Projekt implementace technologie datových schránek ve firmě Bioveta a. s.

Project implementation technology data boxes in the company Bioveta a. s.

Bc. Ladislav Štěpánek

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Bc. Ladislav ŠTĚPÁNEK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Projekt implementace technologie datových schránek ve firmě Bioveta a.s.**

Zásady pro vypracování:

1. **Proveďte průzkum informačních zdrojů k danému tématu a proveďte jeho literární rešerši.**
2. **Popište současný stav a proveďte analýzu současných způsobu řešení datových schránek.**
3. **Porovnejte dnes nabízená řešení.**
4. **Realizujte zvolené řešení a toto diskutujte.**
5. **Vyslovte závěry týkající se implementace a zadání práce.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1. vyd. Brno : Computer Press, 2006. 534 s. ISBN 80-251-0828-7.**
2. **SMEJKAL, Vladimír. Datové Schránky v Právním Řádu ČR. 1. vyd. Praha : ABF a.s., 2009. 176 s. ISBN 978-80-86284-78-1.**
3. **MACKOVÁ, Alena, ŠTĚDROŇ, Bohumír. Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem včetně souvisejících zákonů a prováděcích předpisů. 1. vyd. Praha : Wolters Kluwer, 2009. ISBN 978-80-7357-472-7.**
4. **ATREYA, Mohan, HAMMOND, Ben, PAINE, Stephen. Digital Signatures. 1. vyd. Londýn : McGraw-Hill, 2002. 368 s. ISBN 9780072194821.**
5. **MAO, Wenbo. Modern Cryptography – Theory & Practice. New Jersey : Prentice-Hall, 2003. 1. vyd. 648 s. ISBN 0-13-066943-1.**
6. **BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Olomouc : ANAG, 2008. 157 s. ISBN 978-80-7263-465.**
7. **LIDINSKÝ, Vít, ŠVARCOVÁ, Ivana, BUDIŠ, Petr, LOEBL, Zbyněk, PROCHÁZKOVÁ, Barbora. eGovernment bezpečně. 1. vyd. Praha : Grada, 2008. 160 s. ISBN 978-80-247-2462-1.**
8. **Oficiální informace o datových schránkách od Ministerstva vnitra ČR. [online]. 2010 [cit. 2010-3]. Dostupné na WWW: http://www.datoveschranky.info/.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je navrhnout a popsat implementaci datových schránek ve společnosti Bioveta a. s. V teoretické části práce je podrobná literární rešerše týkající se datových schránek. V praktické části práce je probrána současná implementace datových schránek ve společnosti. Dále jsou zde popsána dnes nabízená řešení implementace datových schránek a jejich možnosti využití. V práci je také vysvětlen současný stav nakládání s dokumenty ve společnosti a v důsledku toho navrhnuté řešení v podobě zavedení systému pro správu dokumentů obsahujícího i funkcionalitu pro obsluhu datových schránek.

Klíčová slova: datová schránka, certifikát, systém pro správu dokumentů.

ABSTRACT

The aim of this thesis is to draft and describe implementation of data boxes in Bioveta a. s. Theoretical part of the thesis deals in detail with literature research related to data boxes. The practical part describes current implementation status of data boxes in Bioveta a. s. and also describes possible solutions available today, for implementation of data boxes and their usage. The thesis also provides information on up to date document management system. It also suggests solution for implementation of document management system including functionality for data box support.

Keywords: data box, certificate, document management system.

Poděkování

Tímto bych chtěl poděkovat vedoucímu své diplomové práce panu doc. Mgr. Romanu Jaškovi, Ph.D. za jeho rady a trpělivé vedení mé práce. Dále pak své rodině za finanční i psychickou podporu za celou dobu mého studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Spuštění projektu datových schránek představuje významný milník v oblasti elektronizace české stání správy. Tento významný krok však má být prospěšný také běžným občanům a firmám, kterým má napomoci k časové a finanční úspoře a také ke snížení administrativní zátěže. Občané a firmy mohou díky datovým schránám jednat se státními orgány (a od letošního roku také mezi sebou navzájem) přímo ze svých kanceláří či domovů. Nemusí už tedy například kvůli daňovému přiznání stát ve frontě s ručně vyplněným formulářem na finančním úřadě, nebo běhat na poštu kvůli odeslání listinné odpovědi na nějaký úřední dotaz. Nyní jim stačí přihlásit se do své datové schránky a jednoduchým způsobem danému úřadu či osobě odpovědět elektronicky.

Projekt datových schránek však není tak ideální, jak by se na první pohled mohlo zdát. Od začátku ho provází různé komplikace. Příčinou těchto komplikací je zřejmě to, že tento projekt je ve své podstatě revoluční, nikde na světě zatím nebyl realizován takto rychlý přechod od listinné komunikace na elektronickou a ještě k tomu povinně pro více než půl milionu subjektů v České republice. Dalším důvodem je krátká doba přípravy všech zúčastněných stran před spuštěním tohoto projektu. Jednak je to technologická nepřipravenost samotného systému datových schránek, různé věci jsou implementovány a měněny za chodu. Daly by se uvést například věci týkající se časových razítek, která byla původně povinná, poté nikoliv a nakonec jsou zase povinná, nebo ověření integrity elektronicky podepsaného dokumentu a jeho následná autorizovaná konverze, případně otázky týkající se bezpečnosti přístupu k systému datových schránek. Dále pak nedořešené legislativní věci, ne vše co se týká datových schránek je v zákonech přesně a srozumitelně definováno. Postupem času jsou ale tyto věci nakonec úspěšně řešeny a datové schránky se stávají použitelnějšími.

Tématem této diplomové práce je implementace datových schránek ve společnosti Bioveta a. s. Jedná se o středně velkou českou firmu zabývající se zejména výrobou veterinárních léčiv. V tomto dokumentu bude podrobně popsána legislativa a princip fungování datových schránek. Bude zde vysvětlena současná implementace datových schránek v této společnosti a podrobněji vysvětlena struktura této společnosti. Popsány budou také v dnešní době nabízená řešení implementace datových schránek. Bude zde také přihlédnuto ke zvyšující se administrativní zátěži v této společnosti spojené s rostoucím množstvím oběhu listinné komunikace uvnitř společnosti.

V závěru práce tedy bude navrhnuto zavedení systému pro správu dokumentů, který by měl tuto skutečnost vyřešit. Tento systém by v sobě měl mít zahrnutu funkcionalitu pro obsluhu datové schránky, řízení oběhu dokumentů z této schránky a nastavení přístupových práv jednotlivým uživatelům. Tato práce by měla sloužit také vedení společnosti jako návod pro realizaci tohoto přechodu (od oběhu papírové dokumentace k elektronickému oběhu dokumentů).

I. TEORETICKÁ ČÁST

1 ZÁKONY UPRAVUJÍCÍ KOMUNIKACI POMOCÍ DATOVÝCH SCHRÁNEK

V této kapitole uvádím stručný přehled právních předpisů, které upravují povinnosti a chování při elektronické komunikaci pomocí datových schránek.

1.1 Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů a o změně některých zákonů, ve znění pozdějších předpisů.

Tento zákon vstoupil v účinnost dne 1. 7. 2009 a pojednává o informačním systému veřejné správy, který upravuje elektronické úkony a autorizované konverze dokumentů prostřednictvím datových schránek. Definuje samotný pojem datová schránka. Určuje také kdo může a kdo musí mít zřízenou datovou schránku. Určuje osoby oprávněné k přístupu do datové schránky, definuje přístupové údaje k datové schránce, zpřístupnění a znepřístupnění datové schránky, podmínky pro zrušení datové schránky, doručování prostřednictvím datové schránky, konverzi a v neposlední řadě také informační systém datových schránek.

1.2 Zákon č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona č. 300/2008 Sb.

Tento zákon novelizoval dva předpisy a to zákon č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a zákon č. 150/2002 Sb., soudní řád správní. V prvním zákoně uvádí, že jednou z možností doručování písemností v exekučním řízení je také doručení do datové schránky a také dovoluje exekutorům provádět autorizovanou konverzi dokumentů. V druhém zákoně stanoví, že při doručování písemností se přednostně doručuje do datové schránky; není-li to možné, doručuje se stejně jako dosud.

1.3 Vyhláška č. 191/2009 Sb., o podrobnostech výkonu spisové služby (dále jen „spisová vyhláška“).

Tato vyhláška se týká nakládání a práce s datovými zprávami, jejich příjem, vyřizování, označování a archivace pomocí spisové služby.

1.4 Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů.

Tato vyhláška upravuje technické náležitosti provádění autorizované konverze dokumentů. Zejména technické náležitosti dokumentu, který provedením konverze vznikl (výstup) a technické náležitosti dokumentu, jehož převedením výstup při konverzi vznikl (vstup).Definuje také vzor osvědčení o vykonání zkoušky zaměstnance provádějícího konverzi na žádost.

1.5 Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

Tato vyhláška definuje náležitosti přístupových údajů pro přihlašování do datové schránky, elektronické prostředky pro přihlašování do datové schránky, přípustné formáty datové zprávy dodávané do datové schránky, maximální velikost datové zprávy dodávané do datové schránky, dobu uložení datové zprávy v datové schránce a způsob tvorby identifikátoru datové schránky.

1.6 Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

Tento zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

1.7 Nařízení vlády č. 495/2004 Sb., o elektronickém podpisu a změně některých dalších zákonů.

Toto nařízení stanoví povinnost orgánů veřejné moci zřídit e-podatelny (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelny jiného úřadu).

Také ukládá povinnost vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací.

1.8 Vyhláška č. 496/2004 Sb., k elektronickým podatelnám.

Tato vyhláška stanoví postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny. Zároveň určuje strukturu údajů kvalifikovaného certifikátu, podle kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat. Tato vyhláška navazuje na nařízení vlády č. 495/2004 Sb., k elektronickým podatelnám, které nařizuje orgánům veřejné moci elektronickou podatelnu zřídit a má sloužit jako návod, jak naplnit podmínky dané tímto nařízením vlády.

1.9 Zákon č. 499/2004 Sb., o archivnictví a spisové službě.

Tento zákon upravuje evidenci a kategorizaci archiválií, práva a povinnosti držitelů a správců archiválií, ochranu archiválií, práva a povinnosti vlastníků archiválií, využívání archiválií, zpracování osobních údajů pro účely archivnictví, soustavu archivů, práva a povinnosti zřizovatelů archivů, spisovou službu, která se vykonává písemnou formou nebo výpočetní technikou, působnost Ministerstva vnitra a dalších správních úřadů na úseku archivnictví a výkonu spisovné služby, správní delikty.

2 ZÁKLADNÍ POJMY

V této kapitole budou vysvětleny základní pojmy a principy vztahující se k fungování datových schránek.

2.1 Kryptografie

Kryptografie (šifrování) je vědní obor, který má za úkol zajistit důvěrnost, popřípadě integritu dané zprávy. Šifrování představuje zakódování přenášené informace pomocí vhodné parametrické jednosměrné funkce tak, aby nebyla srozumitelná třetí osobě. Parametr zde hraje roli speciálního šifrovacího hesla neboli klíče. Dešifrování je opačným procesem, při kterém dochází k převodu zašifrované informace za pomoci dalšího parametru souvisejícího s šifrovacím klíčem na informaci původní.

Klíč se používá buď jeden pro zašifrování i dešifrování (symetrické šifry), nebo dva, jeden klíč pro zašifrování, druhý pro dešifrování (asymetrické šifry).

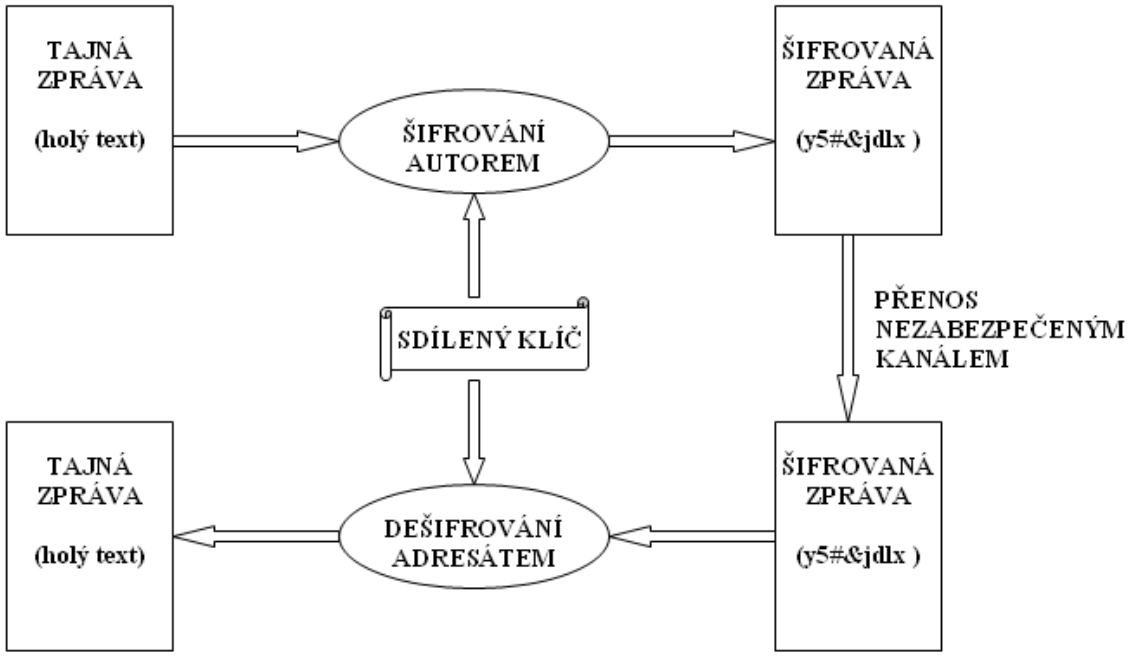
Šifrování hraje v počítačovém prostředí významnou roli, zejména v oblasti počítačové bezpečnosti, lze pomocí něj zajistit například ochranu informací při přenosu z jednoho počítače na druhý, chránit uložené informace před neautorizovaným přístupem nebo při splnění dalších podmínek ověřit, zda je autorem zprávy příslušná osoba.

2.1.1 Symetrická kryptografie

K šifrování zprávy na straně odesílatele je použit stejný (jedinečný) klíč, který je použit na straně příjemce k dešifrování zprávy. Před začátkem komunikace musí tedy být předán příjemci důvěryhodným kanálem šifrovací klíč, pomocí kterého pak může zprávu dešifrovat.

Symetrické šifry jsou velmi rychlé, proto mohou být použity např. pro šifrování vlastních dat, která si pak nikdo nepovolaný (bez znalosti klíče) nepřečte. Tyto algoritmy však neřeší důležitý požadavek neodmítnutelnosti odpovědnosti, protože nelze určit, která strana zprávu odeslala a která ji přijala (obě strany vlastní stejný klíč).

Mezi nejznámější symetrické šifrovací algoritmy patří např. DES (Data Encryption Standard) vyvinutý již v 70. letech minulého století, používající klíč o délce 56 bitů a jeho novější a bezpečnější verze 3DES (trojitě použitý DES).



Obr. 1. Princip šifrování pomocí symetrické kryptografie

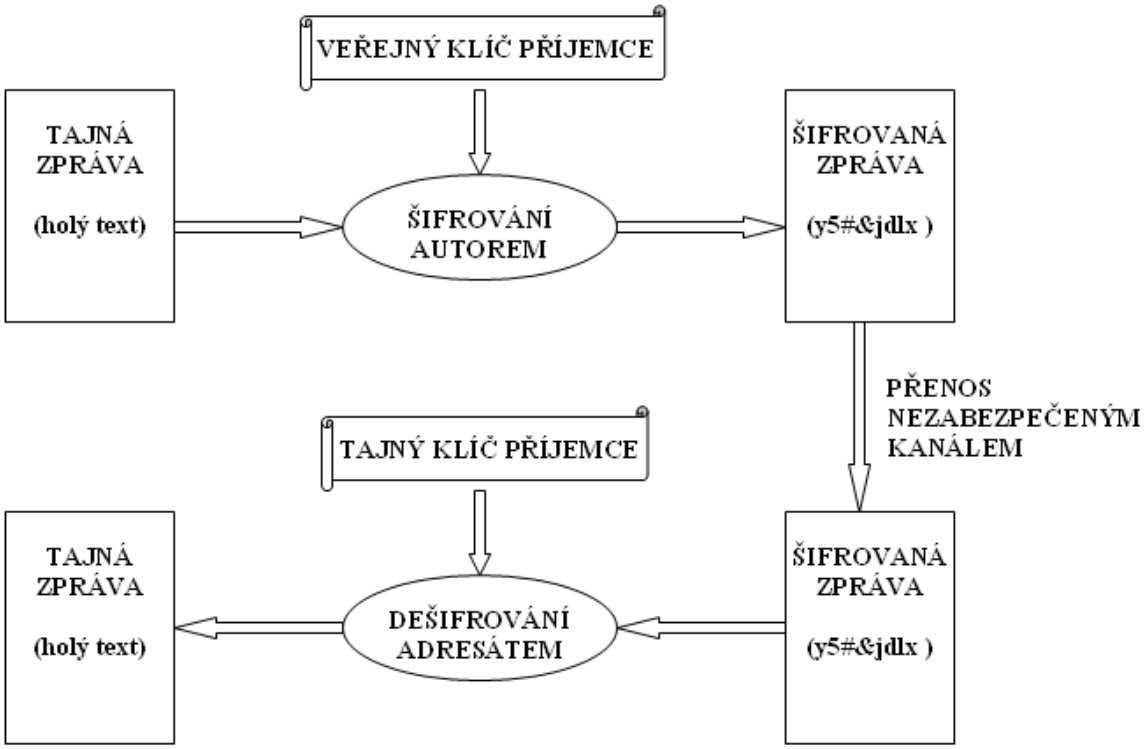
2.1.2 Asymetrická kryptografie

Asymetrická kryptografie využívá jiný klíč pro šifrování a jiný klíč pro dešifrování. Každý subjekt vlastní svůj tajný soukromý klíč pro šifrování (respektive dešifrování) a k němu existuje veřejný klíč (je všeobecně znám), který se používá k dešifrování (respektive k šifrování). Princip tohoto šifrování spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Soukromý a veřejný klíč tedy vždy tvoří nerozlučnou dvojici. Požaduje se, aby odvození soukromého klíče ze známé hodnoty veřejného klíče bylo nesnadné.

Odesílatel buď zasílá příjemci zprávu zašifrovanou pomocí svého soukromého klíče a ten potom pomocí veřejného klíče zprávu dešifruje a zjistí tak, kdo je autorem zprávy. Tomuto principu se říká tzv. digitální podpis. Zprávu nelze podle výše uvedeného postupu považovat za zašifrovanou (důvěrnou), ale pouze za podepsanou, protože veřejný klíč je všeobecně znám a každý tedy může zprávu dešifrovat.

Takto se tedy pomocí asymetrické kryptografie řeší integrita dat a neodmítnutelnost odpovědnosti na straně odesílatele (pokud je prokazatelná unikátní znalost soukromého klíče podepisující osobou). Pozn. Při digitálním podepisování se většinou nepodepisuje celá zpráva, ale jen její charakteristická hodnota (získaná pomocí hashovací funkce), která je pro danou zprávu jedinečná tzv. otisk (hash hodnota). Výše popsaným způsobem však není vyřešena otázka důvěrnosti zpráv, tedy nečitelnosti pro neautorizované subjekty.

K tomu lze využít šifrování zpráv pomocí veřejného klíče adresáta, adresát tuto zašifrovanou zprávu přijme a poté si ji dešifruje pomocí svého soukromého klíče. Takto zašifrovanou zprávu lze dešifrovat pouze soukromým klíčem adresáta, a protože lze předpokládat, že adresát má svůj soukromý klíč utajen (nikdo jiný ho nezná), bude tato zpráva pro ostatní neautorizované subjekty zašifrovaná (nečitelná).



Obr. 2. Princip šifrování pomocí asymetrické kryptografie

Pro přenos zpráv lze samozřejmě použít obě metody šifrování pomocí asymetrické kryptografie současně. Zpráva je tedy nejprve na straně odesílatele digitálně podepsána soukromým klíčem odesílatele, tím je zaručena integrita zprávy a neodmítnutelnost autora dokumentu. A poté je odesílatelem zašifrována pomocí veřejného klíče adresáta, tím je zaručena nečitelnost zprávy pro neoprávněné subjekty. Na straně příjemce je nejprve zpráva dešifrována pomocí jeho soukromého klíče a poté je pomocí veřejného klíče odesílatele zkontrolován její digitální podpis (ověřena identifikace odesílatele).

Mezi nejznámější asymetrické kryptografické algoritmy patří např. RSA, který byl vyvinut v roce 1977 profesory Ronaldem Rivestem, Adi Shamirem a Leonardem Adlemanem a podle jejich příjmení byl také pojmenován. RSA je možné používat jednak jako šifrovací algoritmus a také jako základ pro systém digitálních podpisů. Délka klíčů RSA je libovolná a závisí na použité implementaci.

2.2 Hashovací funkce

Hashovací funkce (anglicky hash function) je jednosměrná transformace (tzv. jednocestná funkce), která z variabilních vstupních veličin (například dokumentu) vrací jednoznačnou hodnotu (textový řetězec) pevné délky, která se nazývá hash hodnota (neboli otisk). Hash hodnota představuje zhuštěnou hodnotu dlouhé zprávy, ze které byla vypočtená, ve významu digitálního otisku prstu velkého dokumentu.

Hashovací funkce mají v praxi velmi mnoho využití. Používají se např. v diagnostice hardware (indikují konečné stavy testů), v komunikaci se používají pro detekci chyb (kódy CRC) a také pro vytváření digitálního podpisu apod. Mezi nejznámější hashovací algoritmy patří MD5 a SHA-1.

2.3 Certifikát

Elektronický certifikát je v podstatě elektronická obdoba občanského průkazu. Tento certifikát je vydávaný certifikační autoritou. Elektronickou formou sděluje informace, které jsou certifikační autoritě známé a umožňují držitele certifikátu jednoznačně identifikovat.

Součástí vydávaného certifikátu jsou tedy identifikační informace o držiteli certifikátu (jméno, bydliště atd.) a dále pak veřejný klíč uživatele certifikátu, doba platnosti certifikátu, identifikace vydavatele (certifikační autorita), číslo certifikátu a případně další informace. Obsah certifikátu je elektronicky podepsán certifikační autoritou (vydavatelem certifikátu), aby bylo možné prokázat, že byl touto autoritou skutečně vydán. Pomocí informací z elektronického certifikátu je možné nejen chránit a autorizovat elektronickou poštu, ale například též zajistit bezpečnou komunikaci na počítačové síti atd. Z pohledu elektronické komunikace se státní správou jsou důležité dva druhy certifikátů. Jsou to kvalifikovaný certifikát a kvalifikovaný systémový certifikát. Kvalifikovaný certifikát je certifikát sloužící k ověření zaručeného elektronického podpisu. Od obyčejného certifikátu se liší tím, že byl vydán kvalifikovanou certifikační autoritou.

Kvalifikovaný systémový certifikát je certifikát sloužící k ověření elektronické značky a vystavuje jej také kvalifikovaná certifikační autorita. Vlastnost kvalifikovatelnosti certifikační autority se potvrzuje akreditačním procesem definovaným relevantními zákonnými normami. Doba platnosti certifikátu je časově omezená. Běžné certifikáty jsou vydávány s platností zpravidla 1 rok a i během této doby je možné zrušit platnost tohoto certifikátu. Důvodem pro toto předčasné zrušení platnosti certifikátu (takzvanou revokaci) může být například ztráta nebo vyzrazení soukromého klíče. Tento soukromý klíč by pak mohl být zneužit cizí osobou, která by se mohla vydávat za skutečného majitele certifikátu. Každá certifikační autorita pravidelně vydává a zveřejňuje seznam zneplatněných certifikátů (CRL = Certificate Revocation List). Interval vydávání CRL je zpravidla 12 nebo 24 hodin a lze jej získat na webových stránkách příslušné certifikační autority.

2.4 Certifikační autorita

Certifikační autorita zajišťuje registraci žádostí o vydání certifikátu, vydávání a správu certifikátu, archivaci a ochranu osobních údajů uživatelů, odvolávání a zneplatnění certifikátu, správu CRL a další činnosti. Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako nezávislý důvěryhodný třetí subjekt, který prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu s jeho dvojicí klíčů respektive s jeho digitálním podpisem. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu.

Důvěryhodnost certifikační autority je zajištěna prokázaným vyhověním legislativním a technickým pravidlům provozu instituce certifikační autority, zveřejněným v tzv. certifikační politice. Certifikační politika je dokument, který stanovuje účel použití certifikátů vydaných pod touto politikou, dále definuje podmínky vydání certifikátů, zneplatnění (revokace) certifikátů apod. Kvalita certifikační politiky určuje míru důvěryhodnosti certifikátů vydaných certifikační autoritou.

Platnost dat uvedených v certifikátu potvrdí certifikační autorita podepsáním dokumentu svým soukromým klíčem a následným vydáním tohoto certifikátu. Znamená to, že certifikát je podepsaným dokumentem se všemi důsledky z toho plynoucími, tedy zejména integrita dat (certifikační autorita jako garant pravosti dokumentu) a autorizace (nelze zaměnit klíč nebo identitu klienta). Tím, že certifikační autorita zaručuje správnost jí vydaného certifikátu, odstraňuje nutnost smluvní důvěryhodné výměny klíčů mezi dvěma subjekty navzájem a jejich dohoda spočívá pouze v domluvě o společně uznávané certifikační autoritě. Důležité je, že se požadavek na dosažení důvěryhodnosti digitálního podpisu na straně klienta redukuje pouze na bezpečné uchování jeho soukromého klíče, protože ostatní je řešeno certifikáty.

Certifikáty je možné kdykoliv ověřit se znalostí veřejného klíče certifikační autority, respektive jejího certifikátu. Existence certifikační autority umožňuje důvěryhodnou komunikaci i subjektům, jenž se navzájem fyzicky nikdy nepotkaly nebo neprovedly složitou proceduru vzájemné důvěryhodné výměny svých klíčů.

2.4.1 Kvalifikovaná certifikační autorita

Kvalifikovaná certifikační autorita je v České republice podle zákona č.227/2000 Sb. taková cetrifikační autorita, které byla udělena akreditace Ministerstvem vnitra České republiky. Vydává tzv. kvalifikované certifikační služby (kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů). Pro získání akreditace od Ministerstva vnitra české republiky musí tato certifikační autorita splňovat podmínky uvedené v tomto zákoně. V současné době v České republice působí 3 kvalifikované certifikační autority (První certifikační autorita a. s., Česká pošta s. p., eIdentity a. s.).

2.5 Elektronický podpis

V České republice byl pojem elektronický podpis zaveden zákonem č. 227/2000 Sb., o elektronickém podpisu. Elektronickým podpisem ve smyslu tohoto zákona se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity (totožnosti) podepsané osoby ve vztahu k datové zprávě. Pro komunikaci s orgány veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb. [23]

Elektronický podpis jsou vlastně digitální data, která podepisující osoba vytváří pomocí svého soukromého klíče a zajišťuje jimi autenticitu dokumentu, integritu dokumentu a nepopiratelnost zodpovědnosti autora podpisu.

2.5.1 Postup vytváření elektronického podpisu

Proces podepsání dokumentu začíná tím, že se vypočte bezpečným kryptografickým jednocestným algoritmem (hashovací funkcí) otisk dokumentu, tzv. hash hodnota. Hash hodnota představuje datový řetězec pevné délky, který jednoznačně charakterizuje text dokumentu. Pokud by se v tomto dokumentu změnil byť jen jeden znak, došlo by ke změně hash hodnoty.

Dnes nejpoužívanějšími kryptografickými hashovacími algoritmy pro digitální podepisování jsou MD5 (Message Digest 5), který v současnosti už není moc bezpečný, SHA-1 (Secure Hash Algorithm) definovaný ve standardu FIPS 180-1 a jeho novější verze definované ve standardu FIPS 180-2 (často souhrnně označované jako SHA-2), které zahrnují SHA-224, SHA-256, SHA-384, SHA-512. Tato hash hodnota se pak zašifruje pomocí asymetrické kryptografie soukromým klíčem podepisujícího. Výsledkem je pak elektronický podpis, který spolu s původním textem tvoří elektronicky podepsaný dokument.

Příjemce dešifruje přijatý elektronický podpis veřejným klíčem podepisujícího, pak svými prostředky vypočte dohodnutým jednocestným hashovacím algoritmem otisk dokumentu a srovná jej s otiskem dokumentu, jehož šifra byla k dokumentu připojena.

Pokud jsou oba otisky stejné, je dokument považován za autentický dokument s nemodifikovaným obsahem. Veřejný a soukromý klíč jsou voleny tak, že podpis zakódovaný jedním klíčem je možné dekódovat pouze druhým klíčem a naopak.

Digitální podpis nezaručuje důvěrnost podepsaného dokumentu. Případně vyžádaná důvěrnost musí být zajištěna dodatečně, např. zašifrováním podepsaného dokumentu veřejným klíčem příjemce (viz šifrování) apod. To, že použitý veřejný klíč je klíčem podepisujícího a je platný, potvrzuje takzvaný certifikát (v případě zaručeného elektronického podpisu kvalifikovaný certifikát), vydaný a elektronicky podepsaný (kvalifikovanou) certifikační autoritou.

Důležitým prvkem, který brání zneužití elektronického podpisu je uchování soukromého klíče na bezpečném místě. Tím je standardně zabezpečené úložiště v paměťovém systému počítače. Soukromý klíč je rovněž možné přechovávat na bezpečnějších a přenosných zařízeních. Tato zařízení jsou vyrobena tak, aby zabránila získání klíče a jeho zneužití. Mezi tato bezpečná média patří USB tokeny, čipové karty apod.

2.6 Elektronická značka

Elektronická značka je zjednodušeně řečeno elektronický podpis generovaný automaticky technickým vybavením. Pro elektronické značky se stejně jako pro elektronický podpis používá technologie digitálních podpisů. Elektronická značka je založena na kvalifikovaném systémovém certifikátu, vydaném akreditovaným poskytovatelem certifikačních služeb. Elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy. Elektronickou značku lze přirovnat k otisku úředního razítka.

2.7 Časové razítko

Časové razítko (z anglického time stamp) je datová zpráva, kterou vydala autorita časových razítek. Tato zpráva důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Časové razítko vždy obsahuje aktuální datum a čas, číslo časového razítka a identifikaci autority, která toto razítko vydala.

Tyto údaje se připojí ke vstupním datům (hash hodnota) a vše se opatří elektronickým podpisem autority časových razítek (TSA = Time Stamping Autority). Toto podepsané časové razítko je pak zasláno zpět žadateli jako odpověď na jeho žádost.

Ověření platnosti časového razítka se provádí stejně jako ověření digitálního podpisu. Nejprve je vypočítána hash hodnota daného souboru (dokumentu) a ta je potom porovnána s hash hodnotou dešifrovanou z časového razítka pomocí certifikátu autority časových razítek (TSA). Pokud se obě hash hodnoty shodují, je časové razítko neporušené a uvedený časový údaj je platný. Také máme jistotu, že obsah souboru se nezměnil.

2.8 Elektronická podatelna (e-podatelna)

Instituce veřejné moci (úřady státní správy) mají od l. l. 2005 za povinnost dle zvláštních předpisů přijímat a vypravovat elektronické úřední písemnosti pomocí elektronické podatelny. Elektronická podatelna je místem, které slouží k přijímání (vstupu) a vypravování (výstupu) elektronických písemností do (z) orgánu veřejné moci.

Tvoří ji souhrn technického vybavení, umožňující se připojit prostřednictvím sítě na elektronickou poštovní schránku, uložit a evidovat doručenou elektronickou poštu a postoupit ji k dalšímu vyřízení, dále obsluha e-podatelny a pravidla pro zacházení s elektronickými písemnostmi, nejčastěji ve formě spisového řádu a návodů pro obsluhu technického vybavení.

2.9 Czech Point

Czech POINT (neboli Český Podací Ověřovací Informační Národní Terminál) je projektem Ministerstva vnitra České republiky. Cílem tohoto projektu je umožnit občanům získat na jednom místě (úřadě) veškeré údaje, opisy a výpisy, které jsou vedeny v centrálních veřejných evidencích a registrech jako je např. výpis z Katastru nemovitostí, výpis z Obchodního rejstříku, výpis z Živnostenského rejstříku, výpis z Rejstříku trestů, výpis z bodového hodnocení řidiče, výpis z insolvenčního rejstříku nebo zde může provést autorizovanou konverzi dokumentů. [21]

Czech Pointy se nacházejí na obecních úřadech s rozšířenou působností, krajských úřadech, u notářů a dalších právnických osob (např. provozovny České pošty s.p. a lokální pracoviště Hospodářské komory ČR s příslušným oprávněním).

V současnosti je v České republice více než 5.820 těchto míst, takže opravdu každý má tyto údaje doslova na dosah ruky a odpadá tím několikahodinové čekání v dlouhých frontách například na výpis z Rejstříku trestu na Rejstříkovém soudu. Také administrativa se zjednodušila, není třeba žádných žádanek.

3 DATOVÉ SCHRÁNKY

3.1 Historie a současnost

Datové schránky jsou dílem Ministerstvo vnitra ČR a jejich provoz zajišťuje Česká pošta s. p. Projekt datových schránek odstartoval s přijetím klíčového zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, účinného od 1. července 2009, který byl do dnešního dne několikrát novelizován. Tento zákon bývá označován také jako eGA čili zákon o eGovernmentu a jeho cílem je vytvoření optimálních podmínek pro elektronickou komunikaci mezi úřady a občany i mezi úřady samotnými. Od 1. července 2009 bylo tedy možné zřizovat podle tohoto zákona datové schránky. Do 90 dnů od tohoto data musela být zřízena datová schránka všem subjektům, které měli mít ze zákona povinně tuto schránku zřízenu (tato problematika bude podrobněji vyložena níže podkapitola 3.3).

Ještě před zakládáním prvních datových schránek byl spuštěn oficiální informační web k datovým schránkám www.datoveschranky.info, obsahující návody na spuštění a používání datových schránek, také legislativu týkající se tohoto tématu a v neposlední řadě zkušební demo simulující činnost datových schránek. Byla také zprovozněna doména www.mojedatovaschranka.cz sloužící k přihlášení do datové schránky přes webový prohlížeč.

Založené datové schránky mohly být aktivovány (zpřístupněny) prvním přihlášením uživatele do své schránky. Dne 1. listopadu 2009 však byly všechny schránky zřízené ze zákona automaticky zpřístupněny (i bez přihlášení uživatele), byl tedy uveden Informační systém datových schránek (ISDS) do ostrého provozu. Došlo k přesunu od doručování úředních písemností poštou na doručování datových zpráv přes Internet (ze zákona daným subjektům), což bývá v mnoha českých médiích označováno jako největší revoluce v administrativě od dob Marie Terezie. Od 1. ledna 2010 je možné využívat datové schránky i pro komerční účely, ale zatím jen pro zasílání faktur a obdobných výzev k zaplacení. Od 1. července 2010 se ale plánuje další rozšíření možností B2B komunikace pomocí datových schránek. Od 1. července 2011 mají být povinně aktivovány datové schránky všem advokátům a daňovým poradcům (kteří se domohli dvouletého odkladu pro povinné užívání datových schránek).

3.2 Co je to datová schránka?

Zákon č. 300/2008 Sb. definuje, že datová schránka je elektronické úložiště, které je určeno k doručování a k provádění úkonů vůči orgánům veřejné moci a od 1. 1. 2010 nově také k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Dokument, dodaný prostřednictvím datové schránky, má stejnou váhu jako doporučená zásilka s dodejkou, a to i do vlastních rukou. Datová schránka umožňuje odesílat datové zprávy, přijímat datové zprávy, zjišťovat stavy odeslaných datových zpráv, přijímat doklady o dodání a doručení, ověřovat, zda adresát má datovou schránku. Orgány veřejné moci mají povinnost komunikovat prostřednictvím datové schránky, má-li ji druhá strana zřízenu. Ostatní subjekty, tedy i právnické osoby, tuto povinnost nemají, z jejich strany se jedná pouze o možnost. Datová schránka pro ně přináší pouze jedinou povinnost, je-li jim zřízena – přijímat zprávy, které byly jejím prostřednictvím doručené. Dále zákon praví, že datovou schránku zřizuje a spravuje Ministerstvo vnitra České republiky (dále jen MVČR). Celý systém datových schránek se označuje v zákoně jako Informační systém datových schránek (dále jen ISDS), jeho správcem je MVČR a provozovatelem držitel poštovní licence tedy Česká pošta s. p.

Jinými slovy datová schránka je vlastně elektronické úložiště pro datové zprávy. Můžeme ji přirovnat k elektronické obdobě zásilky do vlastních rukou. Slouží pro příjem korespondence od orgánů veřejné moci a také pro odesílání korespondence orgánům veřejné moci a od 1. ledna 2010 také ke korespondenci mezi soukromými subjekty navzájem (i když zatím jen omezeně). Ačkoliv celý systém datových schránek (ISDS) může na první pohled připomínat klasickou elektronickou poštu, není tomu tak. Klasická elektronická pošta je vlastně systémem negarantovaným, zatímco ISDS je systémem se zabezpečeným a garantovaným způsobem používání. Pokud se do ISDS vloží nějaká zpráva, ISDS zajistí opatření této zprávy (a jejích eventuálních příloh) časovým razítkem a elektronickou značkou, postará se o spolehlivé doručení do cílové datové schránky, generuje potvrzení o doručení atd. Odesilatel této zprávy se tedy spolehlivě dozví, zda byla jeho zpráva doručena a kdy byla přečtena. A na druhé straně příjemce má záruku, že odesilatel zprávy je skutečně tím, za koho se vydává.

3.3 Kdo má datovou schránku zřízenu ze zákona?

Datovou schránku povinně ze zákona mají zřízeny orgány veřejné moci (OVM) a také právnické osoby (PO) zapsané v obchodním rejstříku. Mezi orgány veřejné moci patří státní orgány (např. ministerstva), orgány územně samosprávných celků (kraje, obce), státní fondy, zdravotní pojišťovny, Česká televize, Český rozhlas, notáři, exekutoři a další. Právnické osoby zapsané v obchodním rejstříku jsou např. všechny obchodní společnosti, družstva včetně bytových družstev, společenství vlastníků jednotek a další. Všichni ostatní (fyzické osoby, podnikající fyzické osoby a právnické osoby nezapsané v obchodním rejstříku) si mohou nechat datovou schránku zřídit na základě jejich žádosti. Datová schránka jim bude zřízena do 3 dnů od podání žádosti. Nově vzniklým OVM nebo PO zapsaným v obchodním rejstříku bude datová schránka zřízena bezodkladně po obdržení informace o zápisu do obchodního rejstříku.

3.4 Přístup do datové schránky

Přístup do datové schránky mají osoby oprávněné, pověřené a administrátor. Oprávněnou osobou je ten, komu byla schránka zřízena a komu přijdou přihlašovací údaje. Oprávněná osoba může následně určit jak administrátory, tak pověřené osoby. Je to fyzická osoba, pro kterou byla datová schránka zřízena, dále pak také statutární orgán PO (pokud je oprávněn jednat za společnost), člen statutárního orgánu PO (pokud je oprávněn jednat za společnost), vedoucí OVM nebo vedoucí organizační složky podniku zahraniční PO působící v České republice. Administrátor je osoba určená oprávněnou osobou pro přístup (a případně správu) do datové schránky. Administrátor může delegovat různé pravomoci na další osoby (v rozsahu, jaký je mu povolen od oprávněné osoby). Pověřená osoba má také povolen přístup k datové schránce od oprávněné osoby nebo administrátora, ale nemůže dále předávat pravomoci dalším osobám.

Do datové schránky je možné se dostat dvěma způsoby, buď přímo přes webové rozhraní (www.mojedatovaschranka.cz) pomocí přidělených přístupových údajů - jména a hesla (případně i volitelného systémového certifikátu pro zvýšení bezpečnosti), nebo přes aplikační rozhraní prostřednictvím aplikace, která je schopna se s informačním systémem datových schránek propojit. Ke zpřístupnění datové schránky dojde prvním přihlášením, nejpozději však patnáctým dnem po doručení přístupových údajů.

3.5 Fikce doručení, změna hesla

Dokument (datová zpráva), který je dodán do datové schránky, je doručen okamžikem přihlášení do datové schránky oprávněnou osobou. Obdobně jako u listovních zásilek funguje fikce doručení tzn. nepřihlásí-li se nikdo do datové schránky ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty. Pokud ve stanovené lhůtě nikdo nevyzvedne datovou zprávu z datové schránky z důvodu dočasné nepřítomnosti nebo z jiného vážného důvodu, může požádat o prominutí zmeškání úkonu (do 15 dnů ode dne, kdy vznikla překážka, která podateli bránila úkon učinit).

Přístupová hesla k datovým schránkám je nutné měnit každých 90 dnů za unikátní doposud nepoužité heslo (tato povinnost v původním zákoně nebyla). A to i v případě, pokud je používána silnější autentizace, opírající se o komerční systémový certifikát. Na změnu hesla ISDS nabídne 5 pokusů, během kterých se sice ke schránce lze přihlásit, ale k jejímu obsahu se bez úspěšné změny hesla nelze dostat. Pokud tyto pokusy nejsou využity, přihlašovací údaje k dané datové schránce jsou zneplatněny.

3.6 Datová zpráva a doba jejího uložení v datové schránce

Zákon uvádí, že dokumenty orgánů veřejné moci doručované prostřednictvím datové schránky a úkony prováděné vůči orgánům veřejné moci prostřednictvím datové schránky a dokumenty fyzických osob, podnikajících fyzických osob a právnických osob dodávané prostřednictvím datové schránky mají formu datové zprávy. Dále také ukládá správci datových schránek (MVČR), aby zajistil opatření každé odeslané datové zprávy časovým razítkem, dále pak zajistil doručení odeslané datové zprávy do datové schránky adresáta, oznámil odesílateli doručení zprávy adresátovi, adresáta informoval o dodání datové zprávy do jeho datové schránky a další povinnosti.

Samotná datová zpráva je vlastně pouze jakýmsi kontejnerem (či obálkou) ve formátu XML (Extensible Markup Language), obsahujícím příslušnou elektronickou značku a kvalifikované časové razítko a samotný obsah zprávy má formu příloh. Počet těchto příloh není omezen co se týká jejich množství, ale celková velikost takovéto datové zprávy (včetně všech jejích příloh) nesmí překročit velikost 10 MB.

Také formát povolených příloh stanovuje neustále aktualizovaná vyhláška. Technické náležitosti užívání datových schránek vydávaná MVČR. Jako příloha datové zprávy nemůže být použit např. živý proud dat (neboli stream) nebo také soubor infikovaný počítačovým virem či spustitelný soubor (např. s příponou .exe) a další.

Datové zprávy jsou podle zákona v datové schránce adresáta uloženy po dobu 90 dnů ode dne doručení, tedy ode dne, kdy se uživatel nebo jeho elektronická spisová služba do schránky přihlásily. Z toho plyne nutnost datové zprávy z datové schránky někam zálohovat, případně provést jejich (autorizovanou) konverzi do listinné podoby pro jejich případné pozdější použití. Oprávněný uživatel nemá možnost zprávy doručené do své datové schránky mazat (nedoručená datová zpráva zůstává i nadále v datové schránce).

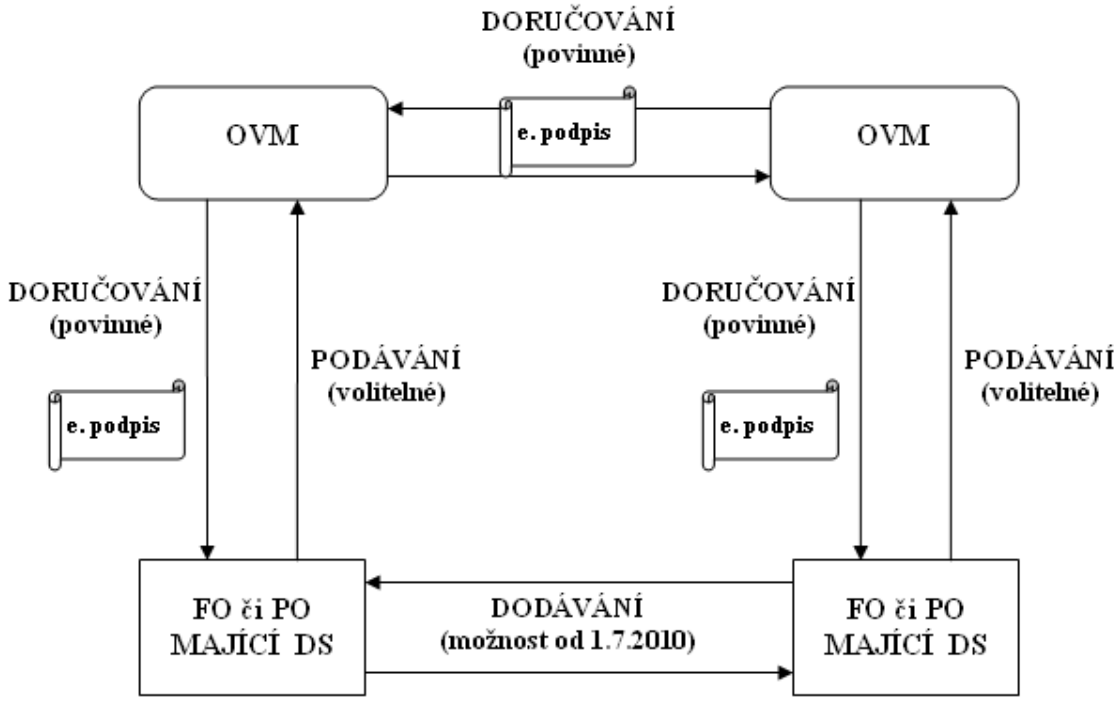
3.7 Autorizovaná konverze

Autorizovaná konverze je podle zákona úplné převedení dokumentu v listinné podobě do elektronického dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky. Úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky. Dokument, který provedením konverze vznikl (dále jen „výstup“), má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl (dále jen „vstup“). Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy, konverze potvrzuje pouze soulad datové zprávy a dokumentu v listinné podobě. [24] Zákon dále definuje dva typy konverzí – konverze na žádost a konverze z moci úřední. Konverzi na žádost provádějí kontaktní místa veřejné správy (Czech POINT). Autorizovaná konverze na žádost se provádí na vyslovenou žádost žadatele a je zpoplatněna (30 Kč za každou započatou stranu formátu A4). Konvertovaný dokument je poté možno odeslat do datové schránky žadatele, nebo vypálit na CD, které kontaktní místo poskytne v ceně účtované za konverzi. Konverzi z moci úřední provádějí orgány veřejné moci pro výkon své působnosti. Existují ale také dokumenty, které nemohou být ze zákona konvertovány, jsou to například jedinečné listiny (např. občanský průkaz), dokumenty obsahující škrty, vsuvky, tam, kdy není zřejmé, zda jde o originál dokumentu, dokumenty, které obsahují plastický text, reliéfní tisk nebo ražbu, suchou pečeť apod.

Dále pak dokumenty nepodepsané uznávaným elektronickým podpisem nebo neoznačené elektronickou značkou toho, kdo dokument vytvořil, zvukové nebo audiovizuální dokumenty a dokumenty v jiné podobě než je listina nebo datová zpráva.

3.8 Doručování prostřednictvím datové schránky

Zákon č. 300/2008 Sb. definuje 3 různé způsoby zasílání do datových schránek. Jde o doručování, podávání a dodávání.



Obr. 3. Způsoby zasílání do datových schránek

Při doručování zprávu odesílá orgán veřejné moci a jejím příjemcem je subjekt vybavený datovou schránkou (ať již jde o orgán veřejné moci, právnickou či fyzickou osobu). V tomto případě je použití datové schránky povinné, protože podle zákona je orgán veřejné moci povinen zasílat datové zprávy do datové schránky příjemce, pokud ji má příjemce zřízenu. Dokument, který prostřednictvím datové schránky zasílá orgán veřejné moci, musí být opatřen uznávaným elektronickým podpisem.

Při podávání zprávu odesílá právnická či fyzická osoba (resp. jiný subjekt než orgán veřejné moci), a příjemcem je naopak orgán veřejné moci. Zákon č. 300/2008 Sb. toto definuje jako „provádění úkonů vůči orgánům veřejné moci“, v praxi jde o různá podání vůči nim. Využití datových schránek je zde volitelné, nikoli povinné.

Dodávání je definované jako přenos dokumentů mezi datovými schránkami fyzických nepodnikajících osob, fyzických podnikajících osob a právnických osob (tzv. B2B komunikace). Tento způsob komunikace bude možný až od 1. července 2010 (s výjimkou zasílání faktur, která je možná již od 1. ledna 2010). Dodávání bude fungovat trochu jinak než doručování a podávání. Například se na něj nebude vztahovat fikce doručení po 10 dnech. Zákon tvrdí, že dodaný dokument se považuje za doručený až tehdy, když příjemce explicitně potvrdí jeho přijetí (což bude bezplatné). Jednotlivé datové zprávy odeslané v rámci dodání bude hradit odesílající.

3.9 Znepřístupnění datové schránky

Jak již bylo řečeno, prvním přihlášením nebo uplynutím patnáctidenní lhůty od doručení přihlašovacích údajů dojde ke zpřístupnění datové schránky. Subjekt s povinným zřízením datové schránky (OVM nebo PO zapsaná v OR) si poté již nemůže nechat schránku znepřístupnit.

Schránka bude automaticky znepřístupněna až v době zániku daného subjektu (výmaz z obchodního rejstříku, úmrtí, zrušení OVM atd.). U ostatních subjektů, kteří si zřídily datovou schránku na žádost, dojde ke znepřístupnění datové schránky nejpozději do tří dnů ode dne podání žádosti o znepřístupnění datové schránky. Tyto subjekty si mohou svou datovou schránku nechat opětovně zpřístupnit. Zpřístupnění jim bude provedeno do tří dnů ode dne podání žádosti. Pokud jim však byla datová schránka znepřístupněna dvakrát za poslední rok, k novému zpřístupnění dojde nejdříve po uplynutí lhůty jednoho roku.

Ke zrušení datové schránky dochází automaticky po uplynutí lhůty tří let od znepřístupnění.

3.10 Zneplatnění přístupových údajů

Od znepřístupnění je třeba odlišovat zneplatnění přístupových údajů. Zneplatnění přístupových údajů může být provedeno dvojím způsobem, buď na žádost nebo automaticky. Na žádost se tak děje např. při ztrátě či kompromitaci přístupových údajů daného subjektu. Tomuto subjektu jsou poté neprodleně zaslány nové přihlašovací údaje. Automaticky dojde např. k zneplatnění přístupových údajů odcházející oprávněné osoby, pokud dojde k oznámení nástupnické oprávněné osoby. Nové přístupové údaje jsou zaslány nástupnické oprávněné osobě.

II. PRAKTICKÁ ČÁST

4 PŘEDTAVENÍ SPOLEČNOSTI

V této kapitole bude krátce přestavena společnost Bioveta a. s. a uvedeno její organizační členění, ze kterého budou patrné vazby mezi jednotlivými odděleními ve firmě nutné pro pozdější pochopení oběhu dokumentů v organizaci.

Název:	Bioveta a. s.
Sídlo:	Komenského 212
	683 23 Ivanovice na Hané
	okres Vyškov
IČ:	25304046
Právní forma	akciová společnost
Datum vzniku:	1.7.1996
Předmět činnosti:	výroba veterinárních léčiv
Ovládající osoba:	BIOVETA Holding a. s., podíl 80,12%

Tab. 1. Základní údaje o společnosti Bioveta a. s.

4.1 Historie

Vznik společnosti je datován až do roku 1918, kdy v Ivanovicích na Hané vznikl Státní ústav pro rozpoznání zvířecích nákaz a výrobu očkovacích látek. O 33 let později došlo k přejmenování tohoto institutu na Bioveta Ivanovice na Hané. V roce 1951 vzniklo logo firmy, které bylo zaregistrováno jako ochranná známka v rejstříku České republiky vedeným Úřadem průmyslového vlastnictví. Logo tvořené nápisem Bioveta nad „ampulí“ v tradičním modrém poli je od r. 1965 chráněno i mezinárodně.

Obr. 4. Logo společnosti

Firma Bioveta Ivanovice na Hané se v minulosti několikrát přetvářela spolu s politickým děním v republice tak, aby v roce 1995 byl tehdejší státní podnik Bioveta zprivatizován společností Bioveta s. r. o. Privatizace podniku proběhla formou veřejné soutěže. 1. července 1996 došlo ke změně právní formy podniku na akciovou společnost.

4.2 Současnost

Společnost Bioveta a. s. je i v současnosti na pozici nejvýznamnějšího a největšího výrobce veterinárních, imunobiologických a farmaceutických přípravků v České republice. Akciová společnost Bioveta sídlí i nadále v Ivanovicích na Hané, kde je umístěna většina jejích výrobních prostor. Další její výrobní závod je umístěn v Opavě.

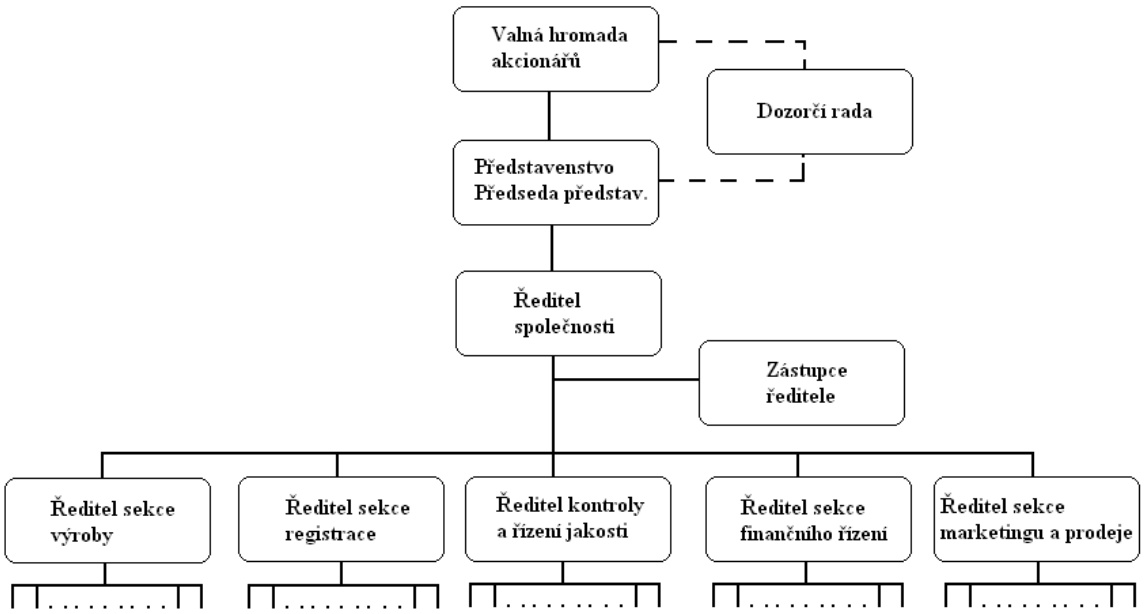
Společnost je držitelem několika certifikátů, například certifikátu správné výrobní praxe (GMP), správné laboratorní praxe (GLP) a správné distribuční praxe (GDP). [14]

Nejvýznamnějšími vlastníky akcií jsou v současnosti čtyři fyzické osoby (akcionáři). K 1. 1. 2010 společnost zaměstnávala 370 zaměstnanců a ve výrobní portfoliu společnosti je přibližně 150 druhů výrobků.

Tyto výrobky jsou určeny jak pro hospodářská zvířata (prasata, skot, ovce), tak pro takzvaná hobby zvířata, kam dnes zahrnujeme psy, kočky, morčata, koně a další. Veterinární přípravky jsou prodávány nejen na českém trhu, ale s úspěchem jsou exportovány do více než 50 zemí světa, což společnosti zaručuje obchodní a finanční stabilitu.

4.3 Organizační struktura společnosti

Nejvyšším orgánem společnosti je valná hromada všech akcionářů. Valná hromada společnosti se schází minimálně jedenkrát ročně, v její kompetenci je volba a odvolání členů dozorčí rady a představenstva společnosti. Představenstvo je statutárním orgánem společnosti. Jmenuje a odvolává ředitele jednotlivých divizí a ze svého středu volí předsedu představenstva. Představenstvo se zpravidla schází jednou měsíčně. Dozorčí rada je kontrolním orgánem společnosti.



Obr. 5. Zjednodušené organizační schéma společnosti Bioveta a. s.

Současný předseda představenstva vykonává funkci ředitele společnosti. Společnost je dále členěna na jednotlivé divize (sekce) viz. obrázek číslo 2. Těchto sekcí je v současnosti pět. Největší co do počtu zaměstnanců je sekce výroby, výzkumu a inovace, která je odpovědná nejen za výrobu produktů, ale od roku 2006 tato sekce zajišťuje výzkum a vývoj nových léčiv a inovaci již existujících produktů či produktových linií.

Sekce výroby rovněž odpovídá za nákup vstupních surovin potřebných k výrobě, kontrolu, seřizování a drobné opravy výrobních zařízení a strojů.

Sekce registrace zajišťuje registraci a certifikaci výrobků v souladu s požadavky státních autorit jak v České republice, tak v zahraničí. Hlavní náplní této sekce je tvorba registrační dokumentace, kterou vytváří ve spolupráci se zaměstnanci sekce výzkumu a vývoje.

Další sekcí je sekce kontroly a řízení jakosti, která dohlíží na kvalitu vstupních surovin a finálních výrobků. Součásti její náplně je rovněž monitoring výrobních procesů a prostor. Mezi nejvýznamnější úkoly patří sledování kvality vody pro injekce, která se používá prakticky ve všech výrobcích společnosti a také sledování kvality ovzduší v jednotlivých laboratořích (teplota, počet částic, vlhkost vzduchu apod.).

Sekce finančního řízení se zabývá řízením finančních toků. V současné době zahrnuje rovněž personální a mzdovou agendu a dále se věnuje dotacím a dotačním projektům.

Klíčovou roli hraje sekce marketingu a prodeje, která je odpovědná za prodej výrobků společnosti Bioveta a. s. na domácím trhu i v zahraničí. Její každodenní náplní je prodej a snaha o zvyšování prodeje výrobků. Mezi běžné činnosti patří kontakt se zákazníky, účast na výstavách a veletrzích, propagace výrobků, monitorování jednotlivých trhů a servis spojený s dodávkami léčiv jejich odběratelům (fakturace, logistika, celnice, certifikace atd.).

V čele jednotlivých sekcí stojí ředitelé, kteří jsou do svých funkcí jmenováni ředitelem společnosti.

5 SOUČASNÁ IMPLEMENTACE DATOVÝCH SCHRÁNEK VE SPOLEČNOSTI BIOVETA A. S.

V této kapitole je popsáno, jak vypadá současná implementace datových schránek ve firmě Bioveta a. s.

5.1 Zřízení DS společnosti a pověření administrátora

Firmě Bioveta a. s. jako akciové společnosti zapsané v obchodním rejstříku byla její datová schránka zřízena ze zákona. V srpnu 2009 dorazily členům statutárního orgánu společnosti přístupové údaje, které Česká pošta s. p. doručila formou tzv. PIN zásilek. Společnost se v té době rozhodla, že prozatím bude k datovým schránkám přistupovat přes webové rozhraní ISDS (na adrese www.mojedatovaschranka.cz). Toto rozhodnutí společnost učinila i z toho důvodu, že ještě neexistovalo vyhovující komerční řešení přes aplikační rozhranní postavené na technologii webových služeb. Členové statutárního orgánu společnosti pověřili k přístupu do datové schránky společnosti pracovníka, který má ve společnosti na starost příjem a vypravování písemností. Tímto pracovníkem je asistentka generálního ředitele společnosti. Právě ona byla určena jako tzv. administrátor, který má stejná práva jako vlastník datové schránky, především může pověřovat další osoby, případně jim pověření odebrat. Rozhodnuto bylo také, že na doručené datové zprávy bude odpovídáno „po staru“ tzn. písemnou formou. Důvodem bylo, že se ve společnosti plánují provést velké změny v oblasti informační infrastruktury. Uvažuje se o zavedení DMS (Document Management Systém = Systém pro správu dokumentů), který by měl obsahovat i modul pro obsluhu datové schránky.

5.2 Příprava počítače administrátora pro přístup do DS přes webové rozhraní

K přístupu k datové schránce přes webové rozhraní ISDS (adresa www.mojedatovaschranka.cz) je nutný osobní počítač s připojením k Internetu a webovým prohlížečem. Pro samotný vstup do ISDS přes webové rozhraní je nutné mít nainstalovaný certifikát certifikační autority PostSignum a také zásuvný modul 602XML Filler.

5.2.1 Instalace certifikátu PostSignum

Protože webové rozhraní ISDS na adrese www.mojedatovaschranka.cz používá serverový certifikát vydaný certifikační autoritou PostSignum (patřící České poště s. p.) a ten není zastoupen mezi certifikáty, které jsou distribuovány jako standardní součást obvyklých webových prohlížečů, je nutné si do svého prohlížeče tento serverový certifikát nainstalovat. Nejprve je nutné stáhnout odpovídající kořenový certifikát Certifikační autority PostSignum na své lokální úložiště. Poté je doporučené si ještě před jeho instalací do systému pečlivě ověřit digitální otisk (hash hodnotu) tohoto kořenového certifikátu. Pravost stažených souborů lze ověřit výpočtem otisku z obsahu celého souboru za použití algoritmů SHA-1 a MD5. Certifikáty jsou úspěšně ověřeny, pokud se vypočtená hodnota otisku shoduje s hodnotou uvedenou v podrobnostech daného souboru na stránkách certifikační autority a v tomto případě i na stránkách Ministerstva vnitra ČR, kde jsou uvedeny otisky všech certifikátů v České republice akreditovaných certifikačních autorit. Pokud by nám ani toto nestačilo, tak je možné navštívit pobočku České pošty s. p. a vyžádat si v tištěné podobě „Prohlášení o pravosti certifikátů Certifikační autority PostSignum“ přímo tam. Po této kontrole už je možné provézt instalaci certifikátu do webového prohlížeče. Postup instalace se může drobně lišit podle použitého webového prohlížeče (Internet Explorer, FireFox), ale princip je obdobný. Je potřeba se přes menu daného prohlížeče dostat až k nabídce certifikáty a námi stažený kořenový certifikát sem importovat (mezi důvěryhodné certifikáty). Při importu je nutné ještě jednou zkontrolovat pravost certifikátu tím, že ověříme, zda kryptografický otisk (SHA-1 nebo MD5) souhlasí s otiskem uvedeným na stránce, odkud byl certifikát stažen. Pokud otisk nesouhlasí certifikát se v žádném případě nedoporučuje instalovat.

5.2.2 Instalace zásuvného modulu XML filler

Pro správný běh ISDS přes webové rozhraní je potřeba mít nainstalovaný ještě zásuvný modul (tzv. plug-in) 602XML Filler, jehož autorem je společnost Software 602 a momentálně je dostupná jeho verze s pořadovým číslem 3.0. Samotná instalace tohoto zásuvného modulu pod nejčastěji používanými prohlížeči Internet Explorer a FireFox není složitá a je to otázkou několika minut.

Nevýhoda přístupu přes webové rozhranní je tedy nutnost mít nainstalovaný tento zásuvný modul v prohlížeči a také udržovat ho v aktuálním stavu (sledovat jestli se neobjevila novější verze tohoto modulu). Bez tohoto modulu totiž není možné přes webové rozhraní ISDS číst datové zprávy z datové schránky.

5.3 Aktivace DS společnosti a prvotní nastavení

Aktivace datové schránky se provede prvním přihlášením do datové schránky nebo po uplynutí 15 dnů od data doručení přístupových údajů. Datová schránka společnosti Bioveta a. s. byla aktivována prvním přihlášením, při kterém byly nastaveny některé parametry této datové schránky. Byl přidán výše zmiňovaný administrátor a byla nastavena e-mailová avíza, která informují konkrétní zaměstnance o nové datové zprávě v datové schránce. Dále byl nastaven certifikát nutný k přihlášení k datové schránce, protože zabezpečení přístupu k datovým schránkám přes ISDS pouze pomocí přihlašovacího jména a hesla se vedení firmy zdálo málo bezpečné. Informační systém datových schránek podporuje zvýšení bezpečnosti přihlašování využitím certifikátu, uloženého na čipové kartě, USB tokenu nebo jiném technickém prostředku. Tento certifikát ovšem neslouží jako náhrada za uživatelské jméno a heslo, ale jako další bezpečnostní prvek k nim. Příslušnému administrátorovi DS ve společnosti byl tedy zřízen speciální USB token iKEy 4000 od České pošty s. p. Na tomto tokenu je bezpečně uložen komerční certifikát pro přístup k datové schránce společnosti a také soukromý klíč (kvalifikovaný certifikát) pro uznávaný elektronický podpis osoby, která má datovou schránku společnosti na starost (administrátor). Tyto certifikáty nelze z jejich úložiště na tokenu exportovat (tedy zkopírovat jinam), protože jsou chráněny PINem a PUKem a při několikanásobném neúspěšném zadání PINu se token zablokuje. V takovém případě lze odblokovat pomocí PUKu, který je několikanásobně delší než PIN. I tady hrozí nebezpečí a sice definitivního zablokování tokenu. K tomuto zablokování dojde po několikanásobném neúspěšném zadání PUKu. Tato operace je nenávratná, token již nelze žádným způsobem odblokovat, musí dojít k tzv. inicializaci, při které dojde ke ztrátě veškerých dat uložených na tokenu. [20] Společnost také zřídila placenou službu Datový trezor (od České pošty s. p.), která slouží k archivaci datových zpráv, po uplynutí 90 dnů o ně tedy společnost nepřijde.

5.4 Současná agenda kolem DS

Jak již bylo řečeno výše o datovou schránku společnosti se stará administrátor určený vedením společnosti. Jedná se o asistentku ředitele společnosti. Tato pracovnice se také stará o vedení agendy spojené s poštou (podrobněji níže). Co se týká datových schránek, tak v současnosti se k nim ve společnosti stále přistupuje pomocí webového rozhranní ISDS, pověřený administrátor datové zprávy z této datové schránky vytiskne a předá pracovníkovi, kterému jsou určeny. V případě potřeby autorizované konverze administrátor podá přes ISDS žádost o provedení autorizované konverze. Poté administrátor, případně osoba, která konvertovaný dokument potřebuje, navštíví s žádostí vygenerovanou systémem ISDS specializované pracoviště Czech Point a dokument si nechá zkonvertovat do listinné podoby. Momentálně tedy naše společnost přes datové schránky přijímá datové zprávy od orgánů veřejné moci, ale zatím jim odpovídá jen papírovou formou. Nevyužívá tedy naplno možností, které datové schránky nabízejí.

6 OBĚH DOKUMENTACE VE SPOLEČNOSTI BIOVETA A. S.

V této kapitole bude vysvětleno, jak vypadá v současnosti oběh (zatím) papírové dokumentace (pošty, příbalových informací a ostatních vnitřních dokumentů) ve společnosti Bioveta a. s.

6.1 Oběh pošty

6.1.1 Příchozí pošta

Veškeré poštovní zásilky, které jsou určeny pro společnost Bioveta a. s., jsou tříděny asistentkou generálního ředitele. Všechny zásilky se zaznamenávají do tzv. knihy přijaté pošty. Každé zásilce je přiděleno unikátní pořadové číslo. Záznam v knize dále uvádí datum příchodu zásilky, komu je zásilka určena, předmět zásilky, pokud je adresována na společnost a ne na konkrétní osobu a v neposlední řadě komu byla zásilka předána k vyřízení. Na zásilku je před jejím předáním uvedeno datum doručení, pořadové číslo a jméno osoby, která je odpovědná za její vyřízení či osoby, které je zásilka určena.

Samotná distribuce zásilek pak probíhá manuálně a to rozdělením do poštovních přihrádek ředitelů jednotlivých sekcí. Odtud jsou vyzvedávány jejich asistentkami a dále distribuovány v rámci jednotlivých sekcí příslušným pracovníkům.

Pokud musí být zásilka distribuována dalším pracovníkům, je pořízen příslušný počet kopií a na každou z nich je napsán rozdělovník se jmény pracovníků, kterým je určen. Pokud jsou tito pracovníci v rámci stejné sekce jako hlavní adresát, je zásilka předána prostřednictvím asistentky ředitele této sekce. V případě, že je zásilka určena pracovníkům více sekcí, je její distribuce opět provedena manuálně prostřednictvím poštovních přihrádek jednotlivých ředitelů sekcí.

6.1.2 Odchozí pošta

Pro odchozí poštu platí podobné postupy jako pro příchozí. Všechny zásilky jsou soustřeďovány na sekci marketingu a prodeje. Zde jsou zaznamenány do tzv. knihy odchozí pošty. Každé odchozí zásilce je přiděleno unikátní číslo a dále zapsáno datum odeslání, adresát a odesílatel. Všechny zásilky jsou po evidenci předány České poště s. p.

6.2 Příbalová informace

Jak již bylo řečeno společnost Bioveta a. s. se zabývá výrobou veterinárních, imunologických a farmaceutických výrobků, proto mezi nejdůležitější dokumenty, které jsou ve firmě vytvářeny patří příbalová informace zde vyráběných produktů. V současné době je systém tvorby a udržování platnosti příbalové informace následující.

Příbalová informace, tedy informace o tom, jak má a může být s konkrétním léčivem nakládáno je vytvořena pracovníky sekce výzkumu a vývoje. Tito pracovníci vytváření první návrh, ve kterém jsou popsány zamýšlené vlastnosti budoucího výrobku. V tomto stádiu je příbalová informace zaslána na sekci registrace, která upraví formální stránku příbalové informace tak, aby odpovídala požadavkům zákona a evropského lékopisu. Sekce registrace poté upravený návrh příbalové informace předává sekci marketingu a prodeje, která se vyjadřuje k produktu z hlediska jeho konkurenceschopnosti na trhu. V obou případech se jedná o vytištěnou kopii, která je po případných komentářích a úpravách potvrzena podpisy ředitelů sekce registrace a marketingu a prodeje. Poté je vrácena na sekci výzkumu a vývoje. Doručení probíhá manuálně prostřednictvím vnitropodnikové pošty.

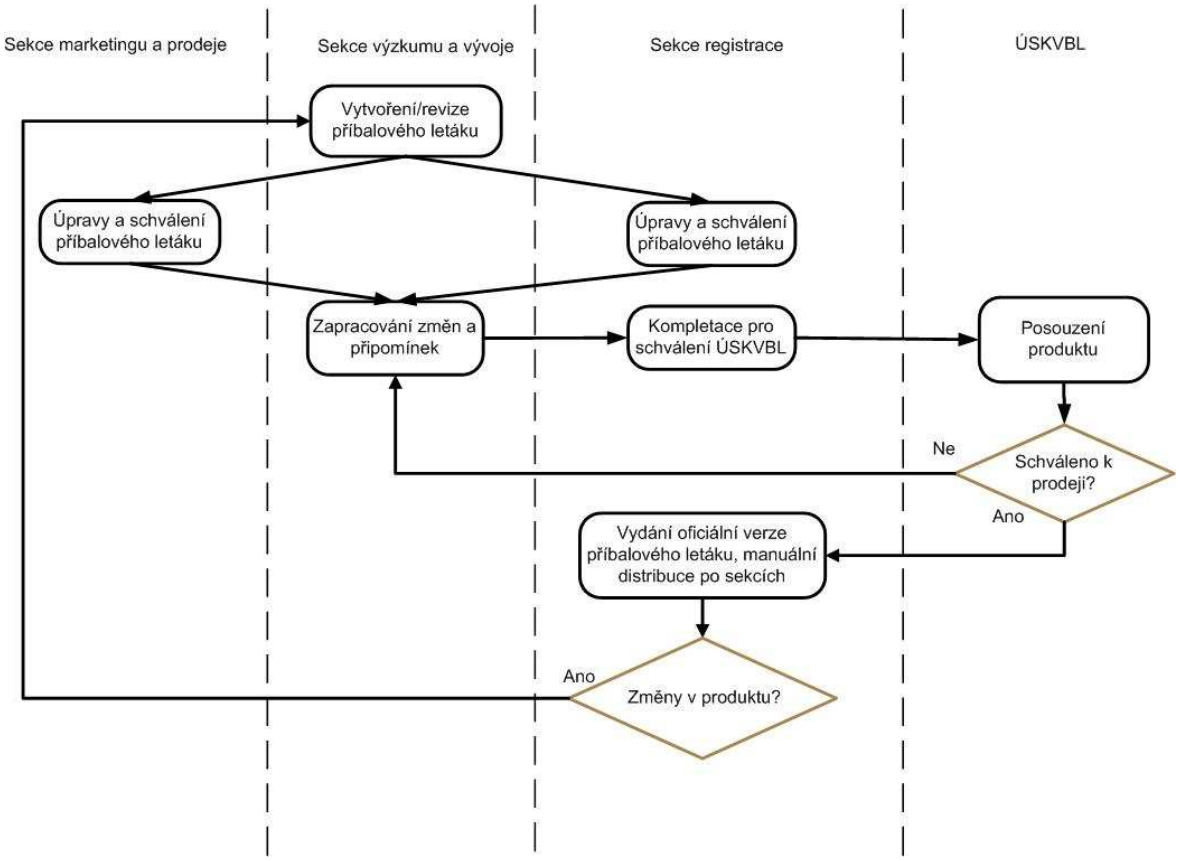
Po odsouhlasení informace a ukončení všech fází výzkumu a vývoje je produkt předložen Ústavu pro státní kontrolu veterinárních biopreparátů a léčiv (ÚSKVBL) ke schválení pro prodej v České republice.

Pokud je výrobek pro prodej schválen, ÚSKVBL vydá schválenou příbalovou informaci pro každý produkt. Tato informace je nejprve doručena sekci registrace, která je odpovědná za komunikaci se státními orgány při schvalování produktů společnosti Bioveta a. s. pro jejich prodej. Sekce registrace vydá závazný vzor příbalové informace, který je v tištěné formě zaslán ředitelům jednotlivých sekcí (výroby, kontroly, prodeje), kteří jej předají odpovědným pracovníkům. Na sekci výroby je vzor uložen na oddělení nákupu, které přebírá dodávky příbalových informací od dodavatelů.

Na sekci kontroly a řízení jakosti je příbalová informace uložena u kvalifikované osoby, která je ze zákona odpovědná za uvolňování produktů k prodeji. Každá dodávka příbalové informace je porovnávána se závazným vzorem. Dále je příbalová informace opět kontrolována při propouštění již zabaleného výrobku k prodeji.

Na sekci marketingu a prodeje je schválená příbalová informace uložena u jejího ředitele a u zaměstnanců, kteří zadávají zakázky do výroby.

V případě změny příbalové informace, je nutné nejprve všechny neplatné verze stáhnout od všech jejich uživatelů a nahradit novým závazným vzorem. Každá verze i kopie příbalové informace je evidována v systému a každé z nich je přiděleno unikátní identifikační číslo. Po stažení všech kopií je sekcí registrace vydán nový závazný vzor příbalové informace. Jeho distribuce probíhá opět stejnou cestou jak je popsáno výše.



Obr. 6. Proces tvorby příbalové informace

6.3 Oběh ostatních (vnitřních) dokumentů

Ve společnosti probíhá samozřejmě i oběh ostatních dokumentů, vytvořených uvnitř společnosti a nutných k jejímu bezproblémovému chodu. Jedná se o papírové dokumenty – faktury ke schválení, dokumenty ke schválení vedením společnosti, dokumenty týkající se plánování výroby, žádanky na nákup materiálu.

Těchto dokumentů ve společnosti neustále přibývá. Vnitřní oběh dokumentů, především jejich distribuce, stále více zatěžuje administrativní pracovníky jednotlivých oddělení, kteří by svůj pracovní čas mohli využívat mnohem efektivněji. Proto společnost plánuje v nejbližší době zavedení systému pro správu dokumentů DMS (Document Management Systém), který by měl zároveň vyřešit implementaci datových schránek ve společnosti Bioveta a. s. pomocí firemní podatelny.

7 DNES NABÍZENÁ ŘEŠENÍ IMPLEMENTACE DATOVÝCH SCHRÁNEK

V této kapitole budou popsána v současné době nabízená řešení implementace datových schránek od nejjednodušších až po komplexní řešení datových schránek pomocí systémů pro správu dokumentů.

7.1 Informační systém datových schránek (ISDS)

Informační systém datových schránek je základní aplikace pro obsluhu datové schránky. Jedná se o přístup k datovým schránkám přes běžný webový prohlížeč na adrese www.mojedatovaschranka.cz. Jde v podstatě o webovou aplikaci, která běží na serveru provozovatele datových schránek (Česká pošta s. p.). Toto řešení má ale několik nevýhod. Jednak potřebuje pro svůj běh speciální doplněk 602 XML Filler (od společnosti Software602), který je potřeba nainstalovat do webového prohlížeče a průběžně aktualizovat. Také je žádoucí do prohlížeče nainstalovat certifikáty certifikační autority PostSignum potřebné pro korektní a bezpečný přístup k ISDS. Možnosti této aplikace jsou značně omezené (na rozdíl třeba od dnešních e-mailových klientů). Tato aplikace má jen základní funkcionalitu, tou je přijímání a odesílání zpráv a doručenek. Neumí například třídit ani filtrovat zprávy, nebo pracovat se složkami. Dalším problémem této aplikace je to, že doručené zprávy jsou po 90 dnech vymazány. Je to v podstatě jen to nejzákladnější řešení přístupu k datovým schránkám pro ty, kdo musejí mít ze zákona zřízenu datovou schránku a nepožadují žádnou další funkcionalitu.

7.2 Konektor umožňující propojení DS s poštovním klientem

Dále je na trhu nabízen například Microsoft Outlook konektor pro datové schránky, tedy řešení od společnosti Microsoft (a jeho partnerů), které umožňuje datové schránky implementovat do programu Microsoft Outlook (počínaje verzí 2003 a novějšími). Instalací tohoto konektoru je poštovní klient Outlook rozšířen o panel nástrojů, který umožní zadat přístupové údaje datové schránky a následně se komunikace s datovou schránkou jeví uživateli jako práce s doručenou či odeslanou poštou pomocí tohoto poštovního klienta. Základní verze tohoto řešení s omezenou funkcionalitou je zdarma, vyšší verze jsou již zpoplatněny.

Tento produkt je vhodný zejména pro menší firmy, živnostníky a občany mající zřízenu ze zákona jednu datovou schránku. Případně pro lidi, kteří používají poštovního klienta Outlook a nechtějí se učit nové věci. Jeho výhodou je, že umožňuje uchování datových zpráv ve složkách programu Outlook (nehrozí jejich ztráta po 90 dnech) a díky funkcím programu Outlook je možné také filtrování a třídění datových zpráv.

7.3 Samostatné aplikace řešící implementaci DS bez možnosti na napojení na existující struktury oběhu dokumentů v organizaci

Představitelem tohoto řešení je například aplikace Multischránka od společnosti AMOS software. Nejedná se o integraci systému datových schránek do standardních emailových klientů jako v předchozím případě. Cílem tohoto projektu je vytvoření vlastní poštovní aplikace pro datové schránky. Tato aplikace nabízí funkce srovnatelné s běžnými emailovými klienty, je však naprogramována v prostředí Adobe AIR. To umožňuje, aby tato aplikace byla multiplatformní (schopna pracovat na více počítačových platformách). Bez problémů pracuje pod Microsoft Windows na architektuře x86, dále pod Mac OS X a také pod Linuxem. Z uživatelského pohledu je velmi jednoduchá a přívětivá. Umožňuje stahování a zálohování datových zpráv do vlastního prostředí (archivace datových zpráv), off-line práci s datovou schránkou a datovými zprávami. Obsahuje také vlastní adresář, kam se ukládají kontakty. Zvládá také práci s více datovými schránkami současně, upozornění na nově došlé zprávy, nebo jednoduchou práci s formátem PDF (autorizovaná konverze). [16] Jejím nedostatkem ale je, že neumí práci s časovými razítky. Opět se jedná o aplikaci určenou pro menší organizace a živnostníky.

7.4 Aplikace pro propojení DS s již existujícími systémy spisových služeb a e-podatelem

Zástupcem těchto aplikací je například produkt Actis Datové schránky od společnosti Actis. Produkt Actis Datové schránky poskytuje dostatečnou flexibilitu pro integraci s již existujícími systémy spisových služeb, e-podatelen, výpraven nebo jiných aplikací. Obsahuje průvodce, který uživatele provede nutnými úkony pro napojení datové schránky. Podporuje IBM Lotus Domino & Notes od verze 6.5. Plně komunikuje se serverem ISDS, přijímá a odesílá zprávy, včetně získávání doručenek. Lze omezit oprávněné uživatele, kteří mohou odesílat zprávy, a to na úrovni adresátů.

Funkce rychlé odpovědi na zprávu umožní zprávu odmítnout s udáním důvodu. Produkt nabízí nástroje pro cílené směrování zpráv. Distribuovat lze obálky, odkazy na originály s obálkou, originály nebo obálky s rozbaleným obsahem. Umožněno je doslání, vrácení i distribuce pověřeným pracovníkem. Pohyby jsou zaznamenávány do historie. Každé pravidlo obsahuje možnost informování nového okruhu adresátů e-mailem. Jeho základní funkce jsou přijímání zpráv z datových schránek, odesílání zpráv do datových schránek, řízená distribuce zprávy na různá místa (pobočky, zodpovědné osoby) ve společnosti, integrace s existující spisovou službou, vyhledávání identifikačních čísel schránek, napojení na vlastní adresář (bez programování), zjednodušená archivace (po dobu delší jak 90 dní). [15] Tento produkt je určen firmám a organizacím, které již mají zřízenu nějakou spisovou službu či e-podatelnu a chtějí ji mít propojenou se systémem datových schránek.

7.5 Kompletní softwarová řešení pro správu dokumentů v organizaci obsahující modul pro obsluhu DS

Poslední a nejsofistikovanější skupina softwarových aplikací pro datové schránky již představuje řešení pro střední a velké organizace se značným oběhem dokumentů a s nimi spojených úkonů. Systémy pro komplexní správu dokumentů v organizaci jsou nazývány DMS (Document Management Systém) a podrobněji budou popsány dále v práci. Tato řešení se tedy starají nejen o oběh digitálních dokumentů v organizaci, ale mívají v sobě také zabudovanou funkcionalitu pro obsluhu datových schránek. Zajišťují například ukládání a zpracování datových zpráv. Obsahují standardní funkcionality spisové služby a umožňují řídit distribuci přijatých datových zpráv a v nich uložených dokumentů uvnitř organizace včetně sledování stavu a lhůt jejich vyřízení. Po vyřízení datové zprávy umožňují také odeslat odpověď do datové schránky adresáta a evidovat stav jejího doručení. Obsahují také například adresáře kontaktů umožňující evidovat datové schránky adresátů a tyto údaje používat při zpracování přijatých a odesílaných datových zpráv. Bývá v nich možné provádět kompletní evidenci příchozí a odchozí pošty. Umějí také sofistikovaně pracovat s elektronickými podpisy, komerčními certifikáty (pro bezpečné přihlášení) a časovými razítky. Nečiní jim problémy ani práce se soubory typu PDF, tedy formátem vhodným pro autorizovanou konverzi dokumentů. Do těchto systémů je možné integrovat řadu dalších agend.

V neposlední řadě také umožňují automatickou distribuci datových správ uvnitř organizace podle definovaných pravidel nebo řízení přístupu ke zprávám pomocí přístupových práv. Obsahují také nástroje pro manažerské reporty a centrální zpracování. Mezi zástupce těchto systémů patří například DMS sytém SAFE od společnosti AiP Safe s. r. o. obsahující i modul pro datové schránky.

8 ROZBOR POŽADAVKŮ PRO IMPLEMENTACI DMS SYSTÉMU A DATOVÝCH SCHRÁNEK VE SPOLEČNOSTI BIOVETA A. S.

V této kapitole budou probrány očekávané cíle a přínosy zavedení systému pro správu dokumentů (včetně řešení datových schránek) ve společnosti Bioveta a. s. a také definovány požadavky, které tato společnost na implementaci systému pro správu dokumentů má.

8.1 Definice systému pro správu dokumentů

Jestliže organizace vytváří a spravuje velké množství dokumentů, které připravuje více lidí najednou, je vyloučeno, aby se všechny dokumenty pouze ukládaly na nějakém sdíleném síťovém disku v souborech. Je nutné zajistit přístupová práva k jednotlivým dokumentům (případně i jejich částem). Také je dobré rozdělit velké dokumenty na menší části, které budou moci jednotliví uživatelé editovat nezávisle na sobě. Aplikace, které výše popsané funkce nabízejí, se obvykle nazývají systémy pro správu dokumentů (anglicky DMS = Document Management System nebo také EDM = Electronic Document management). Systém pro správu dokumentů lze tedy definovat jako počítačový systém určený ke správě elektronických dokumentů a také zdigitalizovaných papírových dokumentů (např. papírových dokumentů převedených do digitální podoby skenováním).

Podle účelu použití můžeme DMS rozdělit do několika skupin. Jednak jsou to systémy pro ukládání elektronických dokumentů (např. elektronický archiv). Dále pak procesně orientovaná řešení (např. zpracování došlých faktur). Další skupinou představují systémy pro řízení projektů (případně i pracovních týmů). A nakonec jsou smíšené (speciální) systémy, které v sobě kombinují více výše uvedených funkcionalit (e-learning, spisová služba a další).

Typický systém pro správu dokumentů řeší následující problémy. Ukládání elektronických dokumentů do databáze s centralizovaným přístupem, a to například i hromadně nebo přímo z uživatelské aplikace. Opatřování těchto dokumentů takzvaným metapopisem a číslem jejich revize. Metapopis je určen k přidání dodatečné informace k dokumentu (např. autor dokumentu nebo kategorie, kam dokument patří). Tato informace nemusí být součástí obsahu dokumentu.

Většinou je metapopis používán pro rychlejší vyhledání konkrétního dokumentu podle zadaných kritérií. Revizování (verzování) se používá k odlišení různých stavů, ve kterých se dokument může nacházet. DMS má většinou zálohovaných více verzí jednoho dokumentu. DMS také automaticky přiděluje dokumentům a jejich revizím identifikátory (většinou číselné), umožňující jednoznačnou identifikaci každého dokumentu v rámci celého DMS systému. Dokumenty jsou uživatelům poskytovány z jediného centrálního zdroje (distribuovaného, nebo replikovaného), kde jsou vždy uloženy jejich aktuální verze. Tato centralizace snižuje redundanci dat, protože tato data není nutné vyměňovat mezi uživateli navzájem. Stačí je jen vložit do centra a poskytnout odkaz na místo, kde se nachází. DMS systémy umožňují také lepší vyhledávání dokumentů (i jejich částí) podle metapopisů a fulltextových indexů. Další jejich nabízenou funkcionalitou je správa přístupových práv. Přístupová práva slouží k omezení přístupu neautorizovaných uživatelů k datům systému (dokumenty, složky, metapopis atd.). Většinou DMS také podporuje workflow, neboli automatizované procesy oběhu dokumentace. Dovoluje například uživatelům vidět pohromadě dokumenty, které musí být vyřízeny. Managementu pak obvykle poskytuje nástroje pro sledování dokumentu v rámci procesu. Umí například dávat odpovědi na otázky "Které dokumenty jsou připraveny ke schválení déle než týden a stále ještě nebyly schváleny?" a další. [26] DMS podporují také bezpečnou archivaci a obnovení dat v případě potřeby. A také týmovou práci (přístup do společných pracovních oblastí, virtuální schůzky, správa projektů).

8.2 Očekávané cíle a přínosy implementace DMS

Společnost Bioveta a. s. dosud nevyužívala ke zpracování a oběhu svých dokumentů žádné prostředky pro elektronické zpracování dokumentů (Document Management System či Spisové služby). S nástupem datových schránek a jejich povinného používání navrhuji vedení společnosti Bioveta a. s. přistoupení k elektronizaci oběhu dokumentů a vytvoření workflow pro jejich zpracování.

Očekávané přínosy řešení:

- snížení finančních nákladů na odesílání doporučených dopisů (26 Kč za doporučenou zásilku vs. 0 Kč za datovou zprávu pro OVM a 18 Kč za poštovní datovou zprávu B2B komunikace);
- snížení pracovního zatížení administrativních pracovníků majících na starost vyřizování pošty (cesta na poštu, nebo na daný úřad);
- snížení administrativy spojené s řízením oběhu dokumentů uvnitř společnosti (distribuce vnitřních papírových dokumentů tj. například žádanek na nákup materiálu, dokumentů ke schválení vedením, faktur ke schválení apod.);
- digitalizace procesů podatelny (kniha příchozí a odchozí pošty);
- zefektivnění procesu řízení dokumentů – implementací workflow (tvorba, schvalování, distribuce dokumentů, odpovědnosti) v systému DMS;
- snížení tiskových nákladů (tvorba mnoha kopií daných dokumentů pro různá oddělení);
- zvýšení kontroly toku dokumentů a přístupu k nim (obtížně kontrolovatelný proces oběhu papírových dokumentů napříč různými odděleními za účelem doplnění nebo schválení).

8.3 Požadavky společnosti na řešení implementace DMS

Na základě stanovených cílů od vedení společnosti a požadavků ze strany uživatelů bylo vytvořeno zadání shrnující požadavky na hledané řešení.

8.3.1 Technologické požadavky

- řešení založené na technologiích společnosti Microsoft (protože společnost Bioveta a. s. tyto technologie používá):
    - kompatibilita s operačními systémy MS Windows Server 2008;
    - kompatibilita s databázemi MS SQL 2005 nebo 2008;
    - podpora kancelářského balíku Microsoft Office;
- napojení na Active Directory (autentizace vůči Active Directory);
- kompatibilita se současným antivirovým řešením (software NOD 32 od společnosti ESSET);
- možnost napojení na emailový systém Kerio Mailserver;
- maximální využití stávajících hardwarových (HW) prostředků při zachování dostatečné kapacity a propustnosti řešení (tak, aby společnost nemusela investovat do pořízení nového hardwaru, který není nezbytně nutný).

8.3.2 Implementace řízení přístupových práv

- možnost vytváření různých rolí v rámci aplikace – jednotlivým rolím jsou přidělena různá přístupová práva (vedoucí pracovník, koncový uživatel, osoba oprávněná k výběru datové schránky, pracovník podatelny apod.).

8.3.3 Funkční požadavky řešení

- napojení na více datových schránek (osoba oprávněná k přístupu k datové schránce společnosti Bioveta a. s. bude mít přístup i do datové schránky dceřinné společnosti SEVARON PORADENSTVÍ, s. r. o.);
- možnost tvorby jednoduchých workflow (tuto funkci využije společnost nejprve pro proces tvorby a schvalování příbalového letáku s postupným rozšiřováním na další procesy probíhající uvnitř společnosti);
- sledování pohybu dokumentů v rámci společnosti – od příjmu dokumentu (podatelna, ISDS) až po vyřízení dokumentu odpovědnými osobami;
- digitalizace příchozích dokumentů (došlé pošty) a jejich následné zpracování v aplikaci dle definovaných workflow;
- bezpečné a trvalé uložení došlých datových zpráv (ochrana před mazáním zpráv v ISDS po 90 dnech) a dokumentů;
- podpora pro práci s digitálními certifikáty, elektronickým podpisem a časovými razítky (podepisování souborů, formulářů apod.);
- možnosti vyhledávání a filtrování došlých datových zpráv dle jednotlivých organizačních útvarů i dle stavů dokumentu (schváleno, ke schválení, ke zpracování apod.);
- zajištění archivace datových zpráv i dokumentů;
- logování provedených operací, včetně historie úprav datových zpráv a dokumentů.

8.3.4 Požadavky na zpracování datových zpráv

- automatizované přebírání datových zpráv přes aplikační rozhraní;
- vyhledávání datových schránek a odesílání datových zpráv do datové schránky adresáta prostřednictvím aplikace (bez nutnosti přihlašování se do ISDS);
- ověření platnosti datových zpráv i přiložených příloh (ověření platnosti elektronického podpisu a časového razítka, neporušenost zprávy atd.)
- rozebrání datové zprávy přímo aplikací (rozložení na přílohy);
- možnost vytvoření adresáře (pro nejčastěji používané adresáty – ID datových schránek);
- datové zprávy může odesílat pouze odpovědný pracovník (pracovník podatelny);
- vytváření pravidelných (např. měsíčních) reportů o přijatých a odeslaných datových zprávách;
- možnost manuálního i automatického předávání zpráv (např. na základě ID schránky odesílatele);
- možnosti tisku datových zpráv nebo příloh, včetně možnosti uložení kompletní datové zprávy nebo příloh;
- možnost zprocesovat požadavek na autorizovanou konverzi datové zprávy prostřednictvím aplikace (bez nutnosti připojovat se k systému ISDS).

8.3.5 Ostatní požadavky

- technická a implementační podpora minimálně v režimu 5x8 (podpora v režimu 5x8 znamená poskytování technické podpory 5 dnů v týdnu od pondělí do pátku v pracovní době tzn. 8 hodin denně);
- vyškolení všech zaměstnanců, kteří budou s aplikací pracovat.

9 NAVRHOVANÉ ŘEŠENÍ IMPLEMETACE DMS SYSTÉMU A DATOVÝCH SCHRÁNEK VE SPOLEČNOSTI BIOVETA A. S.

V kapitole 7 byla uvedena v současné době nabízená řešení implementace datových schránek. Po výše uvedených poznatcích o nutnosti zavedení systému pro správu dokumentů ve společnosti Bioveta a. s. je patrné, že by se společnost měla rozhodnout pro kompletní softwarové řešení pro správu dokumentů v organizaci obsahující modul pro obsluhu datové schránky. Na současném trhu existuje mnoho řešení implementace DMS. Proto společnosti Bioveta a. s. navrhuji, aby při implementaci DMS ve firmě posuzovala pouze řešení založená na službě Microsoft SharePoint Services. Společnosti doporučuji, aby se zaměřila na službu MS SharePoint Services především z následujících tří důvodů:

- nízké pořizovací náklady (služby MS Sharepoint Services 3.0 jsou poskytovány zdarma k Windows Server 2005 nebo 2008);
- známe prostředí Windows pro zaměstnance, kteří budou s aplikací pracovat – rychlejší orientace v nové aplikaci, odpadá nutnost seznamování se s novým prostředím;
- flexibilní a otevřené řešení, které je možné zcela přizpůsobit potřebám a požadavkům společnosti Bioveta a.s.

9.1 Přehled nabízených implementací datových schránek postavených na platformě Microsoft SharePoint Services

V současné době je na trhu více řešení implementace datových schránek (označovaných zpravidla jako podatelny) založených na službách Microsoft SharePoint Services. Výrobci těchto produktů jsou zejména velké renomované softwarové společnosti (partneři společnosti Microsoft). Nabízejí většinou hotový základní modul pro obsluhu datových schránek (podatelnu) a implementování systému pro správu dokumentů v dané organizaci dělají až na základě požadavků daného klienta. Dále v kapitole uvádím přehled některých dnes nabízených řešení datových schránek postavených na platformě MS SharePoint Services společně se stručným popisem jejich funkcí.

9.1.1 Řešení od společnosti Unicorn Systems

Společnost Unicorn Systems připravila řešení pro práci s datovými schránkami postavené na platformě Windows Sharepoint Services. Zákazníci využívající Windows Server 2003/2008 a Microsoft SQL Server 2005/2008, nemusí tedy kupovat žádný další software. Řešení představuje robustní základ, který je možno parametrizovat nebo dále rozšířit podle požadavků a ve velmi krátké době nasadit do firmy.

Klíčové funkčnosti nabízeného řešení jsou následující:

- Příjem zpráv. Příchozí zprávy mohou být notifikovány e-mailem.
- Odesílání zpráv. Zprávu lze sestavit, vybrat příjemce z adresáře, elektronicky podepsat oprávněnými osobami a odeslat (přímo nebo přes podatelnu).
- Konfigurovatelné workflow zpracování zpráv. Zprávy jsou automaticky nebo manuálně distribuovány odpovědným osobám.
- Konkrétní životní cyklus zprávy při přijímání (zpracování) i odesílání lze nastavit dle požadavků.
- Strukturovaný archiv. Po zpracování lze zprávy uložit do zvoleného místa v archivu (ten obsahuje veškeré doručené a odeslané zprávy). Přístup do archivu mají pouze oprávněné osoby (role).
- Možnost spravovat více datových schránek. Je možné pracovat s více datovými schránkami (v případě více společností).
- Auditování veškerých operací v systému. Lze sledovat činnosti uživatelů i operace nad zprávami.
- Otevřená architektura. Funkčnosti aplikace jsou dostupné přes standardní webové služby. To umožňuje integraci aplikace s dalšími systémy. [27]

9.1.2 Řešení od společnosti Syconix

Produkt E-GOV od společnosti Syconix pro SharePoint je ideální řešení pro komerční organizace. Umožní automatické převzetí, odesílání a dlouhodobou archivaci datových zpráv ve spisech. Řešení je modulární a snadno rozšiřitelné na plnohodnotnou spisovou službu a organizací správy dokumentů.

Řešení umožňuje následující funkce:

- Přihlášení do schránky certifikátem.
- Automatické přijetí a odeslání zpráv z jedné a více datových schránek.
- Načtení údajů z obálky a doplnění skartačního znaku s evidenčním číslem do formuláře zprávy v SharePoint.
- Archivace zprávy v SharePoint ve formátu ZFO potřebném pro autorizovanou konverzi automatický přesun starších zpráv do archivu.
- Variabilní distribuce zpráv a nastavení oprávnění pomocí workflow. [27]

9.1.3 Řešení od společnosti AEC

Řešení AEC ePodatelna přijímá a zpracovává elektronická podání i datové zprávy ze systému ISDS a následně je předává příslušným pracovníkům, případně DMS systému, který je společnost AEC schopna také implementovat na základě požadavků zákazníka. Propojení AEC ePodatelny na Microsoft Sharepoint umožní plně implementovat práci nad přijatými zprávami a dokumenty - procesy workflow, schvalování, uchovávání, evidence dokumentů a jejich metadat, kategorizace, verzování, sledování historie, fulltextové vyhledávání a další.

Přínosy řešení AEC ePodatelna:

- AEC ePodatelna pracuje jako jediné rozhraní pro komunikaci jak s fyzickými osobami, tak s právnickými osobami a orgány veřejné moci.
- AEC ePodatelna umožňuje provozovat vícero virtuálních ePodatelen prostřednictvím jedné aplikace pro detašovaná pracoviště/podřízené organizace.
- Řešení plně respektuje požadavky právních norem, které se vztahují k problematice elektronického podpisu, elektronických podatelen a datových zpráv v oblasti veřejné správy.
- Možnost snadného napojení na již používaný systém pro oběh dokumentů (DMS) nebo spisovou službu pomocí definovaného XML rozhraní. Podání a datové zprávy jsou pak dle předem nastavených pravidel předávány přímo do spisové služby/DMS systému. AEC ePodatelna podporuje napojení na spisové služby z produkce společností ICZ.
- Řešení AEC ePodatelna zahrnuje kvalitní technickou podporu a kontinuální vývoj systému s ohledem na změnu legislativy a doplňování nových funkcionalit. [27]

9.1.4 Řešení společností Diginta a Mainstream

Produkt POSTREGISTR.CZ připravený partnery Diginta a Mainstream respektuje všechny potřeby efektivní, jednoduché, přehledné a řízené distribuce datových zpráv uvnitř společnosti, ale také jejich kompletní a spolehlivou archivaci. Součástí řešení je i intuitivní a pro společnost snadno kontrolovatelné odesílání zpráv. Samozřejmostí je granulární nastavení práv.

- Řešení umožňuje následující funkce:
- Snadné a intuitivní použití ve známém webovém prostředí SharePoint.
- Přizpůsobení vnitřním organizačním pravidlům.
- Přehledná a řízená distribuce zpráv s kompletní sadou manažerských reportů.
- Archivace příchozích i odchozích zpráv, včetně přehledu „pohybu“ zprávy uvnitř společnosti.
- Granulární nastavení uživatelských práv. [27]

9.1.5 Řešení společnosti DIGI TRADE

DIGI TRADE nabízí několik řešení pro obsluhu Datových schránek. Konektor zdarma pro nejmenší zákazníky, řešení pro malé firmy a oddělení zaměřená na maximální jednoduchost i komplexnější systémy zahrnující workflow nad přijatými i odesílanými datovými zprávami.

Nabízené produkty:

- DIGI Konektor: se základní funkcionalitou je poskytován zdarma i pro komerční využití; je základním stavebním kamenem pro škálovatelné řešení nebo integraci se stávajícím dokument management systémem zákazníka.
- DIGI Konektor umožňuje propojení s Microsoft Exchange Server, Microsoft SharePoint Server, tj. s řešeními na standardní platformě jak v oblasti velkých, tak i malých a středních firem.
- Aplikace Datové schránky pro Microsoft SharePoint umožňuje jednoduchou instalací získat prostředí respektující principy bezpečnosti a role uživatelů, workflow pro zpracování datových zpráv a flexibilitu pro napojení na procesy organizace.
- Zásilky BOSS – komplexní aplikace sjednocující práci s Datovými zprávami a dalšími formami korespondence v papírové i elektronické podobě; může být implementována jako samostatná ASPX.NET aplikace nebo jako součást portálového řešení založeného na Microsoft Office SharePoint Server a to vše na nejnovější technologii Microsoft Silverlight. [27]

ZÁVĚR

Jak již bylo řečeno, společnost Bioveta a. s. je největším a nejvýznamnějším producentem veterinárních léčiv v České republice. V současné době ale naplno nevyužívá možností, které nabízejí datové schránky, ani možnosti systémů pro správu dokumentů (DMS). Na doručené datové zprávy je odpovídáno listinou formou, konkrétním pracovníkům jsou předávány také touto formou, i když by mohly být pomocí systému pro správu dokumentů (DMS) předávány automaticky konkrétnímu zaměstnanci v jejich elektronické podobě podle předem nastavených pravidel.

Není zde dokonale vyřešen ani oběh ostatních listinných dokumentů (pošta, vnitřní dokumenty organizace a další). Toto vše přispívá k nadměrnému zatížení administrativních pracovníků, kteří mají oběh dokumentace ve společnosti v náplni práce.

Cílem této práce tedy bylo navrhnout řešení implementaci datových schránek a s ní spojenou implementaci systému pro oběh dokumentů ve společnosti takovým způsobem, aby došlo k automatizaci a nastavení jasných pravidel pro oběh těchto dokumentů.

V práci byla dopodrobna probrána problematika datových schránek, včetně všech právních aspektů, které s užíváním datových schránek souvisí. Byla zde také zmíněna bezpečnostní doporučení nutná pro bezpečné přihlašování do datové schránky přes informační systém datových schránek (ISDS). Následoval popis současné implementace datových schránek ve společnosti Bioveta a. s. a rovněž analýza současného stavu oběhu pošty, příbalových informací a ostatních dokumentů uvnitř společnosti.

Diskutována byla také dnes nabízená řešení implementace datových schránek, od řešení pro nejmenší subjekty, až po komplexní řešení pro organizace s velkým pohybem dokumentace, mezi které firma Bioveta a. s. patří.

Firmě Bioveta a. s. jsem doporučil zavedení systému pro správu dokumentů (DMS) s funkcionalitou umožňující obsluhu datových schránek. V práci byly podrobně probrány přínosy, které může společnost po zavedení systému pro správu dokumentů očekávat.

Dále byly v rámci této diplomové práce zjištěny a definovány konkrétní požadavky vedení společnosti, které by mělo dané řešení systému pro oběh dokumentů splňovat.

Výsledkem práce je návrh, aby implementace systému pro správu dokumentů (obsahující řešení implementace datových schránek) byla založena na službách Microsoft SharePoint. Důvodem pro toto doporučení je, že společnost v současné době využívá technologie společnosti Microsoft, takže implementace systému pro správu dokumentů nebude tak obtížná a tedy i finančně nákladná. Dalším důvodem pro danou volbu byl fakt, že zaměstnanci společnosti jsou zvyklí na práci s programy od společnosti Microsoft, odpadne tedy nutnost seznámení se s novými aplikacemi.

Na závěr byly uvedeny příklady konkrétních systémů pro správu dokumentů s funkcionalitou pro datové schránky založených na službách Microsoft SharePoint.

ZÁVĚR V ANGLIČINĚ

Bioveta a. s. is the biggest and most important producer of veterinary medicine in the Czech Republic. However, the company is not utilizing all possibilities that data boxes can offer nor the possibilities of document management system (DMS). The answers to data messages that are delivered through data boxes are done in hard copy version. The distribution to individual employees is done in hard copy version as well despite documents can be delivered through DMS in electronic format in accordance with clearly pre-defined rules.

The system of hard copy documents distribution (mail, internal documents etc.) is not perfect either and causes overload of employees who are responsible for circulation of documentation within the company.

The aim of this thesis was to draft a data box implementation and document management system implementation within the company in order to automate the circulation of documents and set the criteria for such circulation.

The issue of data boxes has been reviewed in detail including legal aspects related to their usage. The thesis also deals with security recommendations for safe login in data box through data box information system. The practical part describes current implementation of data boxes in Bioveta a. s. and analyses current situation in mail, package inserts and other documents circulation.

Different possibilities of data box implementation have been discussed in the thesis as well. The solutions being described vary from the ones for small entities to complex solutions for large organisations with frequent document circulation such as Bioveta a. s.

The implementation of document management system including data box functionality has been recommended to Bioveta a. s. The benefits to be expected after the implementation of the document management system are described in the thesis too.

Requirements of the company management for document management system have been found out and defined. The thesis results suggest the implementation of the document management system (including data box implementation) to be based on Microsoft SharePoint Services. The rational for this recommendation is the fact that Bioveta a. s. uses Microsoft technologies thus the implementation of document management system will not

be that difficult and costly. The experience of most of the employees with Microsoft products is another reason why Microsoft application is recommended as there will be no need for long term training.

Concrete examples of document management system including data box functionality to be based on Microsoft SharePoint Services are given at the end of the thesis.

SEZNAM POUŽITÉ LITERATURY

[1] DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1. vyd. Brno: Computer Press, 2006. 534 s. ISBN 80-251-0828-7.

[2] SMEJKAL, Vladimír. Datové Schránky v Právním Řádu ČR. 1. vyd. Praha: ABF a.s., 2009. 176 s. ISBN 978-80-86284-78-1.

[3] MACKOVÁ, Alena, ŠTĚDROŇ, Bohumír. Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem včetně souvisejících zákonů a prováděcích předpisů. 1. vyd. Praha: Wolters Kluwer, 2009. ISBN 978-80-7357-472-7.

[4] ATREYA, Mohan, HAMMOND, Ben, PAINE, Stephen. Digital Signatures. 1. vyd. Londýn: McGraw-Hill, 2002. 368 s. ISBN 9780072194821.

[5] BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Olomouc: ANAG, 2008. 157 s. ISBN 978-80-7263-465.

[6] MAO, Wenbo. Modern Cryptography - Theory & Practice. New Jersey: Prentice-Hall, 2003. 1. vyd. 648 s. ISBN 0-13-066943-1.

[7] LIDINSKÝ, Vít, ŠVARCOVÁ, Ivana, BUDIŠ, Petr, LOEBL, Zbyněk, PROCHÁZKOVÁ, Barbora. eGovernment bezpečně. 1. vyd. Praha: Grada, 2008. 160 s. ISBN 978-80-247-2462-1.

[8] SMEJKAL, Vladimír. Elektronický podpis jako nástroj pro zvýšení bezpečnosti informačních systémů. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.vutium.vutbr.cz/tituly/pdf/info/80-214-2447-8.pdf

[9] Oficiální informace o datových schránkách od Ministerstva vnitra ČR. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.mvcr.cz/datove-schranky.aspx.

[10] Oficiální informace o datových schránkách od Ministerstva vnitra ČR. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.datoveschranky.info/.

[11] Informace o datových schránkách na serveru lupa.cz. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.lupa.cz/r/datove-schranky/.

[12] Informace společnosti Microsoft k implementaci datových schránek. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.microsoft.com/cze/datoveschranky/.

[13] Informace zpravodajského portálu časopisu IT Systems k implementaci datových schránek. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.systemonline.cz/datove-schranky/.

[14] Oficiální informace o společnosti Bioveta a. s. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.bioveta.cz/cs/veterinarni-divize/o-spolecnosti/.

[15] Informace společnosti Actis, s. r. o. k jejich aplikaci Actis Datové schránky. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.actis.cz/datove-schranky.

[16] Informace společnosti AMOS Software, spol. s r. o. k aplikaci Multischránka. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.multischranka.cz/.

[17] Informace společnosti Microsoft k aplikaci Microsoft Outlook konektor. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.microsoft.com/cze/datoveschranky/zivnostnik/.

[18] Informace společnosti AiP Safe, s. r. o. k datovým schránkám a DMS sytému SAFE. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.aipsafe.cz/cs.

[19] Informace společnosti AEC, spol. s. r. o. o produktu ePodatelna. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.aec.cz/cz/produkty/epodatelna.

[20] Oficiální informace České pošty s. p. k datovým schránkám. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.ceskaposta.cz/cz/sluzby/datove-schranky/default.htm

[21] Oficiální inormace České pošty s. p. k Czech POINTu. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.ceskaposta.cz/cz/sluzby/czech-point/default.htm.

[21] Úplné znění zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb08300&cd=76&typ=r.

[22] Úplné znění zákona č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona č. 300/2008 Sb. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb08300&cd=76&typ=r.

[23] Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00227&cd=76&typ=r.

[24] Úplné znění vyhlášky č.193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.sagit.cz/pages/sbirkatxt.asp?cd=76&typ=r&zdroj=sb09193.

[25] Úplné znění vyhlášky č.194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek. [online]. 2010 [cit. 2010-4]. Dostupné na WWW: http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb09194&cd=76&typ=r.text

[26] Informace o systémech pro správu dokumentů. [online]. 2010 [cit. 2010-5]. Dostupná na WWW: http://cs.wikipedia.org/wiki/Spr%C3%A1va_dokument%C5%AF.

[27] Informace společnosti Microsoft o konkrétních řešeních implementace datových schránek. [online]. 2010 [cit. 2010-5]. Dostupné na WWW: http://www.microsoft.com/cze/datoveschranky/firma/.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A. S. Akciová společnost.

B2B Z anglického Business to Business, označení pro obchodní vztahy mezi obchodními společnostmi.

CD Z anglického Compact Disc, datové médium.

CRC Z anglického Cyclic Redundancy Check, kontrolní součet.

CRL Z anglického Certificate Revocation List, neboli seznam zneplatněných certifikátů.

DES Z anglického Data Encryption Standard, typ šifrovacího algoritmu.

DMS Z anglického Document Management Systém, systém pro správu dokumentů.

DS Datová schránka.

EDM Z anglického Electronic Document Management, systém pro správu dokumentů.

eGA Z anglického electronic Governament, zkartka označující v České republice zákon o elektronické komunikaci se státní správou.

EXE Z anglického executable, spustitelný.

FIPS Z anglického Federal Information Processing Standards, federální informačně procesní standardy (v USA).

GDP Z anglického Good Distribution Practise, správné distribuční praxe .

GLP Z anglického Good Laboratory Practice, správná laboratorní praxe.

GMP Z anglického Good Manufacturing Practice, správná výrobní praxe.

HW Z anglického Hardware, technickém vybavení počítače.

ISDS Informační systém datových schránek.

MB Z anglické Mega Byte, jednotka informace.

MD5 Z anglického Message Digest 5, typ hashovacího algoritmu.

MS	Microsoft, název americké počítačové firmy.
MVČR	Ministerstvo vnitra České republiky.
OR	Obchodní rejstřík.
OVM	Orgán veřejné moci.
PDF	Z anglického Portable Document Format, přenosný formát dokumentů.
PIN	Z anglického Personal Identification Number, osobní identifikační číslo.
PO	Právnická osoba.
PUK	Z anglického Personal Unblocking Key, osobní odblokovávající klíč.
RSA	Typ šifrovacího algoritmu, pojmenovaný podle iniciál jeho autorů Rivest, Shamir, Adleman.
SHA-1	Z anglického Secure Hash Algorithm, typ hashovacího algoritmu.
S. P.	Státní podnik.
SQL	Z anglického Structured Query Language, strukturovaný dotazovací jazyk.
TSA	Z anglického Time Stamping Autority, autorita časových razítek.
USB	Z anglického Universal Serial Bus, univerzální sériová sběrnice.
ÚSKVBL	Ústavu pro státní kontrolu veterinárních biopreparátů a léčiv.
XML	Z anglického Extensible Markup Language, rozšiřitelný značkovací jazyk.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Diplomová práce je bez příloh.