení min. 600 x 600 dpi)
8. čtečka čipových karet
9. čtečka 2D kódu
10. Internetové připojení
11. certifikát elektronického podpisu, token.

	<p>Provozní řád Czech POINT stanoví postup při konverzi VD</p> <p>Pracoviště standardně provádí konverzi do velikosti A4 a počtu 50 stran</p> <p>Je možno provádět konverzi i větších formátů. Jedná se ale o individuální a nadstavbovou službu jednotlivých kontaktních míst</p>
---	---

6.3 Souhrn

ZÁKLADNÍ PŘEHLED – ROZDĚLENÍ KONVERZE

Podle účelu

1. Z moci úřední (OVM pro výkon své působnosti)
2. Na žádost (na pracovištích Czech POINT)

Podle směru konverze

1. Z elektronické do listinné podoby
2. Z listinné podoby do elektronické

Důležité závěry:

1. Dokument, který provedením konverze vznikl, má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením vznikl.
2. Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve stupu a jejich soulad s právními předpisy
3. Konverze se neprovádí např. u:
 - občanských průkazů, zbrojních průkazů, řidičských průkazů, ...
 - technických formátů
 - audioformátů

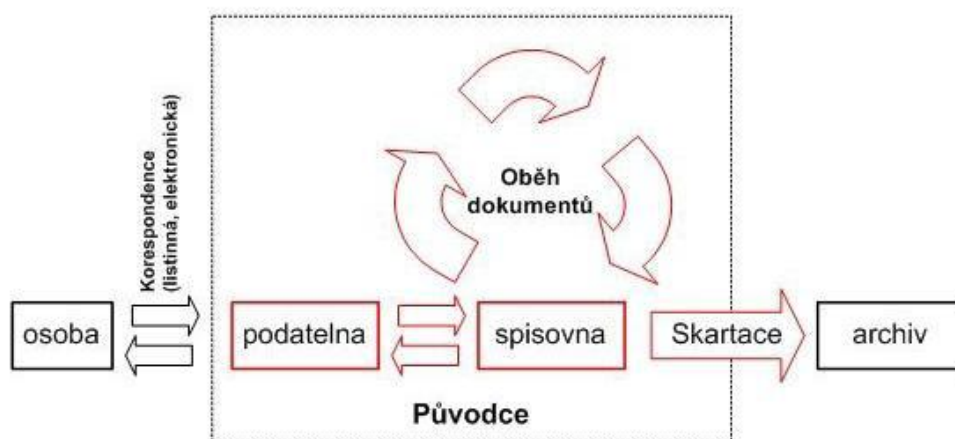
7 Archivace a dlouhodobé ukládání elektronických dokumentů

V této kapitole se budeme zabývat tématy:

1. Archivace a dlouhodobé ukládání listinných a elektronických dokumentů
2. Hlavní problémy ukládání elektronických dokumentů
3. Zajištění právních požadavků na autenticitu a ukládání elektronických dokumentů

7.1 Ukládání dokumentů z různých pohledů

Ukládání dokumentů z **pohledu původce** vysvětluje následující schéma.



Ukládání dokumentů z pohledu předmětu

V tabulce je porovnání listinných a elektronických dokumentů:

Listinné	Elektronické
Obsah je svázaný s nosičem	Informace, která je předmětem archivace, je nezávislá na nosiči a formátu dat
Existuje originál a kopie	Není možné rozlišit kopii a originál
Vlastnosti dokumentu dokladující jeho pravost a autenticitu mizí s fyzikálními vlastnostmi dokumentu	Pravost a autenticita dokumentu je dána metadaty a jejich virtuálními vlastnostmi
Technologie archivace je technologií uchovávání fyzikálních a chemických vlastností dokumentu	Technologie archivace je technologií zachování čitelnosti dat a dokladovatelnosti virtuálních vlastností dokumentu
Interpretace obsahu archivovaného dokumentu je věcí znalosti lidí o prostředí, ve kterém dokument vznikl	
Archivace listinných dokumentů je obor, který se utváří již stovky let	Archivace elektronických dokumentů není starší než několik desítek let, ale je mnohem dynamičtější a neustálý

7.2 Elektronická archivace

Nejdůležitější otázky, které musí elektronická archivace řešit, jsou:

1. Jak zachovat čitelnost nosičů dat?
2. Jak zachovat čitelnost formátů?
3. Jak zachovat dokladovatelnost a pravdivost autenticity dat?

Opatření pro **zachování čitelnosti nosičů dat**:

- **Organizační** - evidence, kontrola, přepisování, likvidace.
- **Technologická** - řeší úroveň kvality médií, mechanik, archivačního prostředí.

Pro archivaci elektronických dokumentů byly vyvinuty **standardy**:

- ISO 14721:2003 - Reference Model for an Open Archival Information System

- General International Standard Archival Information

Vzhledem k vývoji SW se zabýváme otázkou, **jak číst původní data v novém prostředí.**

Přístupy mohou být dva:

1. **Migrace**, kdy přizpůsobujeme data prostředí. Tato metoda je použitelná u dat, u kterých není nutné zachovat vlastnosti dokládající pravost a autenticitu dat.
2. **Emulace**, kdy přizpůsobujeme prostředí datům. Metodu používáme v případě, že spolu s daty ukládáme informace nutné pro přizpůsobení prostředí, tzv. metadata.

7.3 Prokazování pravosti a autenticity dat

Pravost a autenticita dat jsou vlastnosti dokumentu:

- jejichž nosičem jsou jiná metadata jednoznačně spojená s původním dokumentem
- mající své vlastnosti, které způsobují, že jejich prokazatelnost v čase zaniká

Hlavním problémem je omezení platnosti těchto dat/atributů a prokazování jejich existence zpět v čase.

Prokazování pravosti a autenticity dat

Řešení založené na organizačních a právních náležitostech:

- pro jednotlivce relativně náročné na technologii, organizaci a finance,
- pro dokumenty, u kterých je nutné zajistit prokazatelnost pravosti a autenticity dokumentu je třeba použít zákonem garantovaný čas a certifikáty,
- znalost řešení není zatím příliš rozšířena u uživatelů.

Řešení formou centralizace archivační autority:

- subjekt, který formou služby poskytuje technologickou platformu, je důvěryhodný a jeho služby jsou zákonem garantované,
- cena technologie je rozprostřena do jednotlivých cen za poskytování služby,
- je možné řešit oddělení ukládání dat (např. v rámci organizace) a formou archivační autority pouze prokazování jejich pravosti a autenticity.

8 Spisová služba a její další rozvoj v souvislosti se zavedením datových schránek

Spisová služba je **páteřním systémem eGovernmentu v úřadu**. Projekt zavádění spisové služby má úzký vztah k dalším dvěma projektům, a to **Informačnímu systému datových schránek** a k projektu **Národního digitálního archivu**.

Krátce se podíváme na historii zavádění spisových služeb:

- 1991 - renesance pojmu Spisová služba
- 1993 - řešení Spisové služby pro okresní úřady České republiky
- 1999 - jednotná metodika SpS a MV ČR
- 2004 - zákon 499/2004 Sb., o archivnictví a spisové službě
- 2008 - zákon 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (tzv. zákon o eGovernmentu)
- 2009 - novela zákona 499/2004 Sb.
- 2009 - vyhláška o podrobnostech výkonu spisové služby (č. 191/2009)

9 Autorizovaná konverze dokumentů podle zákona 300/2008 Sb.

O konverzi dokumentů jsme se již zmiňovali na mnoha místech kurzu, nyní se podíváme, jak je upravena v zákoně č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi v § 22 - § 26.

§ 22

Konverze

1. Konverzí se rozumí
 - a. úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru (dále jen „dokument obsažený v datové zprávě“), ověření shody obsahu těchto dokumentů a připojení ověřovací doložky, nebo
 - b. úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky.
2. Dokument, který provedením konverze vznikl (dále jen „výstup“), má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl (dále jen „vstup“).
3. Má-li být podle jiného právního předpisu předložen dokument v listinné podobě správnímu orgánu, nebo soudu anebo jinému státnímu orgánu, zejména aby byl užit jako podklad pro vydání rozhodnutí, je tato povinnost splněna předložením jeho výstupu.

§ 23

Subjekty provádějící konverzi

1. Konverzi na žádost provádějí kontaktní místa veřejné správy.
2. Konverzi z moci úřední provádějí orgány veřejné moci pro výkon své působnosti.

9.1 Postup při provádění konverze

§ 24

Postup při provádění konverze

1. Při konverzi do dokumentu v listinné podobě subjekt provádějící konverzi:
 - a. ověří platnost kvalifikovaného časového razítka vstupu, je-li jím vstup opatřen.
 - b. ověří, že kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je založen zaručený elektronický podpis, kterým je podepsán vstup, nebo

- kvalifikovaný systémový certifikát vydaný akreditovaným poskytovatelem certifikačních služeb, na němž je založena elektronická značka, kterou je označen vstup, nebyly před okamžikem uvedeným v kvalifikovaném časovém razítku zneplatněny,
- c. ověří platnost zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (dále jen „uznávaný elektronický podpis“) nebo platnost uznávané elektronické značky.
2. Bezodkladně poté, kdy subjekt provádějící konverzi ověří shodu výstupu se vstupem a shoduje-li se výstup se vstupem, připojí k výstupu ověřovací doložku.
 3. Při konverzi do dokumentu obsaženého v datové zprávě opatří subjekt, který konverzi provedl, výstup svou uznávanou elektronickou značkou nebo uznávaným elektronickým podpisem osoby, která konverzi provedla, a zajistí, aby byl výstup opatřen kvalifikovaným časovým razítkem.
 4. Technické náležitosti provádění konverze, vstupu a výstupu stanoví ministerstvo vyhláškou.
 5. Konverze se neprovádí
 - a. je-li dokument v jiné než v listinné podobě či v podobě datové zprávy
 - b. jde-li o dokument v listinné podobě, jehož jedinečnost nelze konverzí nahradit, zejména o občanský průkaz, cestovní doklad, zbrojní průkaz, řidičský průkaz, vojenskou knížku, služební průkaz, průkaz o povolení k pobytu cizince, rybářský lístek, lovecký lístek nebo jiný průkaz, vkladní knížku, šek, směnku nebo jiný cenný papír, los, sázenku, geometrický plán, rysy a technické kresby
 - c. jsou-li v dokumentu v listinné podobě změny, doplňky, vsuvky nebo škrty, které by mohly zeslabit jeho věrohodnost
 - d. není-li z dokumentu v listinné podobě patrné, zda se jedná o
 - i. prvopis
 - ii. vidimovaný dokument
 - iii. opis nebo kopii pořízenou ze spisu
 - iv. stejnopis písemného vyhotovení rozhodnutí anebo výroku rozhodnutí vydaného podle jiného právního předpisu
 - e. je-li dokument v listinné podobě opatřen plastickým textem nebo otiskem plastického razítka
 - f. toto písmeno bylo ze zákona vypuštěno
 - g. toto písmeno bylo ze zákona vypuštěno
 - h. v případě provedení konverze na žádost, nebyl-li dokument podepsán uznávaným elektronickým podpisem nebo označen uznávanou elektronickou značkou toho, kdo dokument vydal nebo vytvořil
 - i. toto písmeno bylo ze zákona vypuštěno
 - j. jde-li o dokument obsažený v datové zprávě, který nelze konvertovat do listinné podoby, například o zvukový nebo audiovizuální záznam
 - k. pokud dokument obsažený v datové zprávě nesplňuje technické náležitosti podle odstavce 4.
 6. Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy

9.2 Ověřovací doložka, evidence provedených konverzí, zkouška k provádění konverze a přechodná ustanovení

§ 25

Ověřovací doložka

1. Ověřovací doložka konverze do dokumentu obsaženého v datové zprávě je součástí výstupu a obsahuje
 - a. název subjektu, který konverzi provedl

- b. pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí
 - c. údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu
 - d. údaj o tom, z kolika listů se skládá vstup
 - e. údaj o tom, zda vstup obsahuje vodoznak, reliéfní tisk nebo embossing, suchou pečeť nebo reliéfní ražbu, opticky
 - f. variabilní prvek nebo jiný zajišťovací prvek
 - g. datum vyhotovení ověřovací doložky
 - h. jméno, případně jména, a příjmení osoby, která konverzi provedla
2. Ověřovací doložka konverze do dokumentu v listinné podobě je součástí výstupu a obsahuje
- a. název subjektu, který konverzi provedl
 - b. pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí
 - c. údaj o ověření toho, že obsah výstupu odpovídá obsahu vstupu
 - d. údaj o tom, z kolika listů se skládá výstup
 - e. datum vyhotovení ověřovací doložky
 - f. údaj o tom, zda byl vstup podepsán platným uznávaným elektronickým podpisem nebo označen platnou uznávanou elektronickou značkou, číslo kvalifikovaného certifikátu, na němž je uznávaný elektronický podpis založen, nebo číslo kvalifikovaného systémového certifikátu, na němž je uznávaná elektronická značka založena, a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát vydal
 - g. datum a čas uvedené v kvalifikovaném časovém razítku, číslo kvalifikovaného časového razítka a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal, byl-li vstup kvalifikovaným časovým razítkem opatřen
 - h. otisk úředního razítka, jméno, popřípadě jména, příjmení a podpis osoby, která konverzi provedla.

§ 26

Evidence provedených konverzí

1. Subjekt provádějící konverzi vede evidenci provedených konverzí. Záznam v evidenci obsahuje tyto údaje:
 - a. pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí
 - b. datum provedení konverze
 - c. konkrétní označení vstupu a datum jeho sepsání, je-li datum ve vstupu obsaženo
 - d. údaj o uhrazení správního poplatku nebo odměny notáře (uvedení čísla dokladu, kterým byl uhrazen) nebo údaj o osvobození od správního poplatku s odkazem na právní předpis.
2. Údaje podle odstavce 1 jsou v evidenci provedených konverzí uchovávány po dobu 10 let od provedení konverze.

§ 30

Konverzi na žádost provádí u držitele poštovní licence a Hospodářské komory České republiky zaměstnanec, který složil zkoušku. Složení zkoušky se nevyžaduje, splňuje-li zaměstnanec požadavky pro provádění vidimace a legalizace. (§ 14 odst. 1 zákon č. 21/2006 Sb., zákon o ověřování)

Přechodná ustanovení

Po dobu šesti měsíců ode dne, kdy nabudou účinnosti § 1, 2, 17, 18 a 20 tohoto zákona, mohou fyzické osoby, podnikající fyzické osoby a právnické osoby dodávat do datové schránky jiné fyzické osoby, podnikající fyzické osoby nebo právnické osoby pouze faktury nebo obdobné žádosti o zaplacení.

9.3 Souhrn kapitoly



Na konec kapitoly o konverzi si zopakujeme několik nejdůležitějších poznatků:

- autorizovaná konverze je převedení dokumentu v listinné podobě do elektronické (nebo naopak), ověření shody obsahu a připojení ověřovací doložky
- rozlišujeme 2 typy konverze:
 - konverze na žádost na Czech POINTech
 - konverze z moci úřední – OVM pro výkon své působnosti
- Vyhláška o autorizované konverzi dokumentu - účinnost k 1. 7. 2009
- Vyhláška upravuje:
 - technické náležitosti autorizované konverze
 - technické náležitosti vstupu a výstupu (§ 24, odst. 4 vzor osvědčení o vykonání zkoušky (§ 30, odst. 4)

10 Informační zdroje



Na závěr upozorňujeme ještě na několik odkazů na internetové stránky, kde můžete hledat další informace o datových schránkách.

- <http://www.datoveschranky.info>
- <http://www.mvcr.cz/datove-schranky.aspx>
- <http://www.egoncentrum.cz>
- <http://www.institutpraha.cz>
- <http://www.dataschranky.cz> (informace z konference „Datové schránky po roce... a teď už pro všechny!“)

Pochopitelně mezi základní informační zdroje patří provozní řád ISDS, který máte k dispozici také jako přílohu tohoto kurzu.

11 Závěr



V tomto modulu jsme se Vám snažili přiblížit Informační systém datových schránek a vše, co nás čeká v souvislosti se zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

MODUL: ISDS II - Praktické zkušenosti s užitím DS OVM, PO, FO

Tento modul se věnuje práci se všemi typy datových schránek. Klade při tom důraz na představení jejich možností a úskalí. Zároveň nabízí konkrétní statistiky používání datových schránek.

Tento modul si klade za cíl detailně seznámit studenty s praktickými zkušenostmi všech druhů datových schránek.

1 Úvod

Tato část kurzu se věnuje praktickému práci s Informačním systémem datových schránek. Získáte přehled o praktickém používání datové schránky orgánu veřejné moci společně s informacemi o propojení s elektronickou spisovou službou, datové schránky fyzické osoby a datové schránky právnické osoby.

2 Praktická obsluha DS z pohledu úřadu, orgánu veřejné moci (OVM)

Orgán veřejné moci má datovou schránku zřízenou ze zákona a datová schránka, pokud tak vedoucí orgánu veřejné moci neučinil dříve, byla aktivována 1. 11. 2009.

Od toho okamžiku mohli do datové schránky OVM posílat všechny orgány veřejné moci, právnické osoby, fyzické osoby podnikající a fyzické osoby mající datovou schránku, ať již jim byla zřízena na žádost nebo ze zákona, datové zprávy.

2.1 Prvotní (primární) nastavení DS

Vedoucí orgánu veřejné moci se v prvním kroku s pomocí přihlašovacích údajů, které obdržel poštou do vlastních rukou, přihlásil do datové schránky a v nastavení datové schránky přidal uživatele s funkcí „administrátor“.

Touto osobou je zaměstnanec úřadu, nejčastěji pracovník odboru (oddělení) informatiky. Administrátor poté obdržel své přihlašovací údaje a podle pokynů vedoucího OVM, ředitele úřadu, tajemníka nebo jiného nadřízeného nastavil další vlastnosti datové schránky, případně přidal další uživatele ve funkci pověřené osoby.

2.2 Zpřístupnění DS

Těmito kroky, zmíněnými v předchozí kapitole, se stává datová schránka zpřístupněna pro komunikaci, to znamená, že je možné a v rozsahu daném zákonem je i povinností, datové zprávy prostřednictvím informačního systému datových schránek (ISDS) odesílat a přijímat.

Proto, aby úřad (OVM) mohl vytvářet datové zprávy ve formátu daném zákonem je nutné, aby pracovníci, kteří mají podle vnitřní směrnice podpisové právo, měli **možnost vytvářet a připojovat** k datovým dokumentům **elektronický podpis**. Proto každý pracovník OVM s právem podepisovat si musí zřídit **osobní kvalifikovaný certifikát zaměstnance**. Tento certifikát mu vystaví některá ze tří akreditovaných certifikačních autorit v České republice.

2.3 Technické předpoklady komunikace přes ISDS

Protože se jedná o datovou komunikaci, musí mít OVM pro práci s ISDS připraveny a splněny i některé technické předpoklady. Počítač s operačním systémem, který umožní práci s hashovací funkcí SH-2 (to je např. u operačního systému Microsoft Windows XP SP3 a vyšší), připojení k síti internet,

internetový prohlížeč do kterého je možné doinstalovat doplněk pro zobrazování xml formulářů 602 filler, program, který umožňuje převod textového dokumentu do formátu pdf/A a připojení elektronického podpisu. Instalaci doplňku je možné provést z adresy <http://www.mojedatovaschranka.cz/static/pages/testform.html> nebo se provede při prvním otevření formuláře datové zprávy v DS.

Praktická práce s ISDS se významně liší podle toho, zda OVM využívá elektronickou spisovou službu (ESS) nebo nikoliv a pak veškerá evidence od přiřazování čísel jednacích spisů, po evidenci odeslané a došlé pošty a oběh dokladů je prováděn v papírové podobě.

V zákoně 499/2007 Sb. v §63 je řečeno, kteří veřejnoprávní původci vykonávají spisovou službu v elektronických systémech spisové služby. V současné době nemají povinnost vést spisovou službu v elektronické podobě všechny OVM.

Orgány veřejné moci, které nepoužívají elektronickou spisovou službu, komunikují s DS přes webové rozhraní ISDS na adrese <https://www.mojedatovaschranka.cz>

2.4 Způsoby přihlášení do DS

Existují dva způsoby přihlášení s různou mírou bezpečnosti

2.4.1 Přihlášení do DS bez certifikátu

Přihlášení do datové schránky - Windows Internet Explorer

https://login.mojedatovaschranka.cz/nidp/iddff/sso?id software t602

Soubor Úpravy Zobrazit Oblíbené položky Nástroje Nápověda

Oblíbené položky Downl... Přihl... x

Stránka Zabezpečení Nástroje

@ datové schránky INFOLINKA: 270 005 200

Přihlášení **Certifikát**

Uživatelské jméno (ID osoby):

Heslo:

Opište kód z obrázku

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

PŘIHLÁSIT

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

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Česká pošta

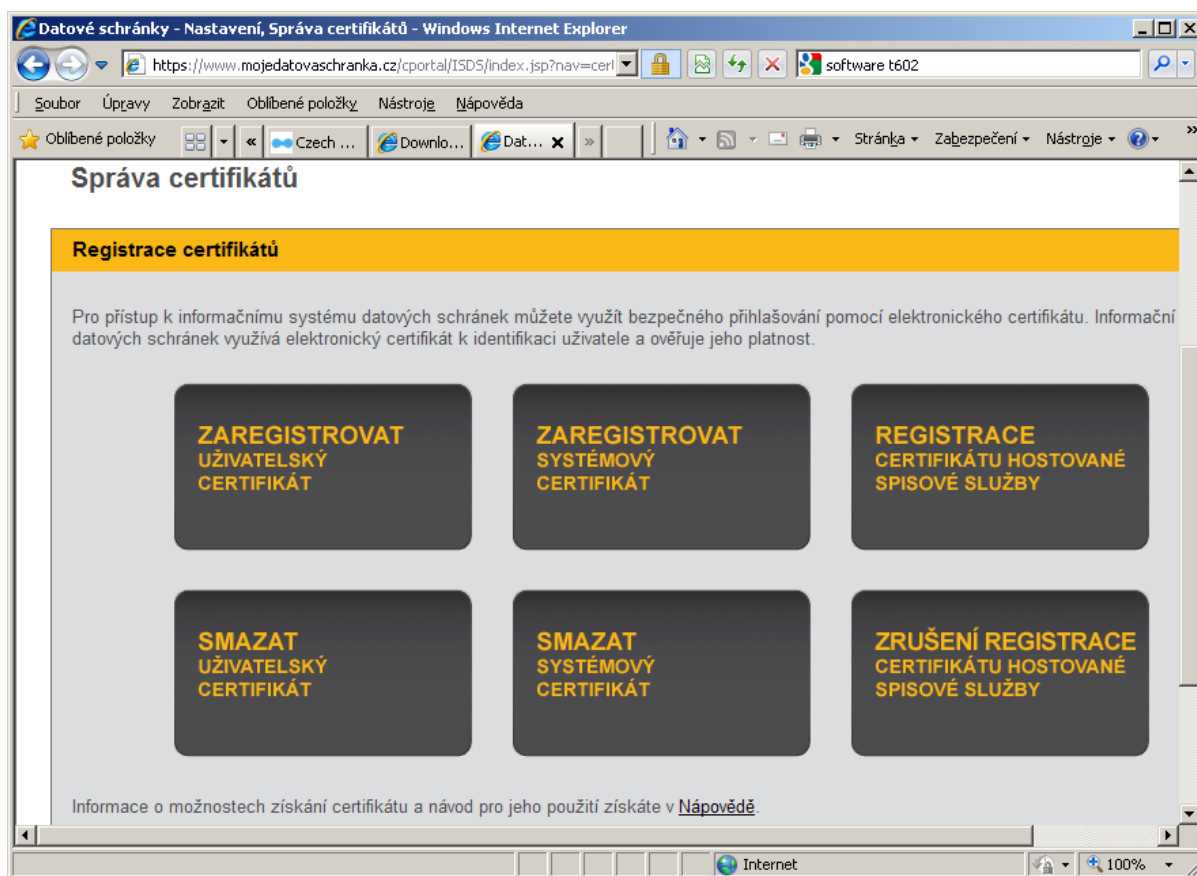
Správce: Ministerstvo vnitra České republiky; Provozovatel: Česká pošta s. p. [Ochrana osobních údajů](#) | [Prohlášení o přístupnosti](#)

Hotovo Internet 100%

Je možné se přihlásit přímo po zadání uživatelského jména, hesla a bezpečnostního kódu. Bezpečnostní kód je v případě špatné čitelnosti možné vygenerovat opakované nebo si jej nechat přehrát ve zvukové podobě.

2.4.2 Přihlášení do DS s certifikátem

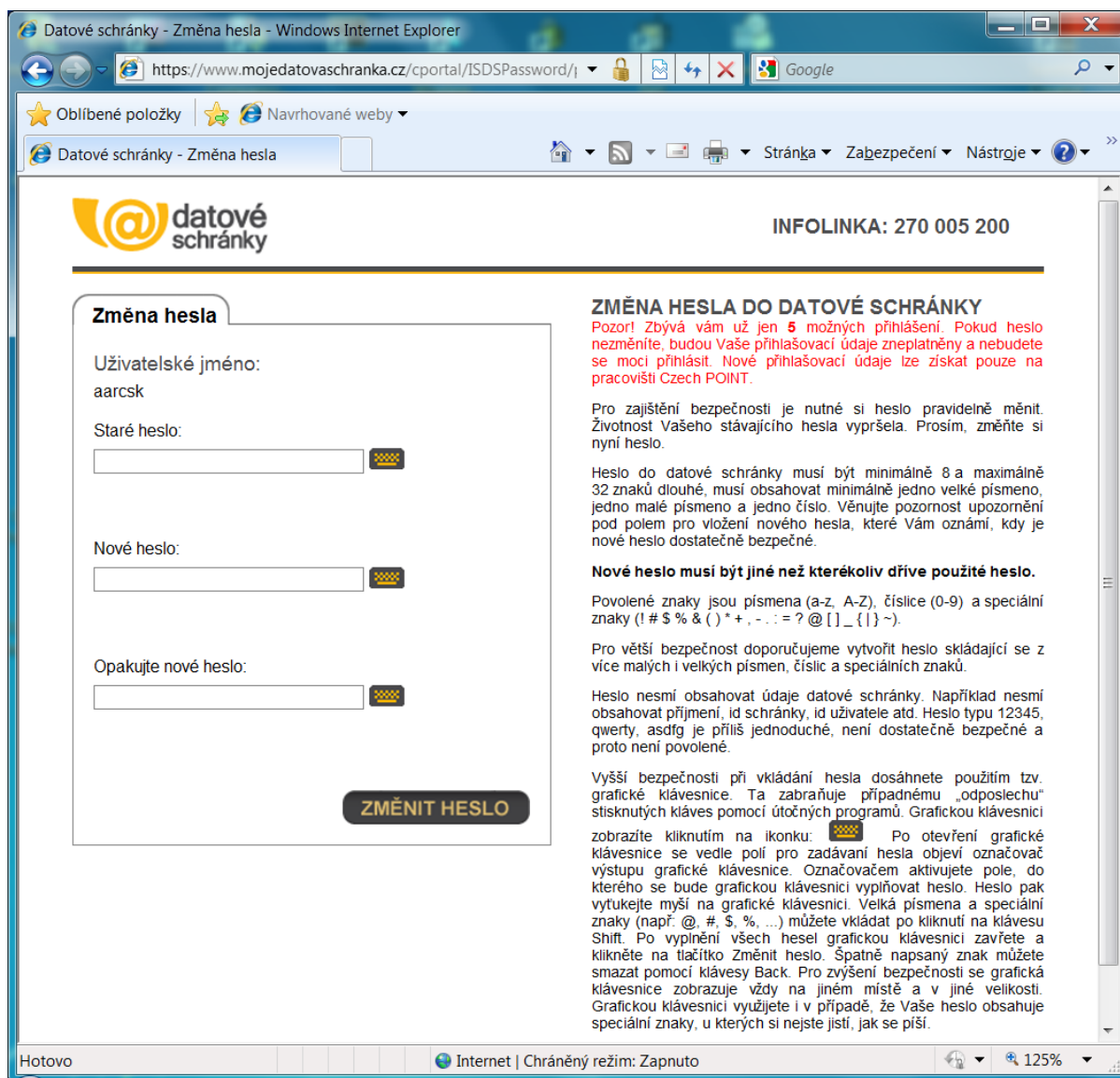
Vyšší úroveň zabezpečení má přihlášení na druhé záložce, s pomocí certifikátu. Pro tento účel je potřeba si pořídit u certifikační autority tzv. komerční certifikát, který je možné mít nainstalovaný v systému, nebo na bezpečném úložišti – tokenu. Aby bylo možné se přihlašovat pomocí certifikátu je potřeba v nastavení datové schránky v oddíle správa certifikátů, zaregistrovat uživatelský certifikát respektive jeho sériové číslo.



Pokud nechceme přihlašování pomocí certifikátu dále používat, můžeme uživatelský certifikát smazat. Registrace dalších certifikátů slouží pro přístup programu elektronické spisové služby prostřednictvím webové služby. Při použití certifikátu pro zabezpečené přihlašování je potřeba dát pozor na vypršení platnosti certifikátu a včas jej obnovit.

2.4.3 Heslo pro přístup do DS

Heslo pro přístup do datové schránky má omezenou platnost na 90 dní a je potřeba jej periodicky měnit. Při prvním přihlášení do DS je rovněž vyžadována změna hesla. Pokud platnost hesla vyprší, dává nám systém ještě 5 možností se přihlásit pod starým heslem, než se přístup uzamkne.



V případě, že heslo nezměníme včas a přístup je uzamčen je nutné požádat na pracovišti Czechpoint o zneplatnění přístupových údajů k DS a vystavení nových. Opakované vystavení nových údajů je zpoplatněno.

2.4.4 Uchovávání DZ

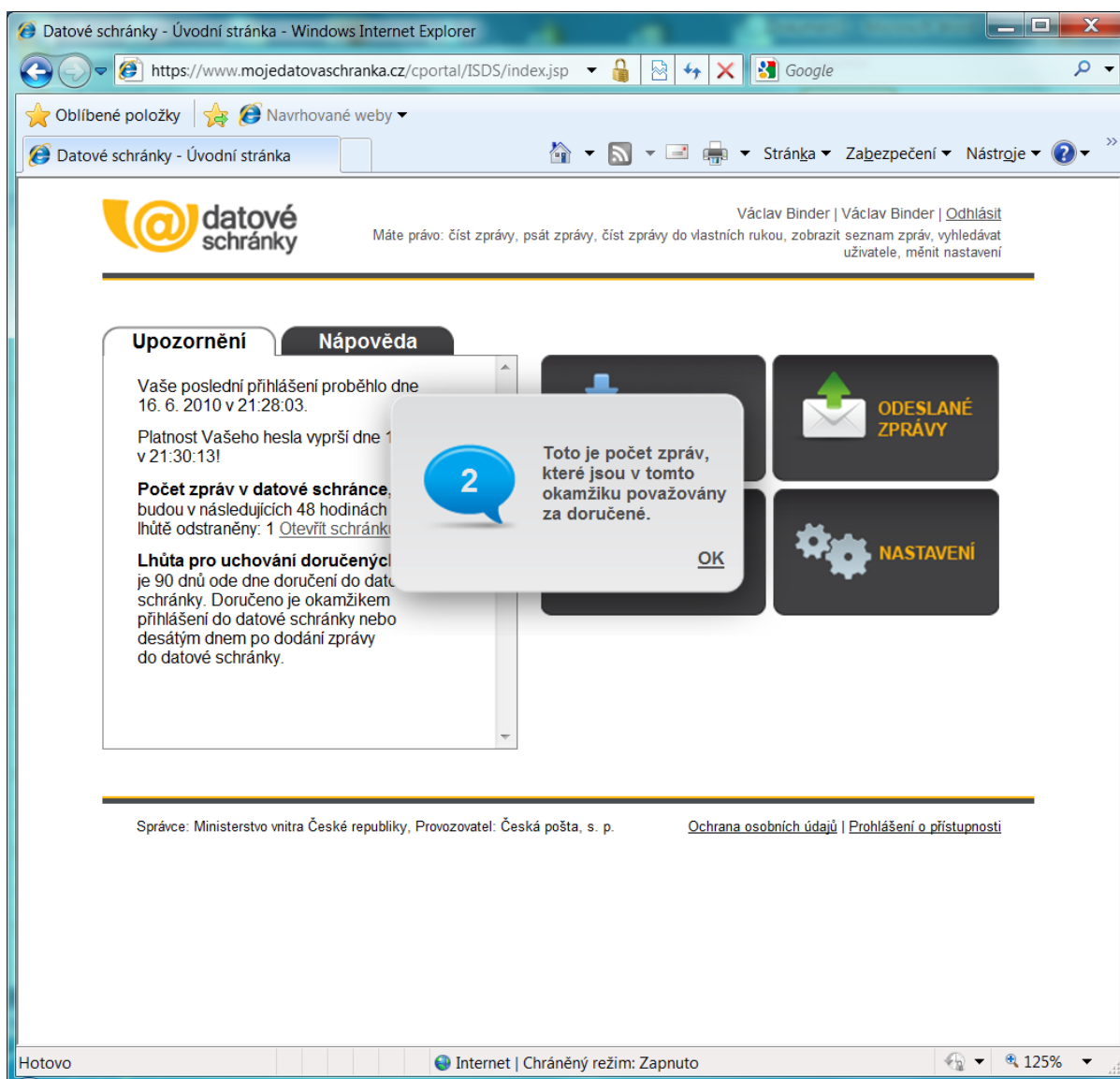
ISDS uchovává datové zprávy po dobu 90 dní od doručení. Po této době je datová zpráva vymazána a zůstanou zachována pouze určitá metadata o existenci zprávy a jejím průchodem ISDS. Proto je důležité v přechodném období, než budou vybudována technologická centra s garantovanými úložišti, zajistit bezpečné ukládání odeslaných i došlých zpráv z DS. Je důležité ukládat zprávu celou, to znamená i s obálkou – soubor s příponou „zfo“. Tento soubor, kromě metadata obsahuje i důležité časové razítko, které připojuje ke zprávě ISDS v okamžiku doručení zprávy do DS. Důležité je rovněž bezpečně ukládat a archivovat doručky. Ty jsou připojeny k odeslaným datovým zprávám v okamžiku kdy oprávněná nebo pověřená osoba vstoupí do datové schránky a dodaná zpráva se v ní nachází, nebo když nastane fikce doručení.

Další možností pro ukládání zpráv z datové schránky, je využití doplňkové služby DS datový trezor. Tato služba je zpoplatněna a je možné ji objednat na kontaktním místě CzechPoint. Datové zprávy v DS, které expirovaly, se pak přesouvají do datového trezoru. V rozhraní DS pak přibude tlačítko, které umožní vstup do datového trezoru a práci se zprávami v něm uloženými.

Způsob archivace datových zpráv si může úřad zvolit sám, ale vždy takový, aby byl splněn požadavek zákona v tomto případě zákona 499/2004 Sb. §69a odstavec (3).

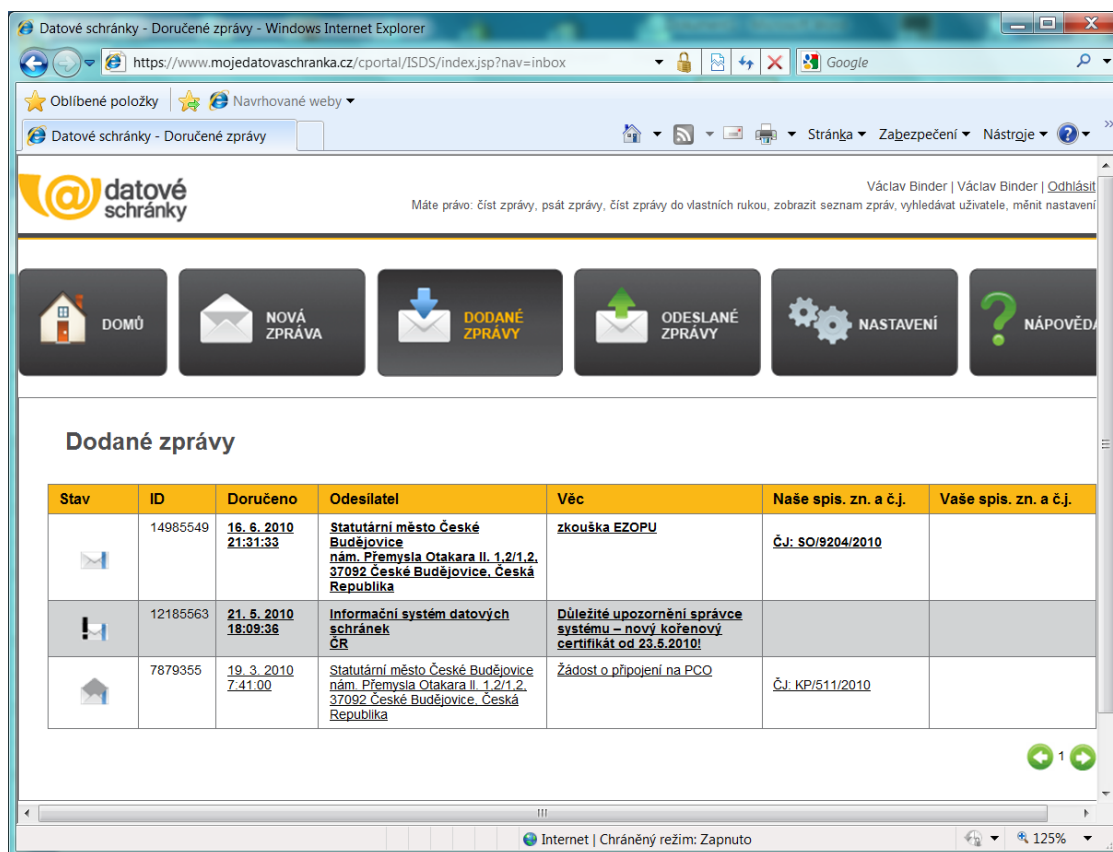
2.5 Přijetí dokumentu prostřednictvím DS

Při vstupu do datové schránky se zobrazí počet nově došlých zpráv od posledního vstupu.



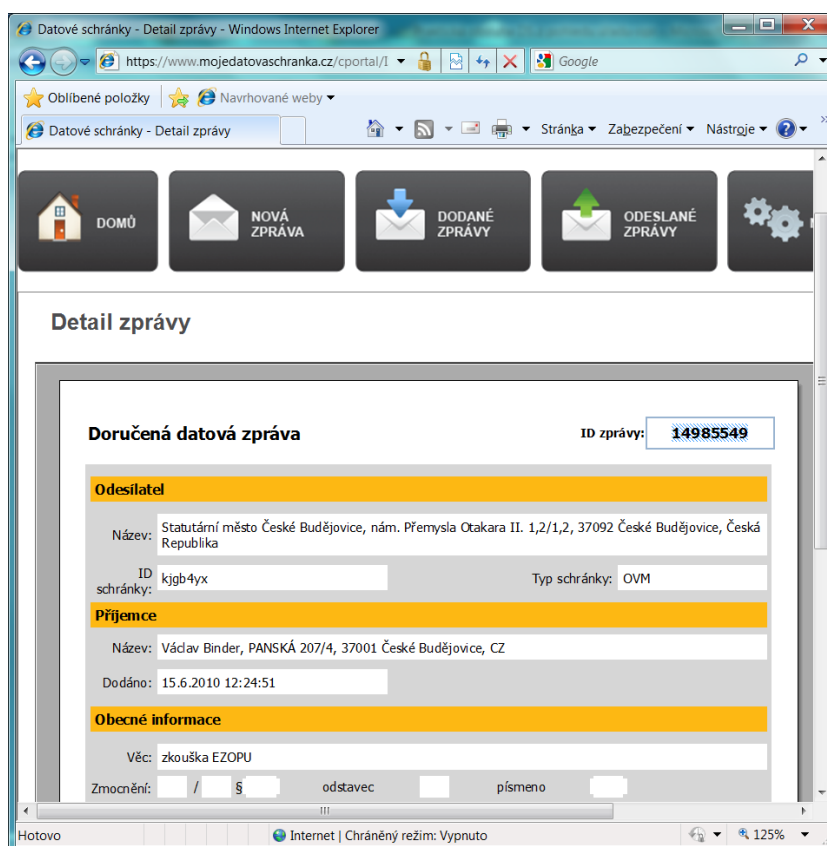
2.5.1 Dodané zprávy

Po vstupu do složky „Dodané zprávy“ vidíme seznam všech zpráv, které do datové schránky došly a ještě se v ní nacházejí. Ikona ve sloupci stav označuje rozlišení zpráv na ty, které jsme ještě nepřečetli, na ty které jsme již otevřeli, zvláštní ikonou jsou označeny zprávy určené do vlastních rukou a zprávy zaslané ISDS (systémové zprávy a informace).



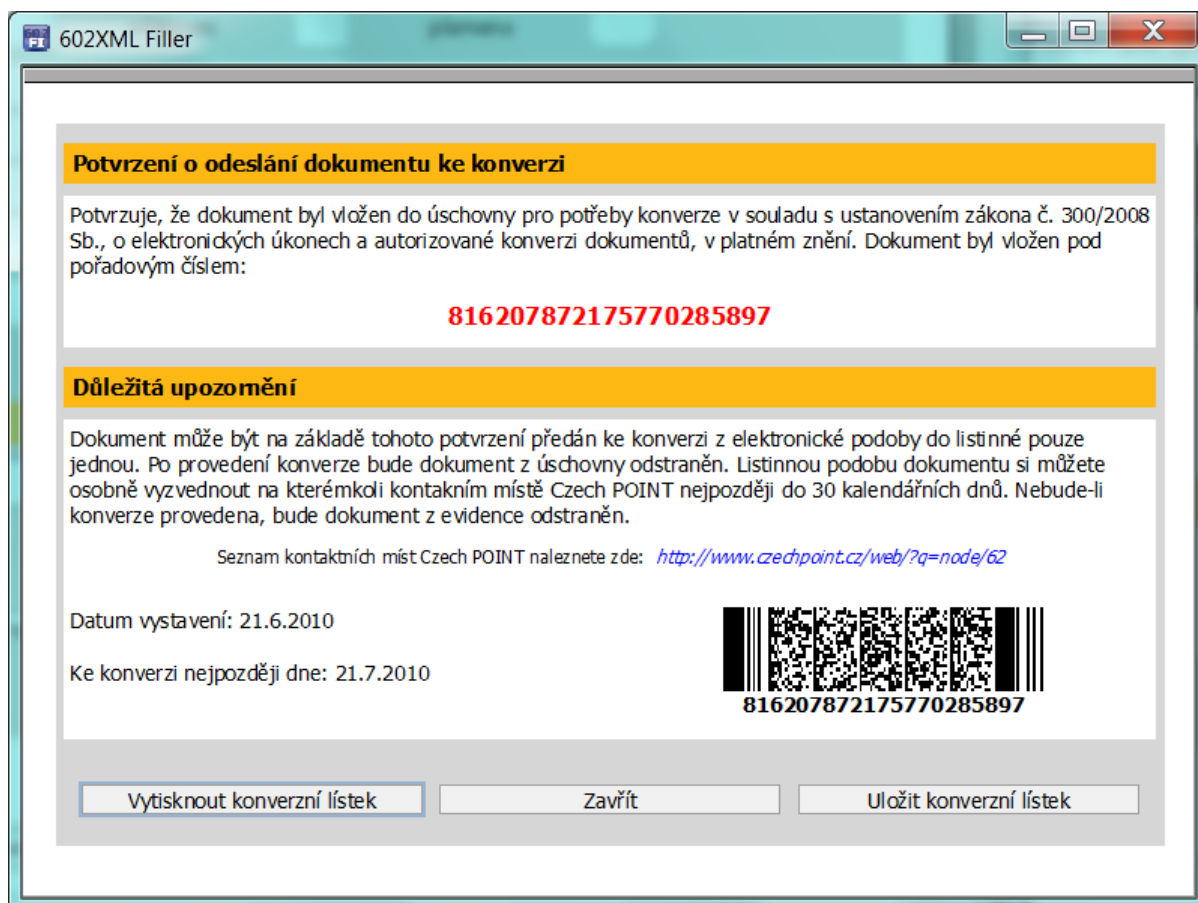
2.5.2 Detail zprávy

Kliknutím myši kdekoli v řádku zprávy se otevře formulář s detailem zprávy. Předpokladem otevření je nainstalovaný doplněk 602 filler. Pokud dosud nebyl nainstalován, zobrazí se požadavek na jeho instalaci. Pokud toto schválíme a prohlížeč má nastaveno povolení k instalaci doplňků, ten se nainstaluje a následně se formulář zobrazí.



Máme několik možností co se zprávou udělat. Přílohu (případně přílohy) zprávy je možné otevřít, vytisknout, uložit, odeslat ke konverzi. Odeslat ke konverzi znamená odeslat do úschovny Czech POINTu pro následné provedení autorizované konverze do listinné podoby.

2.5.3 Uložení DZ



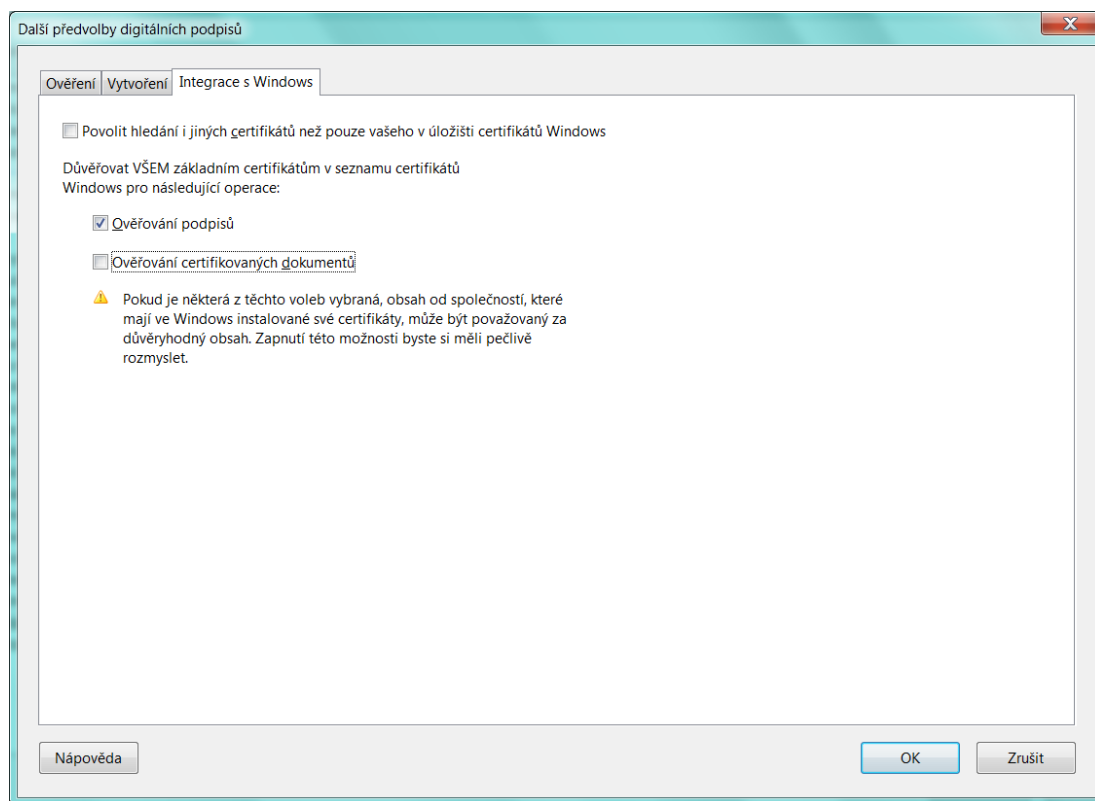
Nejdůležitějším úkonem je uložení celé datové zprávy na disk, to znamená do bezpečného úložiště, kde budeme zprávy archivovat, abychom s nimi mohli následně provádět další úkony. Jméno souboru má tvar „DDZ_identifikační číslo datové zprávy.zfo“.

Pokud příjemce obdrží dokument v digitální podobě prostřednictvím DS, ověří tak jak ukládá zákon 499/2004 §69a odstavec (2) „Je-li doručený dokument v digitální podobě opatřen uznávaným elektronickým podpisem, elektronickou značkou nebo kvalifikovaným časovým razítkem, platnost uznávaného elektronického podpisu, elektronické značky nebo kvalifikovaného časového razítka a platnost kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu.“ Pro ověření platnosti uznávaného elektronického podpisu je nutné použít nějaký softwarový prostředek, nejnázve program Adobe Reader. Předpokladem správné funkce programu je instalace kořenových certifikátů všech tří akreditovaných certifikačních autorit. Jsou to tyto: První certifikační autorita a.s., Česká pošta s. p. (Postsignum) a Eidentity a.s.

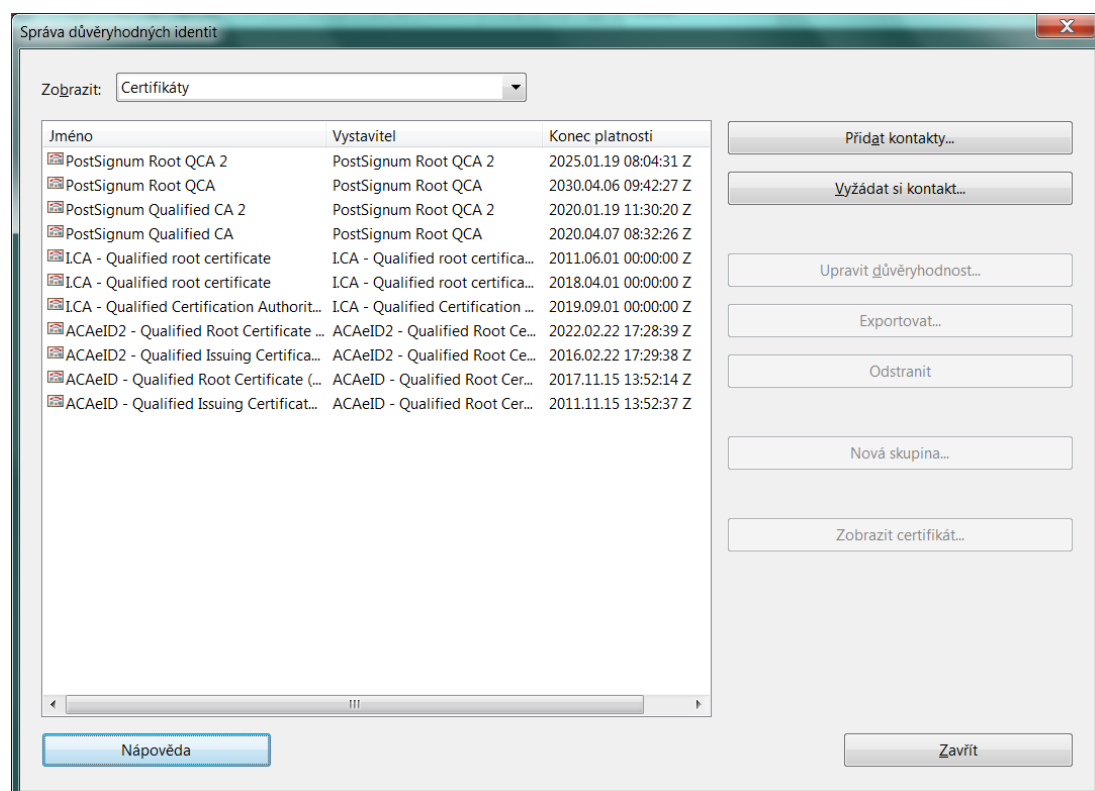
Vzhledem k tomu, že jsou v platnosti certifikáty postavené na algoritmu hashovací funkce SH-1, tak nově vydávané certifikáty s algoritmem SH-2, je nutné instalovat kořenové certifikáty pro oba typy certifikátů.

2.5.4 Instalace kořenových certifikátů

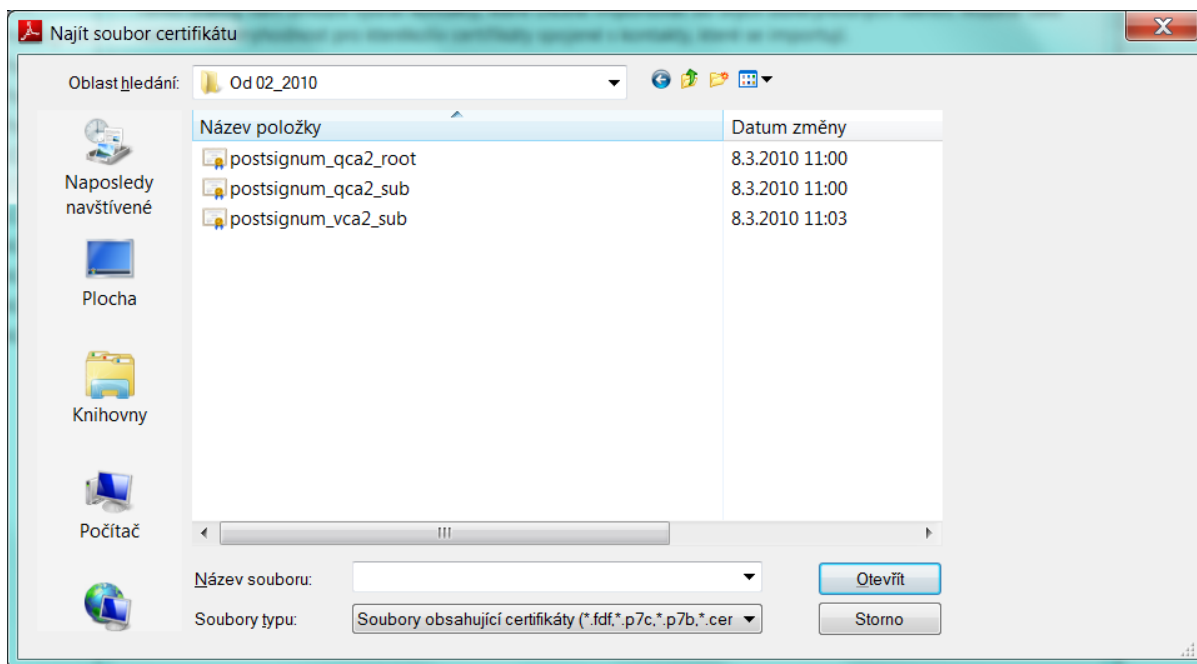
Tyto kořenové certifikáty je možné nainstalovat do operačního systému a v programu Adobe Reader ve volbě v horním menu postupně „Úpravy - Předvolby...- Zabezpečení - tlačítko Další předvolby - záložka Integrace s Windows vložit zatržítko u Ověřování podpisů“.



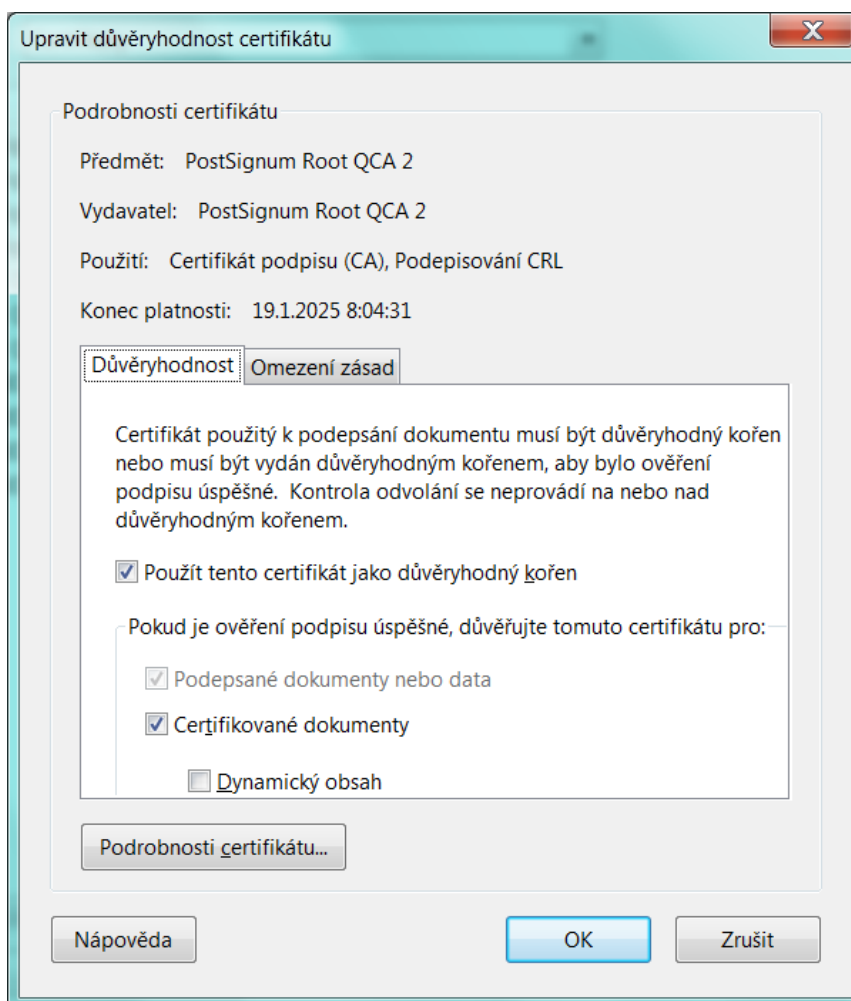
Jiná možnost je nainstalovat kořenové certifikáty přímo do programu Adobe Reader. V tomto případě postupujeme takto: Volba v horním menu „Dokument – Správa důvěryhodných identit... - Zobrazit volba Certifikáty



Pokud seznam neobsahuje všechny kořenové certifikáty je nutné je postupně nainstalovat. Stiskneme tlačítko „Přidat kontakty...“ – Procházet – a na disku počítače vyhledáme složku s kořenovými certifikáty akreditovaných certifikačních autorit, které jsme si dříve stáhly z jejich webových stránek

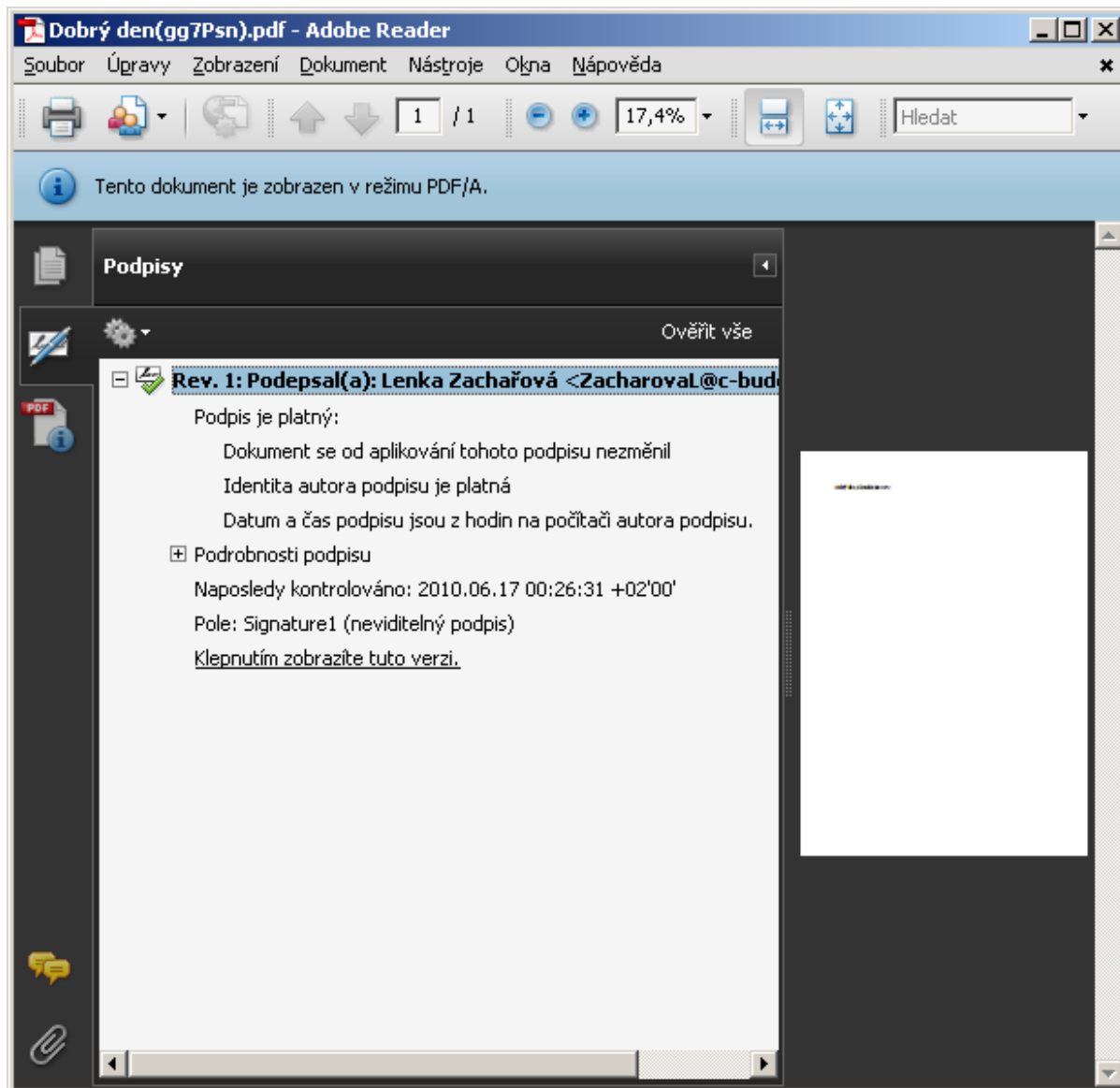


Když certifikáty postupně nainstalujeme, pro každý z nich nastavíme důvěryhodnost. Pod tlačítkem „Upravit důvěryhodnost“ se zobrazí okno, kde zatrhneme požadovaný rozsah důvěry.



Takto nastavený program Adobe Reader správně vyhodnotí platnost či neplatnost kvalifikovaného certifikátu, který byl použit pro vytvoření elektronického podpisu datové zprávy. Při ověřování elektronického podpisu je potřeba aby byl počítač připojen k síti internet, neboť program Adobe Reader ověřuje dotazem na webu certifikační autority, zdali použitý certifikát není v seznamu odvolaných a zneplatněných certifikátů. Správně podepsaný dokument je označen takto.

2.5.5 Konverze dokumentů z digitální podoby do listinné



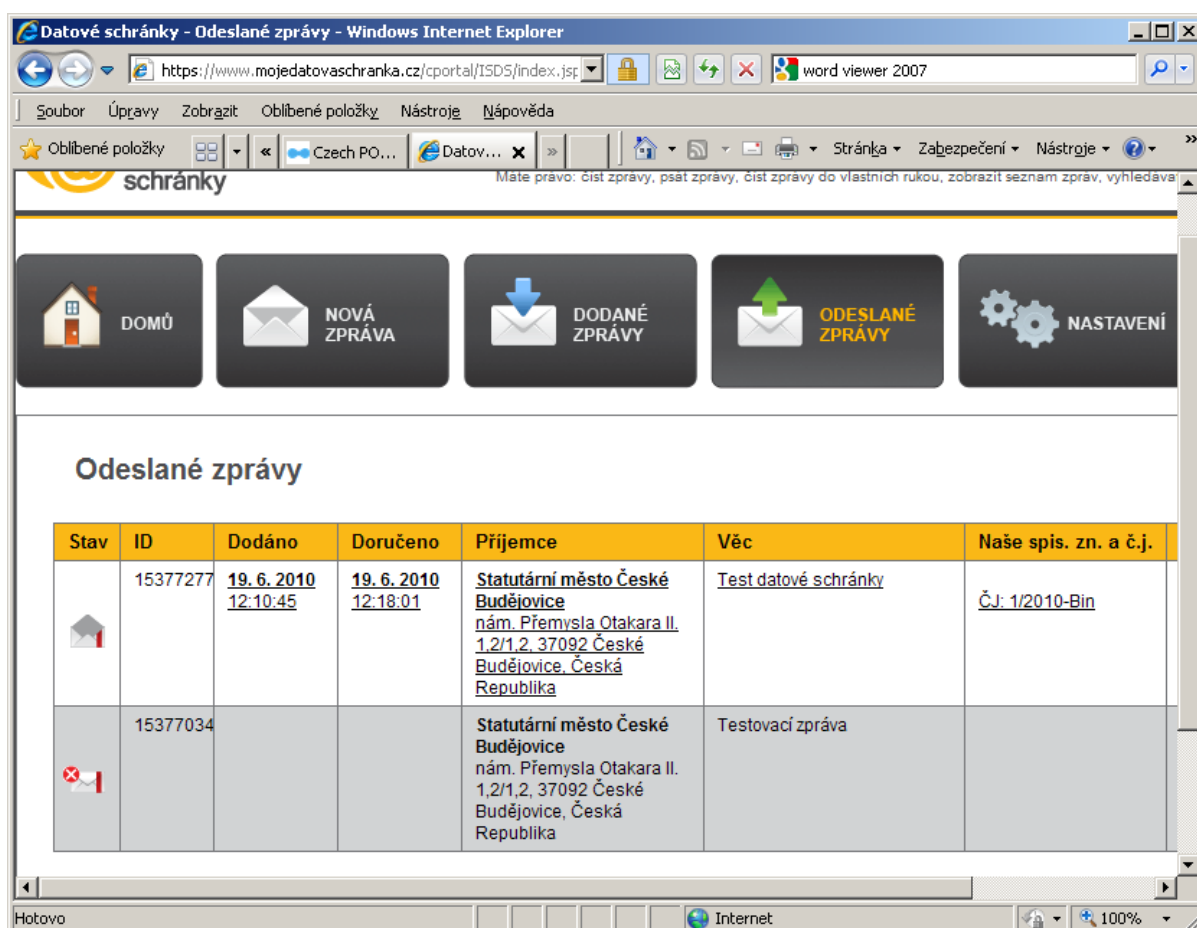
Pokud potřebujeme ať z důvodu založení do spisu nebo jednání na jiných orgánech z digitální podoby dokumentu získat listinnou (papírovou) verzi, musíme postupovat v duchu zákona 499/2004 Sb. §69a odstavec (4) který říká, že „převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak a změnu formátu dokumentu v digitální podobě provádí určený původce postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost jeho obsahu, čitelnost dokumentu a bezpečnost procesu převádění nebo změny formátu.“ Jediný způsob, který toto zajistí je tzv. „autorizovaná konverze dokumentu, v tomto případě konverze z elektronické do listinné podoby.

Czechpoint ve své části nazvané Czechpoint&Office umožňuje provádět tzv. konverzi z moci úřední, tj. pro potřeby orgánu veřejné moci pro výkon činností v rozsahu jeho pravomoci. Takto vzniklý dokument má platnost originálu a s jako takovým je s ním možné pracovat.

2.6 Odesílání dokumentu prostřednictvím DS

Dokument vzniká na úřadě nejčastěji v některém textovém editoru (např. Microsoft Word) Pokud tento dokument by v listinné podobě osahoval vlastnoruční podpis, musí v digitální podobě být zkonvertován do formátu pdf /A a připojen elektronický podpis. Na tuto operaci potřebujeme vhodný počítačový program. Může to být např.: program Prit2PDF od firmy Software602. Takto musí být vytvořen tzv. hlavní dokument. Pokud jde o přílohy, mohou být v různých formátech, které vytváří tabulkové procesory, textové editory, programy pro vytváření prezentací, různé formy bitmapových obrázků, zvuk a video. Seznam povolených formátů obsahuje příloha 3 vyhlášky 194/2009 Sb., o stanovení podrobností užívání a provozování ISDS. Pokud máme digitální soubor dat ve formátu, který vyhláška nezmiňuje, je, pokud to lze a je to účelné, takový soubor do některého z vyjmenovaných formátů zkonvertovat (např.: formátu pdf).

Není možné systém obejít tím způsobem, že bychom soubor s nepovolenou příponou přejmenovali na soubor ze seznamu povolených a adresát by jej následně přejmenoval zpátky. Tento nesoulad mezi příponou souboru a jeho skutečným datovým formátem systém datových schránek rozpozná a odeslání celé zprávy adresátovi zablokuje. V odeslaných zprávách bude taková zpráva označena křížkem v červeném kolečku:



A následně obdrží odesílatel zprávu od ISDS tohoto znění, například:

„Informujeme Vás, že Vaše datová zpráva 15377034 určená do datové schránky kjgb4yx byla zničena podle par. 20 odst. 2 zákona 300/2008 Sb.“

Může se stát, že máme digitální dokument v nevyjmenovaném formátu, v případě konverze do jiného datového formátu by dokument ztratil podstatné vlastnosti, nebo konverze není vůbec možná. Příkladem jsou datové formáty, které vznikají v programech pro projektování staveb a strojů. V tom případě vytvoříme hlavní dokument v listinné podobě, odpovědná osoba jej opatří vlastnoručním

podpisem, výkresovou dokumentaci rovněž vytiskneme, případně vypálíme na CD a pošleme klasickou poštou, to i v případě, kdy je adresátem OVM nebo právnická či fyzická osoba, která má zřízenou datovou schránku. Takový postup je v souladu se zákonem, neboť v zákoně 300/2008 Sb. §17 odstavec (1) se praví, že se posílá prostřednictvím datové schránky „Umožňuje-li to povaha dokumentu...“. Do datové schránky není také možné poslat přílohy, jejichž velikost je větší než 10 MB.

2.6.1 Odeslání nové DZ

Odeslání datové správy prostřednictvím webového rozhraní ISDS se provádí tak, že v menu zvolíme volbu „Nová zpráva“.

2.6.1.1 Výběr adresáta

Zobrazí se formulář pro výběr adresáta. Zde vybereme typ adresáta, zdali je to OVM, PO, FO nebo FOP. Poté zadáme vyhledání podle kritérií. Nejspolehlivější způsob nalezení adresáta je podle ID datové schránky.

Pokud hledáme orgán veřejné moci, právnickou osobu nebo fyzickou osobu je nejlepším vyhledávacím kritériem IČ, které je jednoznačným identifikátorem.

Pokud hledáme podle jiných vyhledávacích kritérií, můžeme se setkat s problémy. Jako příklad je možné uvést vyhledávání OVM - notáře a exekutora. Jak je patrné z následujících obrázků notáře nalezneme, pokud do údaje jméno zadáme nejprve příjmení následované jménem, u exekutora při použití tohoto pořadí systém nic nenalezne a je nutné hledat podle křestního jména a příjmení.

Datové schránky - Nová zpráva - Windows Internet Explorer
https://www.mojedatovaschranka.cz/portal/ISDS/index.jsp

Výběr adresáta

Vyberte typ schránky. Poté vyplňte vyhledávací pole a stiskněte tlačítko Vyhledat. V levém spodním sloupci zaškrtněte vybranou datovou schránku, do které chcete odeslat datovou zprávu a stiskněte tlačítko Přidat. Takto můžete přidat více adresátů. Nakonec klikněte na tlačítko Připravit zprávu.

Typ schránky: **Orgán veřejné moci** Vybrat ID schránky: *

Identifikační číslo (IČ): * Název organizace: **Tomanová Jana** *

VYHLEDAT **VYMAZAT FORMULÁŘ** **ROZŠÍŘENÉ HLEDÁNÍ**

Neznáte-li IČ hledaného subjektu, klikněte na jeden z odkazů: [Vyhledávání orgánů veřejné moci](#) | [Vyhledávání právnických osob a podnikajících fyzických osob](#)

Vyplňte pole označená hvězdičkou. Modře označené pole může být vyplněno samostatně. Červeně označená pole musí být vyplněna současně. Neoznačená pole slouží pouze k upřesnění dotazu.

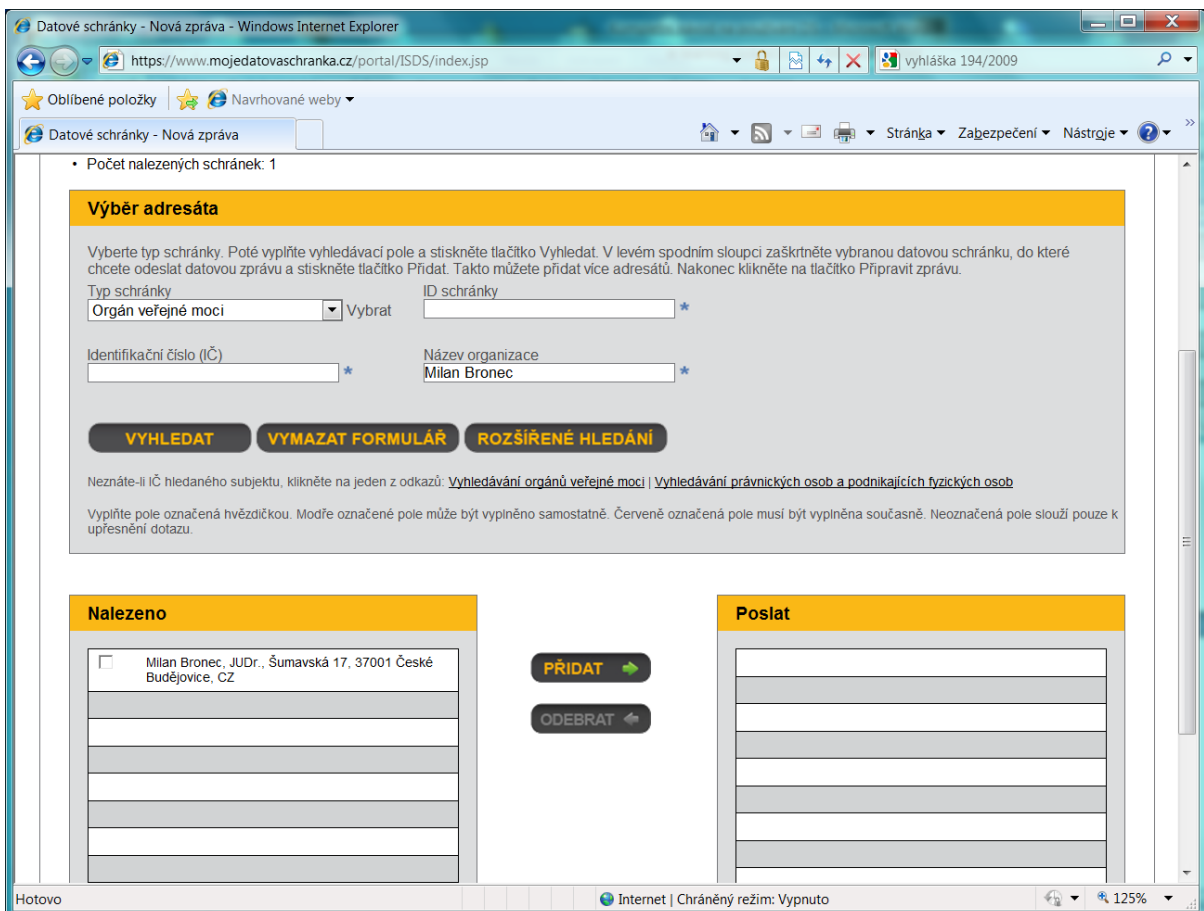
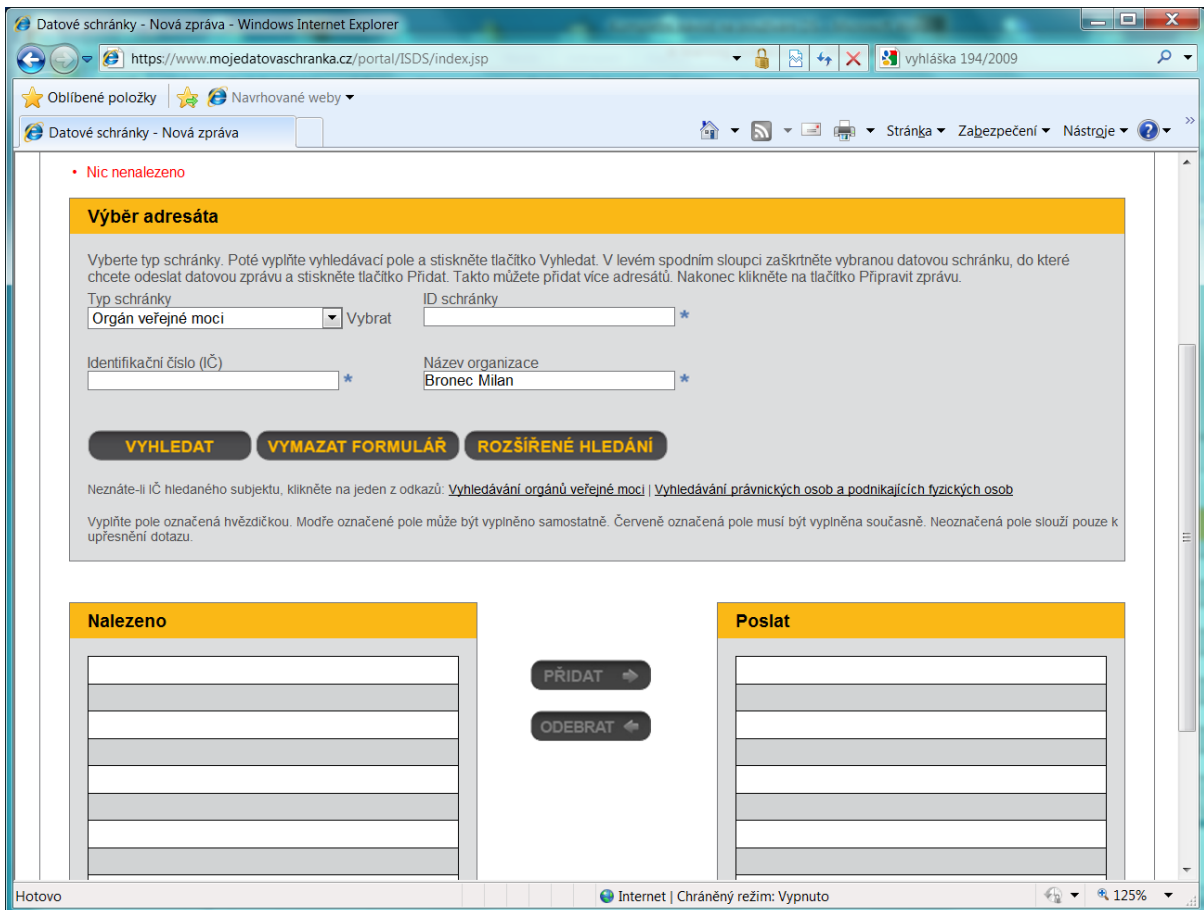
Nalezeno

<input type="checkbox"/>	JUDr. Tomanová Jana - notářka, Široká 434/13, 37001 České Budějovice, CZ
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

PŘIDAT **ODEBRÁT**

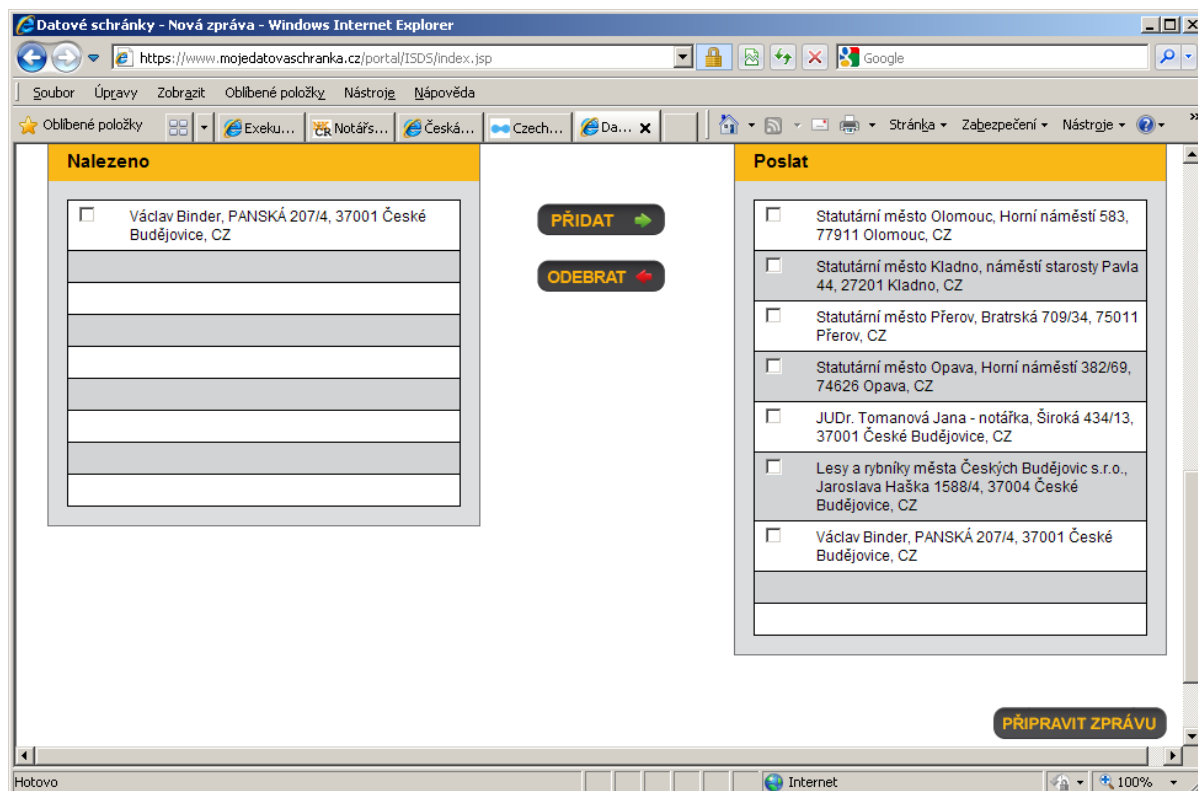
Poslat

Internet | Chráněný režim: Vypnuto 125%



System logicky neumožňuje nalézt jako adresáta sebe sama. Nalezneme-li příjemce, přeneseme jej z části formuláře Nalezeno do části Poslat. Můžeme postupně vyhledávat další adresáty a přesouvat je

do části poslat, v případě že stejný dokument chceme poslat více adresátům. Je možné kombinovat všechny typy adresátů.



2.6.1.2 Příprava zprávy

Máme-li seznam adresátů kompletní, pokračujeme tlačítkem Připravit zprávu. Otevře se formulář zprávy. Údaj o odesílateli a příjemci je předvyplněn. Vyplníme všechny ostatní, nám známe položky formuláře. Formulář umožňuje zaškrtnout volbu „Do vlastních rukou“. Pokud tuto volbu zvolíme a současně nevyplníme položku „K rukám“ kde bude jméno osoby, do jejichž vlastních rukou má být dokument doručen, způsobíme adresátovi potíže. Pokud využívá systém elektronické spisové služby a oprávněná osoba není tou osobou, která by jediná mohla přijímat došlé dokumenty určené do vlastních rukou, nebude moci příjemce klauzuli do vlastních rukou dodržet.

Z toho vyplývá, že vyplnění položek „K rukám“ a zatržení volby „Do vlastních rukou“ má smysl jen pokud jsou vyplněny obě nebo žádná. Dále se připojí hlavní dokument, a pokud existují, také přílohy. Pokud takto rozpracujeme formulář a potřebujeme dohledat ještě nějakou informaci, je možné zvolit „Uložit koncept datové zprávy na disk“. Později budeme moci pokračovat v doplnění a odeslání zprávy pouhým rozkliknutím uložené zprávy aniž bych se přihlašoval pře webové rozhraní do DS. Přihlašovací údaje do DS si vyžádá uložený formulář.

2.6.1.3 Odeslání zprávy

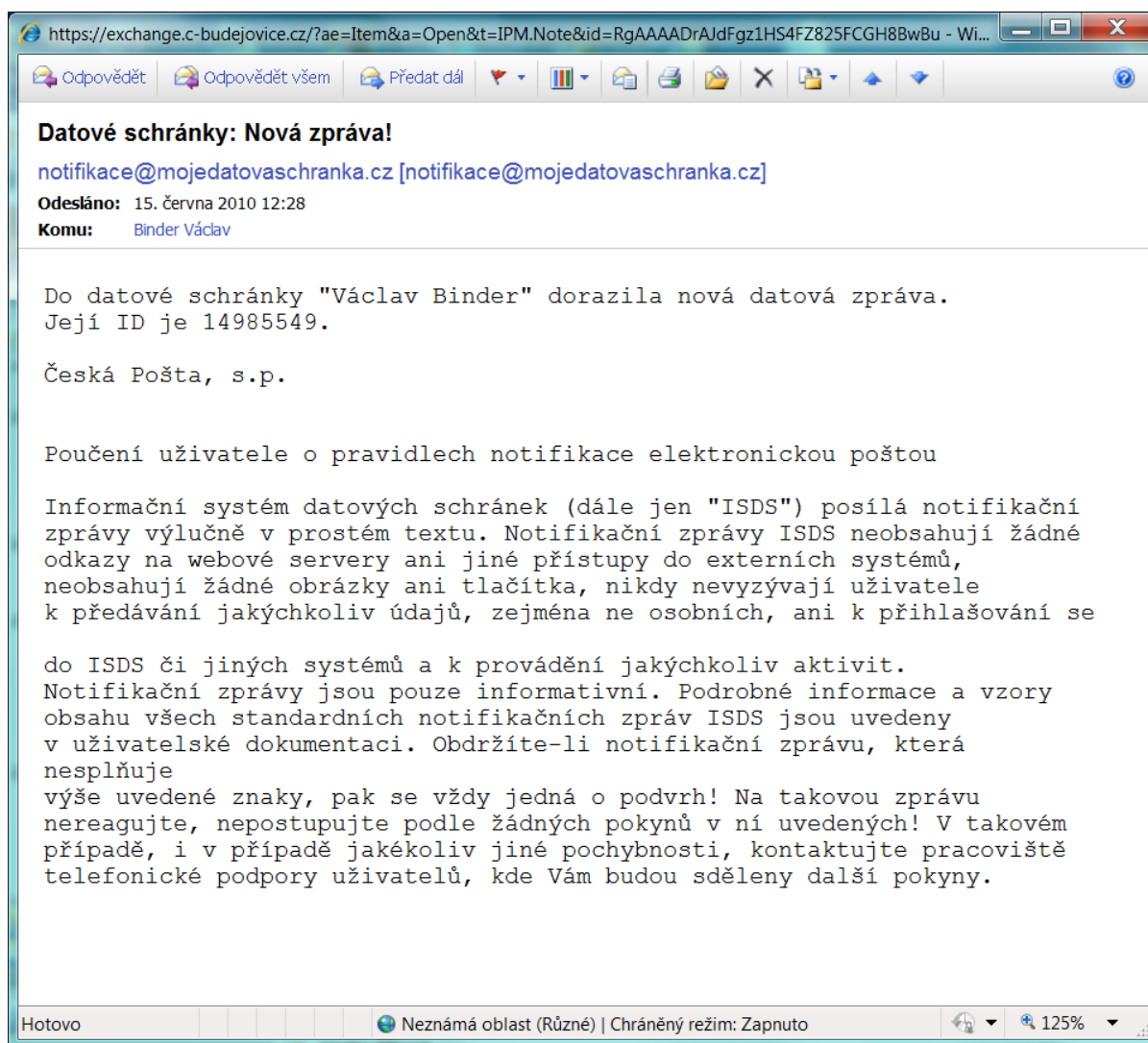
Pokud nepotřebuji ukládat koncept, stiskem tlačítka „Odeslat zprávu odešlu zprávu všem uvedeným příjemcům. Pokud odeslání proběhne v pořádku, systém nám to oznámí. Pokud nechci pokračovat v odeslání zprávy, operaci stornuji tlačítkem „Zavřít datovou zprávu“.

2.6.1.4 Oznámení o doručení zprávy

Po vstupu příjemce do DS nebo po 10 dnech, kdy nastane fikce doručení, se ve složce Odeslaných zpráv objeví u této odeslané zprávy doručenka s údaji o datu a čase doručení. Tuto je vhodné si uložit do počítače a zajistit její bezpečnou archivaci, neboť doručenka je součástí spisu.

2.6.2 Upozornění na doručené zprávy

Pokud jde o úřad malé obce, který nemá elektronickou spisovou službu, a zprávy nepřicházejí do datové schránky každý den, je vhodné využít možnost, kterou datová schránky nabízí a nastavit si upozorňování na zprávy došlé do DS emailem (bezplatná funkcionalita) nebo prostřednictvím SMS (služba je za úplatou). Upozornění na došlou zprávu do DS pak vypadá například takto:



2.6.3 Změny nastavení DS

Pokud jde o změny pověřených osob, případně rozsahu jejich oprávnění, může toto provést administrátor DS v sekci „Nastavení“. V případě, že oprávněná osoba, pověřená osoba nebo administrátor zapomene přístupové údaje k DS nebo má podezření na jejich kompromitaci, požádá administrátor nebo oprávněná osoba o zneplatnění stávajících údajů a vystavení nových. Tuto operaci je možné s výhodou provést na kontaktním místě CzP. Pokud dojde ke změně oprávněné osoby, tj. vedoucího orgánu veřejné moci (např.: z důvodu rezignace nebo odvolání) je potřeba aby nový

vedoucí orgánu veřejné moci nebo administrátor oznámil tyto skutečnosti Ministerstvu vnitra, které podle zákona 300/2008 Sb. §12 odst. (3) provede zneplatnění údajů původnímu vedoucímu OVM a vystavení nových pro nového vedoucího OVM. O zneplatnění přístupových údajů je rovněž možné požádat prostřednictvím kontaktního místa CzP.

2.7 Opatřování dokumentu časovým razítkem

Záležitost připojování časového razítka k dokumentu odesílanému do DS je poměrně složitá. Výklad zákona, který se touto problematikou zabývá tj. zákona 499/2004 Sb. v §69a není jednoznačný. Pravděpodobně z tohoto důvodu a dále zřejmě i z důvodu toho, že použití časového razítka je poskytovatelem této služby zpoplatněno, a že celkově by se mohlo jednat o ne nevýznamné finanční částky vydané za jeho užití, se časové razítko prakticky v úřadech dosud nepoužívá a to ani ve velkých úřadech, které provozují systémy elektronické spisové služby.

Pro vytvoření názoru na to zda časové razítko používat, je možné vycházet ze „Stanoviska odboru archivní správy a spisové služby k užívání časového razítka v souvislosti s odesíláním a ukládáním dokumentů v digitální podobě č.j. MV-3691-1/AS-2010“.

2.7.1 Ověření pravosti dokumentu

Podstatným konstatováním ze stanoviska je toto:

„Co se týče vlivu kvalifikovaného časového razítka na pravost dokumentu obsaženého v datové zprávě, konstatujeme, že absence kvalifikovaného časového razítka nečiní dokument nepravým, a neměla by tudíž ovlivnit jeho akceptaci orgánem veřejné moci či jiným subjektem. Přítomnost kvalifikovaného časového razítka na dokumentu obsaženého v datové zprávě je však nezbytným předpokladem toho, aby bylo možno na dokument aplikovat domněnku pravosti po celou dobu existence dokumentu, konstruovanou podle §69a odst. 8 Zákona č. 499/2004 Sb.“

2.7.2 Uchovávání dokumentů

Opatřování dokumentů v digitální podobě kvalifikovaným časovým razítkem je tedy důležité pro prokazování jejich pravosti po celou dobu existence. Souvisí také s uchováváním dokumentů v digitální podobě se zaručením jejich vlastností podle požadavků §69a odst. 3 zákona č. 499/2004 Sb., ve znění pozdějších předpisů. Aby si uchovávané dokumenty zachovaly požadované vlastnosti, je potřebné nejen je opatřovat všemi náležitostmi včetně kvalifikovaného časového razítka, ale také využívat k jejich zpracování a ukládání takový software pro zabezpečení spisové služby vedené v elektronické podobě v elektronických systémech spisové služby, který je schopen technickými prostředky takové vlastnosti zabezpečit. Nástrojem pro zaručení záznamů o všech operacích prováděných s dokumenty a jejich uchování je jeho součástí, tzv. transakční protokol.

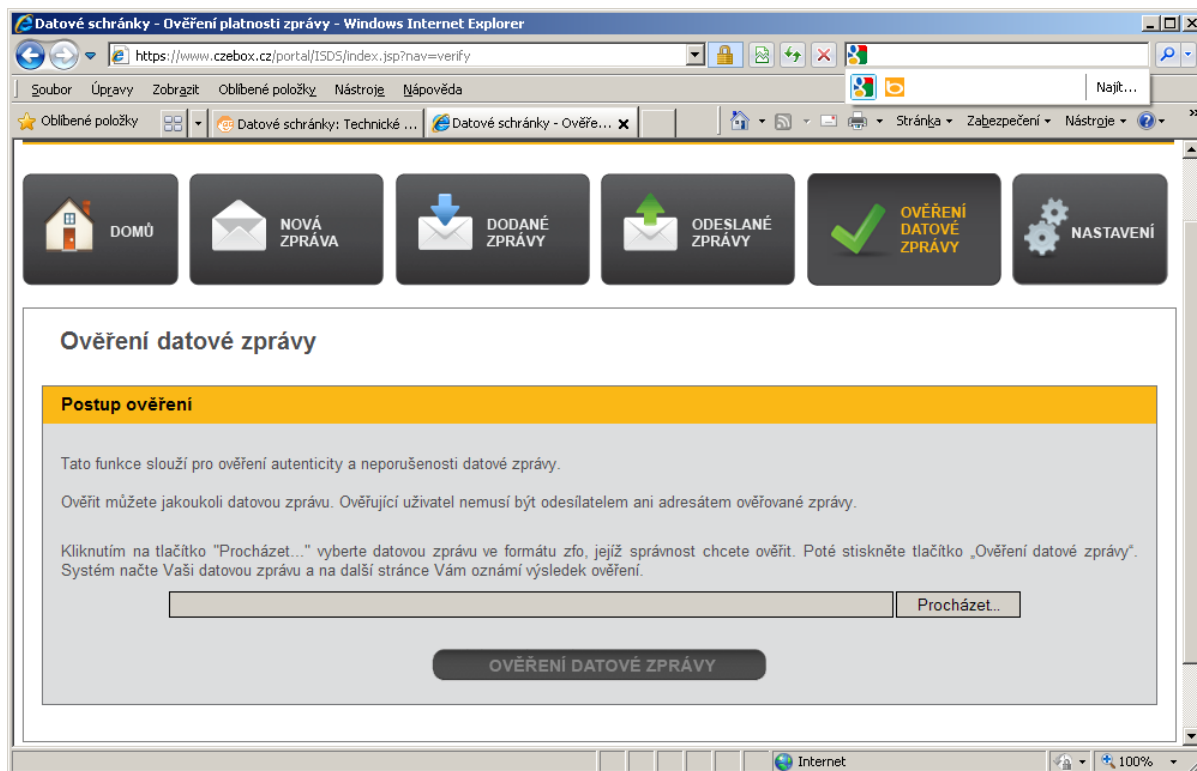
2.7.3 Opatřování dokumentu časovým razítkem

Z těchto konstatování lze odvodit, že by orgány veřejné moci měli digitální dokumenty vzniklé na úřadě, tak na úřad přijaté, pokud již časové razítko neobsahují, časovým razítkem opatřovat.

2.7.3.1 Úřad bez ESS

Pokud úřad nemá elektronickou spisovou službu, která připojování časového razítka má jako svou funkcionalitu, musí si na tuto operaci pořídit speciální software, který to zajistí. Takový produkt vytvořila a prodává např.: firma Software 602.

Pro ověření autentičnosti datové zprávy je připravena služba v ISDS, pomocí které si bude moci vlastník DS ověřit zda datová zpráva prošla ISDS a zda nebyla změněna. Tato funkce je již implementována v testovacím systému zkušebních datových stránek.



2.7.3.2 Úřad s ESS

Pokud je na úřadě provozovaná elektronická spisová služba je práce s DS odlišná. Žádný pracovník úřadu ani osoba oprávněná ani osoba pověřená nepřistupuje (kromě výjimečných případů – jako je změna hesla apod.) do datové schránky přímo. Do DS schránky se přihlašuje program elektronické spisové služby (ESS) prostřednictvím webové služby a ověření je provedeno pomocí „Systémovým certifikátu“ což je obdoba osobního certifikátu určená pro počítačové systémy a je potřeba nechat jej vystavit některou s akreditovaných certifikačních autorit. Administrátor DS pak v nastavení DS provede aktivaci systémového certifikátu.

Technický prostředek obecně, v tomto případě ESS musí splňovat technické požadavky uvedené ve vyhlášce 194/2009 Sb., o stanovení podrobností a provozování informačního systému datových schránek a v provozním řádu ISDS a vydavatel technického prostředku musí zveřejnit prohlášení o shodě použitých sad technických prostředků zveřejněných v provozním řádu ISDS. Tyto záležitosti zůstávají pro pracovníka neviditelné, jeho způsob práce v systému elektronické spisové služby se zavedením ISDS významně nezmění.

2.8 Práce s dokumenty v ESS

To podstatnou změnou je, že dokument je pouze v elektronické podobě a neexistuje k němu listinná podoba. Pokud dokument v papírové podobě je nutný a v některých případech tomu tak je, neboť stávající zákony ukládají vést spis v papírové podobě, je nutné elektronický dokument vytisknout, opatřit číslem jednacím a po jeho zpracování založit do spisu. Takový dokument má ovšem pouze informativní hodnotu, pokud by měl být použit pro jednání, v rámci něhož by bylo nutné ověřit pravost dokumentu, musí se použít pro konverzi do listinné podoby autorizovaná konverze. Autorizovaná konverze je jedna z funkcionalit systému Czechpoint, pro práci úřadu se využije jeho část CzechPoint&Office.

Pracovník úřadu zpracuje a vyhotoví v rámci řešeného případu všechny potřebné dokumenty, včetně příloh stejným způsobem v případě že dokument bude vypraven z úřadu klasickou poštou nebo do DS příjemce. To znamená, že dokumenty vytváří elektronicky v programové aplikaci, kterou úřad používá např. Microsoft Office. Vzhledem k tomu, že existuje a na úřadech je využíváno několik systémů ESS od různých dodavatelů, liší se práce s dokumenty a se spisy podle konkrétních vlastností toho kterého programu. Principy práce se spisovou službou jsou ovšem shodné a v dalším textu budeme práci v programu ESS popisována obecně bez ohledu na konkrétní programový produkt.

2.8.1 Vytvoření dokumentu v ESS

Pracovník v systému ESS založí dokument a příslušný spis. Pakliže je práce na dokumentu ukončena doplní přílohy. Postup práce se nyní bude lišit podle toho, zdali příjemce vlastní datovou schránku a jestli povaha dokumentu umožňuje odeslání do DS. Pokud nejsou obě tyto podmínky splněny, pracovník všechny materiály následně vytiskne, zkompletuje a připraví k podpisu oprávněnému pracovníkovi. Vedoucí pracovník dokument vlastnoručně podepíše, pracovníce na spisovém uzlu vytiskne obálky s adresou příjemce a čárovým kódem. Dokument pak v systému spisové služby předá k vypravení, čímž se dokument přesune na spisový uzel – podatelna. Současně fyzicky předá obálky s dokumenty na podatelnu. Pracovníce na podatelně obálky ofrankují, pomocí čtečky čárového kódu se načtou obálky a označí příslušné dokumenty určené k odvozu na poštovní úřad v programu ESS a tím je dokument v evidenci označen jako vypravený.

2.8.2 Příprava dokumentu k odeslání

Pokud příjemce má DS a povaha dokumentu umožňuje odeslání dokumentu do DS je povinností OVM tak učinit. Tento způsob odeslání je podle zákona přednostní. Aby bylo možné dokument jako celek odeslat do DS musí být kompletně včetně všech příloh v digitální podobě. To znamená, pokud některá z příloh existuje pouze v listinné podobě, je nutné ji digitalizovat, to znamená naskenovat a převést do některého z formátů, které jsou povolenými formáty pro odesílání do DS. V rámci programu spisové služby je potřebné vyhledat ID datové schránky adresáta, případně adresátů, pokud je stejný dokument odeslán více příjemcům. ESS toto provádí spojením s ISDS přes webovou službu. Postupně se vytváří v ESS interní adresář příjemců a ID jejich datových schránek. Protože může dojít k zneplatnění DS, je toto nutno vždy v existenci DS ověřovat.

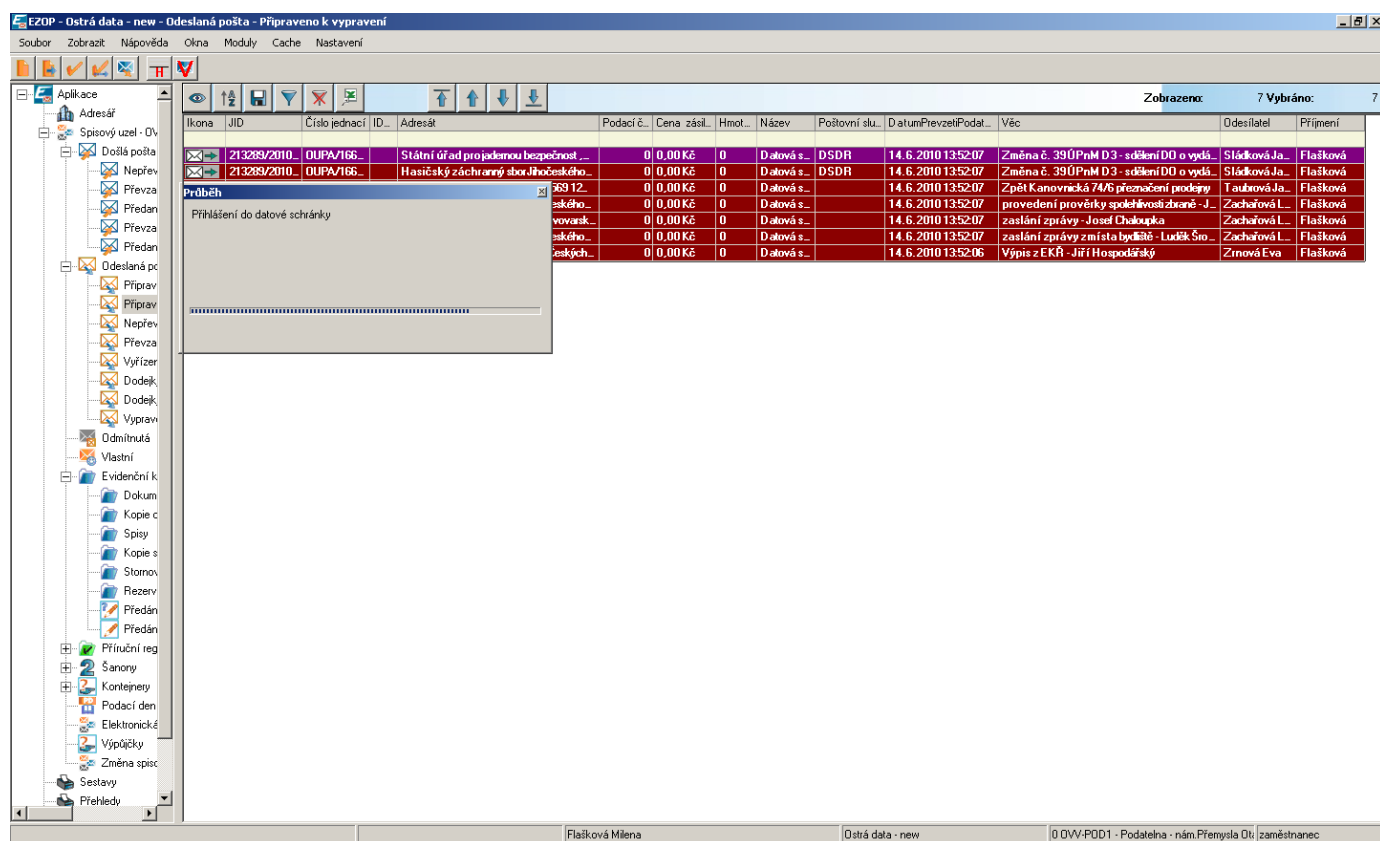
Další operací, kterou pracovník provede je převedení hlavního dokumentu do formátu pdf/A. Pokud je sám oprávněn k podepsání, dokument současně elektronicky podepíše, pokud ne předá nadřízenému pracovníkovi. Nadřízený pracovník v programu ESS otevře složku označenou např.: Určeno k podpisu, v ní obsažené dokumenty přečte, a pokud souhlasí s obsahem stiskem tlačítka, připojí

elektronický podpis. Pokud není s obsahem spokojený, odešle zpět zpracovateli. Podepsané dokumenty v programu ESS pracovníce na spisovém uzlu odešle podepsané dokumenty k vypravení, čímž se přesunou na spisový uzel – podatelna. Každý pracovník s právem podpisu musí mít pořízen osobní kvalifikovaný certifikát u některé z akreditovaných certifikačních autorit. Tento certifikát musí být uložen v systému ESS a na základě přihlášení do programu je pak využit pro vytvoření elektronického podpisu.

2.8.3 Činnost spisového uzlu při práci s ISDS

Činnost spisového uzlu podatelna při práci se ISDS je následující: pracovníce na podatelně několikrát denně podle vnitřních předpisů a směrnic úřadu OVM spustí komunikaci ESS s ISDS. Program se prostřednictvím webové služby spojí s ISDS a provede:

1. odeslání všech dokumentů připravených k vypravení do DS.
2. Stažení všech nových zpráv došlých do DS od doby poslední komunikace s DS.
3. Stažení všech doručenek došlých k odeslaným zprávám od posledního načtení.



2.8.4 Pošta zasílaná mezi odbory jako dotčenými orgány

Jedná se o poštu, která je předávána mezi odbory téhož úřadu samosprávy (obecní, městské, magistrátní a krajské úřady), které k sobě mají vztah jako dotčené orgány (vystupují vůči sobě jako externí partneři).

Protože v ISDS není možné poslat přes datovou schránku dokument do téže datové schránky (sám sobě), bylo by toto věc možné řešit žádostí o „zřízení další datové schránky orgánu veřejné moci“, s tím že by první datová schránka sloužila odborům samosprávy a druhá pro odbory vykonávající státní správu v přenesené působnosti. To by ovšem naráželo na problém, který by vznikl, pro vnější

odesílatele, kteří by museli rozlišit, zda se jedná o samosprávný odbor nebo odbor vykonávající státní správu. Tuto znalost běžně občané ani firmy nemají a dokumenty by chodily do nesprávných datových schránek.

Proto je tato věc řešena v rámci spisové služby úřadu a dokumenty zasílané mezi odbory téhož úřadu přes ISDS neprocházejí. Z jednoho odboru je dokument vypravován přes podatelnu a na odboru příjemce je dokument zaevidován jako nový externí dokument došlý do organizace (eviduje podatelna). Přestože dokument ve skutečnosti neopustí úřad je odesílatelem označen jako dokument vypravený podatelnou a podatelna jej vypraví jako externí dokument. Protože adresátem je vnitřní odbor úřadu neopustí dokument úřad, ale je označen jako externí přijatý dokument a objeví se v došlé poště odboru příjemce.

2.8.5 Systémové zprávy ISDS

Součástí došlých zpráv jsou i „Systémové zprávy ISDS“. Tyto obvykle obsahují informaci o tom, že odeslaná zpráva nebyla z nějaké příčiny, obvykle porušení pravidel o obsahu a formátu odeslané zprávy doručena. U takových zpráv pracovníce podatelny musí přečíst obsah zprávy, vyhledat v složce Odeslaná pošta/Vypraveno do DS zjistit odesílající odbor nebo odesílatele a systémovou zprávu mu předat.

2.8.6 Vybrané problémy při práci s doručeními DZ

S došlými zprávami z DS pracovníce podatelny dále pracují. Každou zprávu musí otevřít, zjistit adresáta a následně zprávu předat na příslušný spisový uzel. Pokud je zpráva označena „do vlastních rukou“ a současně je uvedeno „k rukám“ jméno konkrétního pracovníka, zprávu neotvírají a předají ji na spisový uzel. Velmi často má zpráva příznak do vlastních rukou a v položce k rukám není nic uvedeno. Tím se dostává pracovník podatelny do situace, kdy nezná adresáta a přitom by zprávu neměl otevřít, aby jej mohl zjistit. Všechny takové zprávy by měli být odeslány zpět odesílateli jako nedoručitelné. Vzhledem k četnosti takto chybně označených zpráv je praxe taková, že pracovník podatelny příjemce zjistí a zprávu mu předá. Dalším poměrně častým jevem na rozdíl od klasické pošty je, že stejná zpráva přijde do DS opakovaně.

Proč se tak děje může být z důvodu chyby programu ESS na straně odesílatele, nebo si pracovník není jistý, zda zprávu poslal a pošle ji znovu „pro jistotu“. Rovněž přicházejí zprávy, které na příslušný úřad nepatří, nebo úřad není příslušný konkrétní záležitost řešit. Takové zprávy se obvykle prostřednictvím jednoho určeného spisového uzlu zasílají odesílateli zpět nebo se přeposílají na úřad věcně příslušný. Jinou chybou je, že hlavní dokument není elektronicky podepsán. To pracovníce podatelny předají příjemci a ten to pak řeší obvykle vrácením zprávy, s tím že nemá potřebné náležitosti. Zdůrazněme, že v tomto případě se jedná o orgán veřejné moci.

Další chybou v došlých zprávách je, že zpráva přijde pouze jednou, přestože podle rozdělovníku je určena více příjemcům. Toto se řeší upozorněním odesílatele.

2.9 Statistika vývoje komunikace přes DS

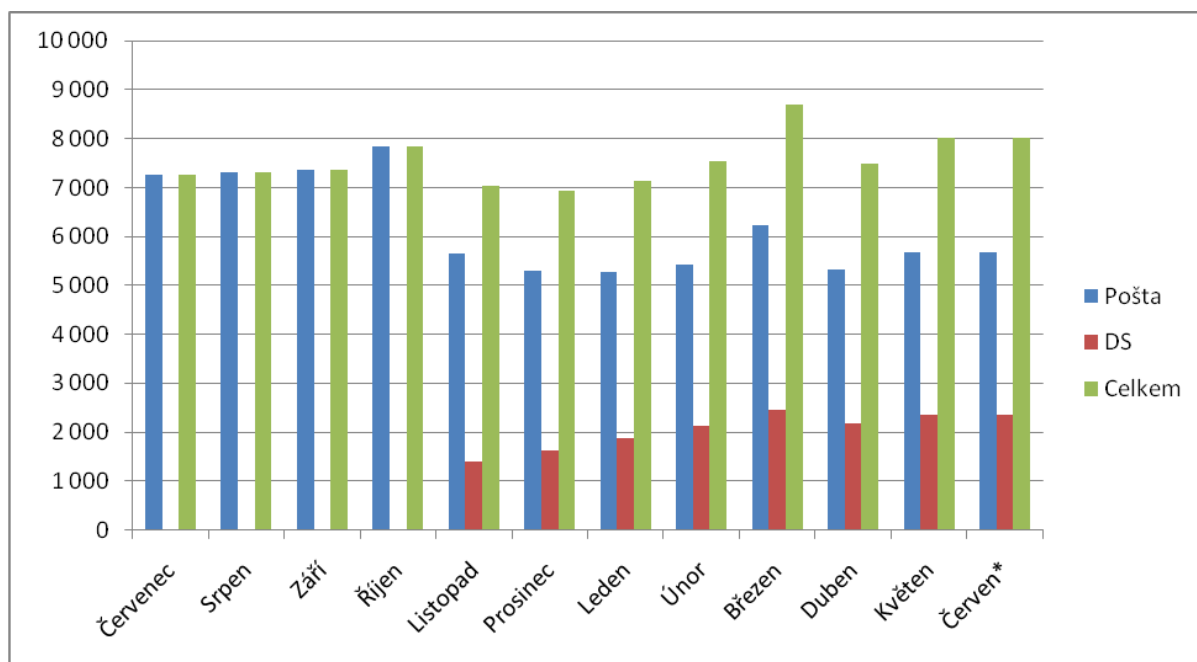
Pro ilustraci jsou uvedeny údaje z magistrátního úřadu menšího statutárního města. Z následujících tabulek je patrný vývoj nárůstu počtu zpráv došlých a odeslaných přes DS.

Je vidět poměr mezi klasickou došlou a vypravovanou poštou a DS. Zajímavé jsou i údaje o čase potřebném ke zpracování datových zpráv.

2.9.1 Přehled přijaté pošty

2009/10	Pošta	DS	CELKEM
Červenec	7 261	x	7 261
Srpen	7 301	x	7 301
Září	7 373	x	7 373
Říjen	7 833	x	7 833
Listopad	5 646	1 389	7 035
Prosinec	5 307	1 616	6 923
Leden	5 272	1 864	7 136
Únor	5 428	2 120	7 548
Březen	6 234	2 462	8 696
Duben	5 318	2 181	7 499
Květen	5 668	2 353	8 021
Červen*	5 668	2 353	8 021

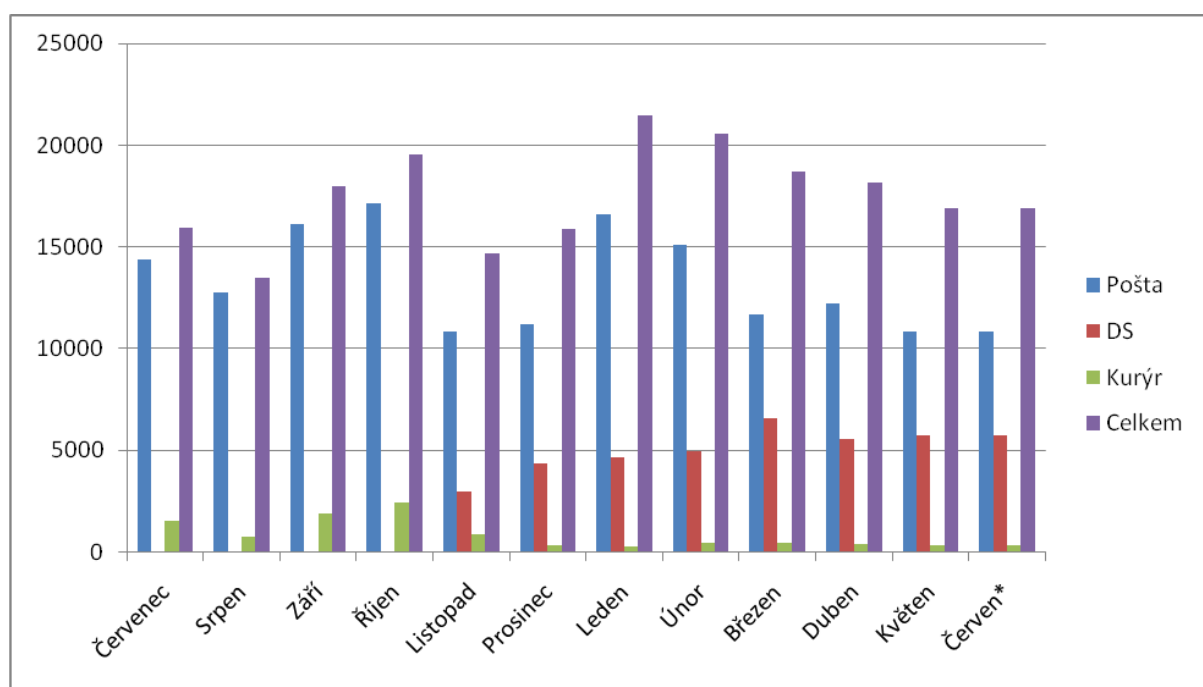
*) údaje za červen jsou neúplné



2.9.2 Přehled vypravené pošty

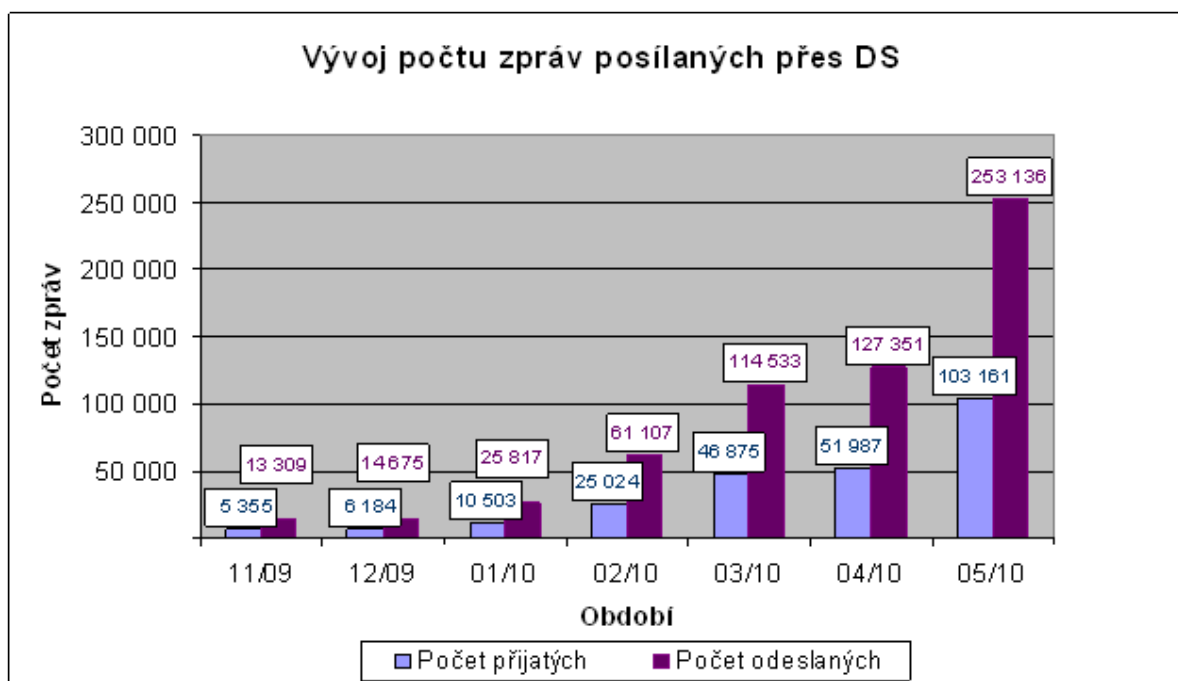
2009/10	Pošta	Datové schránky	Kurýr	CELKEM
Červenec	14377	x	1543	15920
Srpen	12752	x	730	13482
Září	16115	x	1881	17996
Říjen	17125	x	2409	19534
Listopad	10847	2973	885	14705
Prosinec	11171	4376	314	15861
Leden	16573	4626	253	21452
Únor	15120	4972	449	20541
Březen	11684	6546	465	18695
Duben	12205	5552	380	18137
Květen	10822	5741	343	16906
Červen*	10822	5741	343	16909

*) údaje za červen jsou neúplné



2.9.3 Časová náročnost zpracování došlých a odeslaných DZ

11/2009- 05/2010	Došlé zprávy do DS				Odeslané zprávy do DS		
	Počet (ks)	Doba stahování (min.)	Celk. doba zpracování (min.)	Průměr na 1 zprávu (min.)	Počet (ks)	Celk. doba zpracování (min.)	Průměr na 1 zprávu (min.)
11/09	5 355	3 294	13 899	2,60	13 309	1 790	0,13
12/09	6 184	3 669	15 804	2,56	14 675	1 951	0,13
01/10	10 503	6 401	27 127	2,58	25 817	3 475	0,13
02/10	25 024	15 218	64 618	2,58	61 107	8 257	0,14
03/10	46 875	28 461	120 884	2,58	114 533	15 452	0,13
04/10	51 987	31 637	134 213	2,58	127 351	17 154	0,13
05/10	103 161	62 751	266 271	2,58	253 136	34 077	0,13



2.9.4 Shrnutí statistik

Z tabulek a grafů je patrné, že dochází k nárůstu počtu zpráv, které prochází pře DS. Trend je takový, že dochází k celkovému nárůstu korespondence mezi úřadem a vnějšími subjekty. Výrazně narostl počet zpráv prošlých DS a v poměru k tomu poklesl počet zpráv došlých a odeslaných prostřednictvím pošty. Relativně vysoký podíl přes poštu došlých (přibližně 2/3) a přes poštu vypravených (asi 1/2) dopisů, je dán tím, že část korespondence mezi orgány veřejné a právníckými osobami a především ve vztahu k fyzickým osobám – občanům musí být vyhotovována a odesílána v listinné podobě. Ale i část korespondence mezi orgány veřejné moci navzájem probíhá stále v listinné podobě klasickou poštou. Jde především o korespondenci se soudy a orgány policie, kde existují specifické okolnosti, např. důkazní materiály nebo velký rozsah spisu.

Podle celostátních statistik odeslali uživatelé do dubna 2010 10 miliónů datových zpráv. Nevyzvednutých zpráv do 10 dnů od dodání do DS jsou 4%.

3 DS z pohledu Právnícké osoby

Právnícké osobě zapsané v obchodním rejstříku byla zřízená DS ze zákona a aktivovaná 1. 11. 2009. Od toho dne mohly přicházet a přicházely do DS zprávy od OVM. Vzhledem k nepřesným a neúplným údajům v obchodním rejstříku neobdrželi přihlašovací údaje k DS vždy statutární zástupci právnických osob nebo je obdrželi na nesprávnou adresu. Tento stav se postupně napravil, takže se nakonec dostaly přihlašovací údaje ke správným osobám. Jsou podstatné rozdíly mezi jednotlivými společnostmi, pokud jde o velikost. Práce se systémem DS a digitální podobou dokumentů obecně vyžaduje určité technické a personální zajištění. Velké firmy mají kvalitní informační a komunikační prostředky, odbornou správu těchto systémů, zkušené a zaškolené pracovníky, kteří jsou zvyklí pracovat s počítačovými informačními systémy. Tyto firmy používají obvykle elektronickou spisovou službu a programy pro správu dokumentů (DMS). Mnohé z nich již provozovaly systémy elektronické výměny zpráv se svými partnery a dodavateli, obdobně k ISDS.

U menších firem je tomu právě naopak. Jen někteří pracovníci mají k dispozici výpočetní techniku, programové prostředky jsou zastaralé, připojení k internetu pomalé a nespolehlivé. Pokud jde o správu počítačů a softwaru děje se tak formou nakupované služby, tito odborní pracovníci jsou povoláni jen v případě poruchy nebo jiného problému. Rovněž systém zaškolování pracovníků nebývá na dostatečné úrovni. Pro takový typ firmy přináší komunikace přes DS určité problémy. Technické nedostatky je možné vyřešit inovací výpočetní techniky, nainstalováním potřebného softwaru, provedení upgradu stávajícího. Případně zajištění dostatečně rychlého a spolehlivého připojení k síti internet. Větším problémem je při absenci elektronické spisové služby nalezení vhodného způsobu práce s elektronickými dokumenty. Proto je potřeba vytvořit bezpečné, spolehlivé a zálohované úložiště pro datové zprávy došlé do DS. Často to v malých firmách, pokud frekvence zpráv došlých do DS není velká, řeší tak, že prostřednictvím Czechpointu provedou autorizovanou konverzi z elektronické do listinné podoby a s dokumentem v listinné podobě již nakládají podle stávajících zvyklostí.

3.1 Komunikace prostřednictvím ISDS s OVM

Právnícké osoby komunikují s OVM prostřednictvím DS pokud OVM o to přímo požádají, jako např. finanční úřady. Pokud OVM pošle zprávu do DS právnické osobě pak i tato obvykle odpoví prostřednictvím DS. V ostatních případech právnické osoby preferují papírovou korespondenci. Pokud právnická osoba chce využít DS ke komunikaci s OVM může tak učinit, aniž by statutární zástupce připojoval k digitálnímu dokumentu elektronický podpis. Stačí hlavní dokument převést do formátu pdf 1.3 a vyšší.

Lze ale doporučit, aby i vzhledem k zanedbatelným nákladům na pořízení osobního kvalifikovaného certifikátu a softwaru, který umí vytvořit elektronický podpis, si statutární zástupci právnických osob kvalifikovaný certifikát pořídili a zprávy odesílané přes DS elektronicky podepisovali. Posílí tím autentičnost a nepopíratelnost pravosti dokumentu.

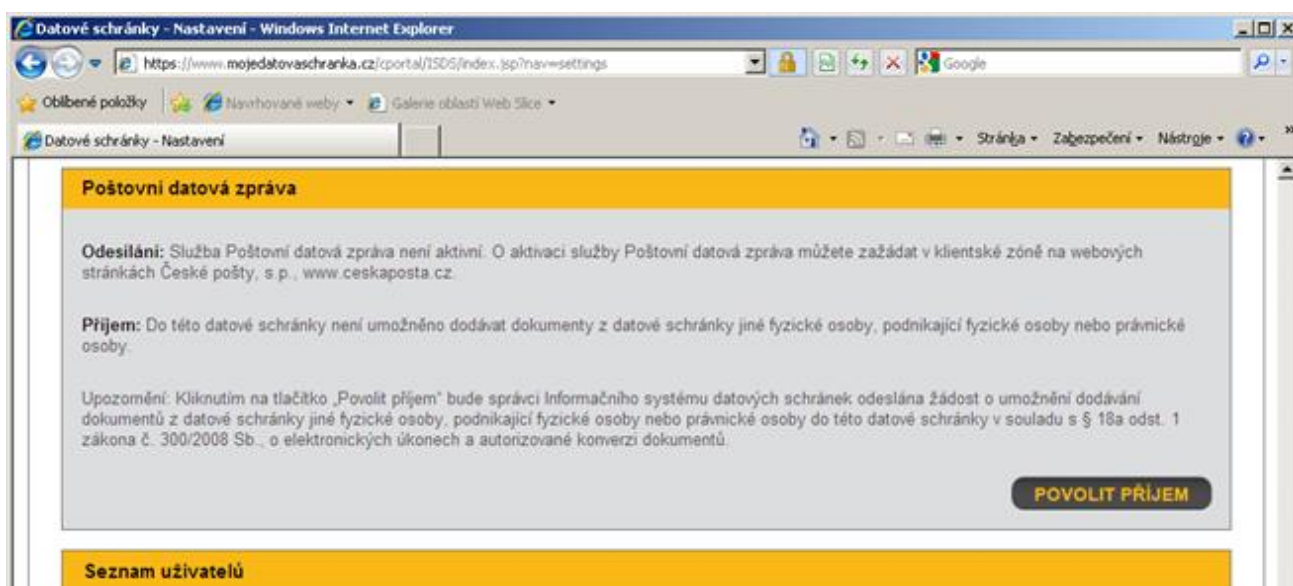
3.2 Komunikace prostřednictvím ISDS mezi PO

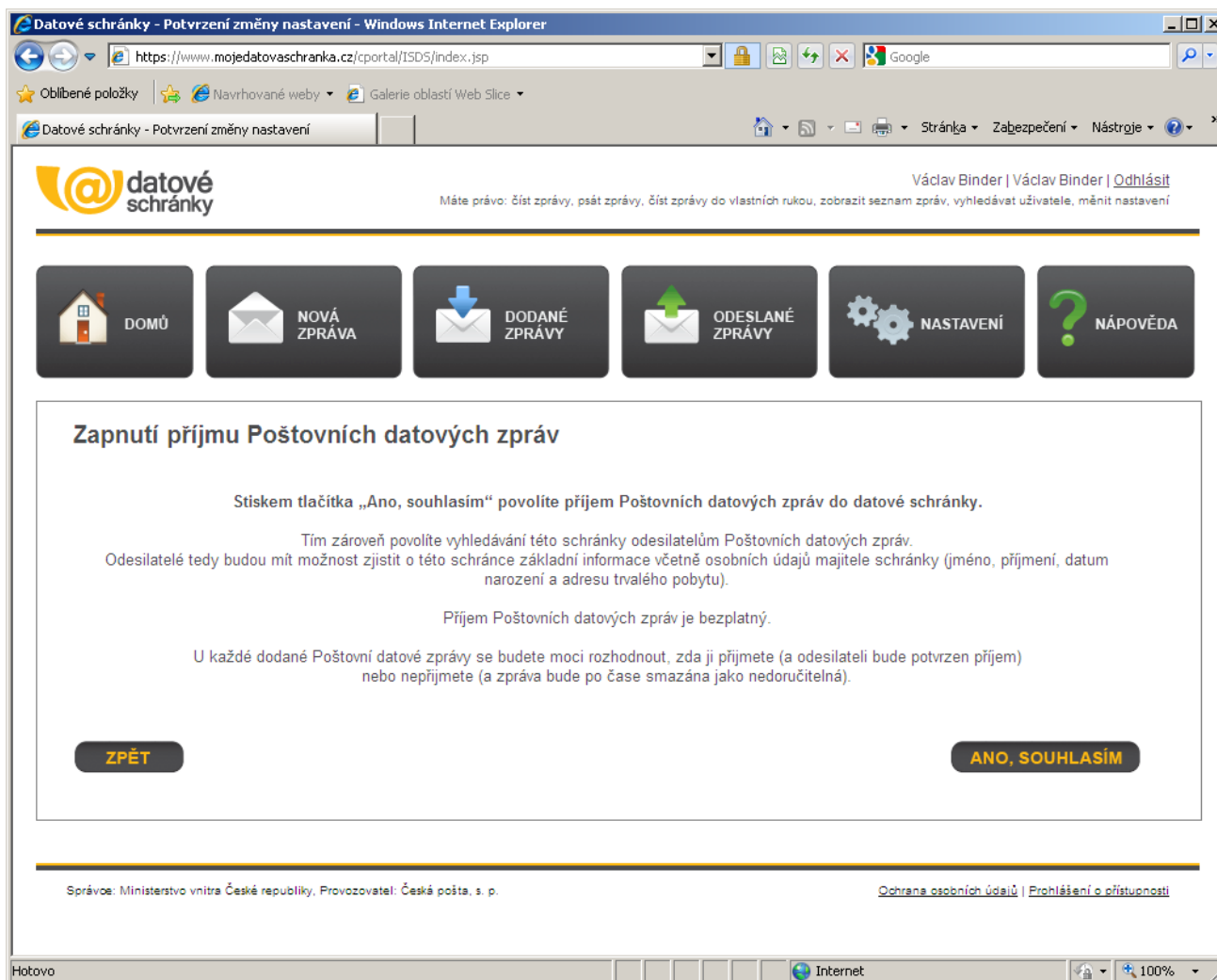
Využitelnost elektronického podpisu se ještě zvýší tím, že od 1. 7. 2010 je již možná komunikace přes DS i mezi právníckými a fyzickými osobami navzájem, bez omezení obsahu zprávy. Od 1. 11. 2009 bylo možné posílat a přijímat zprávy prostřednictvím DS jen ve vztahu k OVM. Od 1. 1. 2010 pak i mezi právníckými osobami mezi sebou v omezeném rozsahu dokumentů platebního styku (faktur).

3.3 Poštovní datová zpráva

Od 1.1 2010 zavedla Česká pošta s. p. v rámci Informačního systému datových schránek novou službu s názvem Poštovní datová zpráva. Odesílání Poštovní datové zprávy je zpoplatněno. Cena se skládá z měsíčního paušálu a z částky zaplacené za každou datovou zprávu. Aktivace služby se provádí plně elektronicky na internetových stránkách České pošty v Klientské zóně na adrese www.ceskaposta.cz.

Příjem Poštovní datové zprávy je zdarma. Nejdříve je však zapotřebí aktivovat tuto službu v uživatelském nastavení vlastníka datové schránky. To se provede v nastavení DS.





4 DS z pohledu FO a PFO

Fyzická osoba a fyzická osoba podnikající si musí o zřízení DS požádat.

4.1 Žádost o zřízení DS

Žádost o zřízení Datové schránky lze podat následujícími způsoby:

- Na kontaktním místě veřejné správy (pracoviště Czech POINT) V tomto případě není nutné žádost opatřovat úředně ověřeným podpisem (viz Zákon 300/2008 Sb. §27 Odst. 2)
- Vyplněním elektronického formuláře žádosti, jeho podepsáním zaručeným elektronickým podpisem a následným odesláním na e-podatelnu Správce (posta@mvcz.cz) Formulář žádosti je na webu www.datoveschranky.info
- Vyplněním formuláře žádosti, jeho vytištěním, opatřením ověřeným podpisem a zasláním na poštovní adresu Správce.

4.2 Zřízení DS na žádost

Pokud žádost obsahuje všechny zákonné náležitosti a zároveň (v případě fyzické osoby a podnikající fyzické osoby) byla osoba žadatele jednoznačně identifikována v databázi evidence obyvatel, Správce

zřídí Datovou schránku do 3 pracovních dnů od přijetí žádosti. Přístupové údaje jsou následně žadateli zaslány poštovní zásilkou do vlastních rukou .

Od toho okamžiku může fyzická osoba využívat systém datových stránek. V nastavení datové schránky může přidat další uživatele ve funkci administrátora nebo pověřené osoby a nastavit jim oprávnění v tomto rozsahu:

- Číst zprávy
- Číst zprávy určené do vlastních rukou
- Vytvářet a odesílat datové zprávy
- Prohlížet seznam dodaných zpráv i doručenek
- Vyhledávat datové schránky

4.3 Nastavení DS

Může si nastavit zaslání upozornění na došlé zprávy do DS emailem nebo SMS. Nastavit bezpečné přihlašování pomocí certifikátu. Nastavit přijímání poštovních zpráv, což mu umožní přijímání poštovních datových zpráv od právnických a fyzických osob.

Mimo systém DS si může objednat dolňkovou službu Datový trezor, nebo zaslání Poštovní datové správy – obě služby jsou zpoplatněny.

Po nastavení datové schránky je možné ji používat. Určitě budou do datové schránky přicházet zprávy od OVM, protože těm to ukládá zákon. Pokud má fyzická osoba nastaveno přijímání poštovních datových zpráv může dostávat zprávy i od jiných fyzických nebo právnických osob pokud mají DS a zprovozněnou službu zaslání poštovních datových zpráv.

4.4 Využitelnost DS

Využitelnost DS pro fyzické osobu odvisí od toho jak častý je její písemný styk s OVM. Pokud je častý, má tento pohodlný rychlý, kdekoliv ve světě mimo místo trvalého bydliště dostupný způsob komunikace, své nesporné výhody. Naproti tomu přináší určitou zátěž spojenou s bezpečnou archivací došlých zpráv a rizikem jejich ztráty, která je oproti papírovým dokumentum vyšší.

Využitelnost DS pro fyzické osoby je zejména odvislé od toho jak rychle zaimplementují OVM do svých datových stránek formulářová řešení, tak aby bylo možné různá podání na úřady vyplnit přímo na webu, včetně logických kontrol správnosti a úplnosti a následně je odeslat do DS.

4.5 Znepřístupnění DS

Pokud fyzická osoba zjistí, že ji používání DS nevyhovuje může požádat o její znepřístupnění.

4.6 Testovací prostředí ISDS

Pro otestování způsobu práce s datovou schránkou je možné využít „Zkušebního prostředí informačního systému datových stránek“. Na adrese <http://www.datoveschranky.info> je možné

zažádat o zřízení testovací datové schránky. V té si pak v určitém omezeném rozsahu může uživatel ověřit funkčnost a způsob práce s ISDS.

5 Závěr

V tomto modulu jsme se Vám snažili přiblížit Informační systém datových schránek a veškeré souvislosti se zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Získali jste teoretické informace o legislativě ISDS a praktické informace o práci se všemi typy datových schránek.