VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

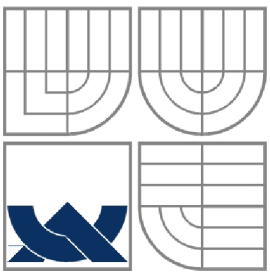
ELEKTRONICKÁ PODATELNA PRO OBECNÍ ÚŘADY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

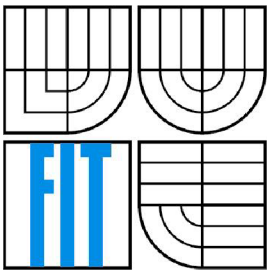
AUTOR PRÁCE
AUTHOR

KAREL STRÁNSKÝ

BRNO 2007



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ELEKTRONICKÁ PODATELNA PRO OBECNÍ ÚŘADY

ELECTRONIC REGISTRY FOR LOCAL AUTHORITY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR

KAREL STRÁNSKÝ

VEDOUCÍ PRÁCE
SUPERVISOR

MGR. MAREK RYCHLÝ

BRNO 2007

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav informačních systémů Akademický rok 2006/2007

Zadání bakalářské práce

Řešitel: **Stránský Karel**
Obor: Informační technologie
Téma: **Elektronická podatelna pro obecní úřady**
Kategorie: Databáze

Pokyny:

1. Seznamte se s platnou legislativou ČR o elektronických podatelnách a souvisejícími předpisy.
2. Analyzujte příslušné předpisy a sestavte specifikaci inf. systému elektronické podatelny obecního úřadu. Ve specifikaci vyznačte minimální požadavky tak, jak jsou vyžadovány legislativou, a požadavky související s elektronickým podpisem.
3. Navrhněte inf. systém elektronické podatelny. Systém umožní elektronicky přijímat datové zprávy v běžně rozšířených formátech pomocí webového rozhraní i elektronické pošty, sledovat stav jejich zpracování a vyřízení. Navrhněte funkce pro podpis a ověření zpráv pomocí elektronického podpisu.
4. Implementujte podatelnu jako webovou aplikaci.
5. Diskutujte výsledky práce a navrhněte možná rozšíření.

Literatura:

- vyhláška č. 496/2004 Sb., o elektronických podatelnách.
- zákon č. 227/2000 Sb., o elektronickém podpisu, a prováděcí předpisy.
- existující implementace elektronických podatelen
- Gamma, E.: Design Patterns -- Elements of Reusable Object-Oriented Software, Massachusetts, Addison-Wesley, 1997. 395 s.
- UML Resource Page. [http://www.uml.org/]

Při obhajobě semestrální části projektu je požadováno:

- Bod 1 a 2.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním paměťovém médiu (disketa, CD-ROM), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Rychlý Marek, Mgr.**, UIFS FIT VUT
Datum zadání: 1. listopadu 2006
Datum odevzdání: 15. května 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Ing. Jaroslav Zendulka, CSc.
vedoucí ústavu

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami

1. Pan

Jméno a příjmení: **Karel Stránský**
Id studenta: 88705
Bytem: Petrovice u Karviné 207, 735 72 Petrovice u Karviné
Narozen: 10. 09. 1984, Karviná
(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta informačních technologií
se sídlem Božetěchova 2/1, 612 66 Brno, IČO 00216305
jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....
(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
bakalářská práce

Název VŠKP: Elektronická podatelna pro obecní úřady
Vedoucí/školitel VŠKP: Rychlý Marek, Mgr.
Ústav: Ústav informačních systémů
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:
tištěné formě počet exemplářů: 1
elektronické formě počet exemplářů: 2 (1 ve skladu dokumentů, 1 na CD)

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizování výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti:
   - ☒ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

.....	.....
Nabyvatel	Autor

Abstrakt

Bakalářská práce „Elektronická podatelna pro obecní úřady“ je zaměřena na využití elektronických podatelen pro elektronickou komunikaci občanů s orgány veřejné správy. První část práce popisuje legislativní stránku související s e-podatelnami, princip jejich fungování a důležité požadavky, jenž jsou na e-podatelny kladeny. Dále jsou zahrnuty základní informace o elektronickém podpisu, jeho vytváření a ověřování, o certifikátech a certfikačních autoritách a je popsáno využití digitálního podpisu při komunikaci přes elektronickou podatelnu. Druhá část práce je věnována konkrétnímu návrhu a řešení jednotlivých problémů implementovaného ukázkového systému elektronické podatelny.

Klíčová slova

Elektronická podatelna, elektronický podpis, digitální podpis, elektronická značka, časové razítko, certifikát, certifikační autorita, datová zpráva, šifrování, šifrovací metody, hashovací funkce

Abstract

Bachelor thesis „Electronic registry for local authority“ is focused on usage of electronic registries for electronic communication between citizens and public authority. The first part describes the legislative page incidental with e-registries, principles of their functionality, and important requierements which are set on e-registiries. Furthermore elementary electronic signature‘s informations are included, along with creation and verification, and informations about certificates and certification authorities. The usage of digital signature at communication with electronic registry is also described. The second part is used to present particular koncept of implemented sample electronic registry’s system, and the solution of picked problems.

Keywords

Electronic registry, electronic signature, digital signature, electronic mark, time stamp, certificate, certification authority, data message, cryptography, encryption methods, hash function

Citace

Karel Stránský: Elektronická podatelna pro obecní úřady, bakalářská práce, Brno, FIT VUT v Brně, 2007

Elektronická podatelna pro obecní úřady

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Mgr. Marka Rychlého.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Jméno Příjmení
Datum

Poděkování

Tímto bych chtěl poděkovat vedoucímu své bakalářské práce panu Mgr. Marku Rychlému za jeho podnětné rady, poskytnutí informačních pramenů a odborné vedení celé práce.

Obsah

Úvod

V současné době je využívání internetu obvyklou součástí aktivity mnoha lidí. A už dávno se nejedná o pouhé získávání informací, ale standardem se stala i tzv. elektronická komunikace, nahrazující osobní přítomnost na tom kterém místě. Bankovní převody, placení inkasa, online nákupy apod. se stávají běžnou praxí, díky níž lze ušetřit peníze a hlavně čas. V rámci toho trendu se dostává do popředí zájem státu, umožnit lidem elektronickou formou komunikovat se státní správou – úřady. Z tohoto důvodu se na scéně objevují tzv. elektronické podatelny, díky nimž může kterýkoliv občan vyřídit veškeré potřebné formality bez nutnosti osobní přítomnosti na úřadech.

Tato bakalářská práce je věnována právě problematice elektronických podatelen pro obecní úřady (resp. orgánů veřejné správy obecně), jejího využití v oblasti odesílání a přijímání elektronických dokumentů a dalšími důležitými náležitostmi, které s danou problematikou úzce souvisejí. Zejména se jedná o téma elektronického (digitálního) podpisu, o platnou legislativu České republiky vztahující se jednak k výše zmíněnému elektronickému (digitálnímu) podpisu a rovněž zákony a předpisy zabývající se samotnou oblastí elektronických podatelen určených pro státní správu.

Téma jsem si zvolil pro jeho širší možnosti uplatnění. Dochází zde k prolínání informačních technologií a kryptografie, což jsou věci, které se mohou v budoucnu uplatnit v mnoha sférách, nejenom při elektronické komunikaci občana s úřadem.

Bakalářská práce je rozdělena do 7 hlavních oddílů. V tom prvním se věnuji legislativnímu pozadí elektronických podatelen v ČR. V dalším oddíle je popisována podstata a princip fungování elektronických podatelen a typům zasílaných datových zpráv. Třetí oddíl se zabývá teorií tvorby a ověřování elektronického podpisu (šifrování, hashování) a jeho použití společně s certifikáty v komunikaci s orgány veřejné správy. Ve čtvrtém oddílu se věnuji návrhu ukázkového systému elektronické podatelny. Pátý oddíl obsahuje konkrétní popis řešených problémů v samotné implementaci. V posledních dvou kapitolách je shrnutí výsledků práce a nástin dalšího vývoje a rozšíření vytvořeného systému.

1 Legislativa e-podatelen v ČR

Je pochopitelné, že pokud chceme stavět na stejnou váhu papírové a elektronické podání, musí být oblast elektronických podatelen ošetřena nejen technicky, ale také legislativně takovým způsobem, aby nedocházelo z právního hlediska k nežádoucím skutečnostem.

V této kapitole je proto uveden a stručně nastíněn obsah několika stěžejích právních norem, které se týkají provozu elektronických podatelen a upravující povinnosti občana a úřadu při vzájemné elektronické komunikaci.

1.1 Hlavní legislativní normy

Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č.227/2004 Sb., o elektronickém podpisu a o změně některých dalších zákonů stanovuje povinnost orgánů veřejné moci zřídit jednu nebo více elektronických podatelen (popřípadě zajistit přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny jiného orgánu). Určuje taktéž povinnost vybavit zaměstnance, právně způsobilé k úkonům v oblasti orgánů veřejné moci, kvalifikovanými certifikáty (zaručeným elektronickým podpisem) [1].

Vyhláška č. 496/2004 Sb., o elektronických podatelnách ustanovuje postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny a struktury údajů kvalifikovaného certifikátu, na základě kterých je možné podepisující osobu při přijímání datových zpráv prostřednictvím elektronické podatelny jednoznačně identifikovat. Vyhláška říká, jakým způsobem má být nakládáno s doručenou datovou zprávou (podáním) a jak odesílatele datové zprávy informovat o doručení, popřípadě jej uvědomovat o nesrovnalostech v učiněném elektronickém podání. Vyhláška dále upravuje způsob odesílání datových zpráv ze strany orgánů veřejné moci a jejich následné evidence [2].

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb. 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 [3].

1.1.1 Další právní normy

Níže je uveden soupis několika dalších právních norem souvisejících s problematikou elektronických podatelen:

- Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy.
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

2 Elektronická podatelna

2.1 Co je elektronická podatelna

Elektronická podatelna (e-podatelna) je ve své podstatě elektronickou náhražkou (obdobou) klasických kamenných podatelen na úřadě s obsluhujícím úředníkem na přepážce. Lze ji v praxi chápat jako počítač s programem pro její provoz. Elektronická podatelna se tak stává pracovištěm orgánů veřejné správy (kupříkladu obecního úřadu), které je určeno pro příjem (a následnou evidenci) a odesílání datových zpráv (elektronických písemností) a pomocí níž je možné tyto došlé zprávy potvrzovat.

Elektronická podatelna je určena všem občanům (fyzickým osobám), kteří chtějí komunikovat s orgánem veřejné správy elektronickou formou [4].

2.1.1 Elektronická komunikace

Obecně může mít elektronická komunikace mezi občanem a orgánem veřejné správy (např. obecním úřadem) několik podob.

Jednou z možných forem je ta, kdy se občan fyzicky dostaví na patřičný obecní úřad s příslušným podáním, ale daný dokument či dokumenty nemá v papírové podobě, ale má je uloženy na nějakém datovém nosiči (CD, DVD, disketa). Daný datový nosič pak předá k tomu pověřenému pracovníkovi, který podání následně vyřídí. Jelikož je podávající na úřadě fyzicky přítomen, může být jeho totožnost ověřena stejným způsobem jako u klasického „papírového“ podání, tedy vlastnoručním podpisem podávajícího.

Vzniká ovšem potřeba „zafixovat“ obsah podání, tak aby nemohlo být v budoucnu změněno a nemohlo být zpochybněno to, co dané podání obsahuje (nutné pro vyhnutí se případným sporům občana, jenž tvrdí, že uvedl něco jiného, než udává úřad). Velice důležitá je také norma pro čitelnost elektronického podání, tzn. podání musí být v takovém datovém formátu, který úřad akceptuje.

Nejčastější podobou elektronické komunikace je však situace, kdy se občan na úřad fyzicky nedostaví, ale patřičnou písemnost doručí pomocí elektronické pošty, nebo přes webové rozhraní daného úřadu. I zde je nutnost „fixace“ obsahu a čitelnosti, ale navíc zde vzniká potřeba bezpečného a nezpochybnitelného ověření totožnosti podávajícího. To je nutné pro ošetření případné možnosti, že by podávající v budoucnu popíral fakt, že podání učinil [4].

2.2 Princip fungování elektronické podatelny

Elektronická podatelna se skládá z několika elementů. Na jedné straně stojí klient, jehož snahou je učinit elektronické podání. Na straně druhé existuje systém, který zpracovává přijaté datové zprávy, a pověření pracovníci orgánu veřejné správy, jenž mají na starosti samotné vyřizování podaných elektronických písemností.

2.2.1 Klient

Klient (resp. odesílatel) se k webovému rozhraní elektronické podatelny daného úřadu připojí prostřednictvím svého internetového prohlížeče, jehož provoz zajišťuje právě tento konkrétní úřad. Zde získá veškeré informace související s registrací, posíláním podání, popřípadě zpětné kontroly stavu jeho podání.

Chce-li uživatel učinit elektronické podání, musí být zaregistrován v systému a zejména musí vložit svůj platný certifikát vydaný uznávanou certifikační autoritou. *Certifikát je nutný pro ověření totožnosti odesílatele a platnosti a jednoznačnosti podané elektronické písemnosti.* Po odeslaní daného podání může uživatel kdykoliv přes webové rozhraní úřadu kontrolovat, v jakém stádiu vyřízení se momentálně nachází. Klient má samozřejmě možnost sledovat stav kteréhokoliv svého podání, jenž v minulosti provedl.

2.2.2 Automat

Automatický systém pracuje na serveru úřadu. Tento systém má na starosti přijímání, kontrolu a následnou evidenci došlých datových zpráv. Kontrola došlé datové zprávy se skládá z následujících bodů:

- Kontrola přítomnosti škodlivého kódu softwaru (počítačový vir, nežádoucí spam apod.), pomocí stávajících a dostupných antivirových a antispamových nástrojů. Každá takto infikovaná datová zpráva se chápe jako nevyžádaná a v důsledku toho nedochází k jejímu dalšímu zpracovávání.
- Kontrola pravosti a platnosti elektronického podpisu datové zprávy. Pokud došlo k úspěšnému ověření podpisu, je podání dále zpracováváno, v opačném případě dochází k zastavení zpracovávání, protože se objevuje důvodné podezření, že se s zprávou bylo nějakým způsobem manipulováno a je tak zpochybněna její důvěryhodnost.

Každé příchozí podání (tedy jeho veškerý obsah) je systémem uložen do databáze příchozích podání a je mu automaticky přiděleno unikátní identifikační číslo, pod kterým je podání po celou dobu svého životního cyklu vedeno.

Systém musí rovněž podle zákona informovat odesílatele datové zprávy o jejím úspěšném (či neúspěšném) přijetí do systému elektronické podatelny. To činí tzv. doručovací zprávou, která je v podobě emailové zprávy zaslána na emailovou adresu odesílatele (pokud je možné takovouto adresu zjistit). V případě, že odesílatel danou doručovací zprávu neobdrží, měl by odeslanou datovou zprávu považovat za nedoručenou.

2.2.3 Pracovník úřadu

Pověřený pracovník orgánu veřejné správy (úředník) zastupuje v systému elektronické podatelny roli úředníka, který v klasické kamenné podatelně přijímá podání (tzn. pracovník na přepážce). Jeho úkolem je příchozí podání kontrolovat (zjišťování korektnosti uvedených údajů v písemnostech) a předávat je k vyřízení tomu určeným složkám úřadu.

Pokud pracovník úřadu zjistí nesrovnalosti v podání, je povinen o těchto skutečnostech informovat odesílatele a vyžadovat nápravu uvedených dat. Každý takto pověřený pracovník úřadu je vybaven platným kvalifikovaným certifikátem (vydávaný akreditovaným poskytovatelem certifikačních služeb) a zaručeným elektronickým podpisem, pomocí něhož podepisuje informační zprávy (jejich obsahem jsou informace o nesrovnalostech v údajích podání), které zasílá odesílateli elektronického podání.

2.3 Datové zprávy

Datovou zprávou se rozumějí elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou.

2.3.1 Příjem datových zpráv na datových nosičích

Datové zprávy však nemusí být podatelnou přijímány pouze elektronickou cestou. Odesílatel může, jak již bylo zmíněno, podávané datové zprávy uložit na datový nosič (běžně disketa, CD) a ten poté osobně předat na podatelně. Proto je nutné, aby úřad zajistil „sběr“ těchto nosičů, a tedy uvedl dobu a místo, kdy a kde je možné takovéto nosiče s elektronickými dokumenty úřadu předávat. Tyto dokumenty se řídí stejnými pravidly jako dokumenty předávané elektronickou formou.

2.3.2 Formáty datových zpráv

Datové zprávy (elektronické písemnosti), které uživatel posílá do elektronické podatelny, musejí být takovém formátu, které daná podatelna akceptuje.

Seznam takovýchto formátů musí být uveřejněn na stránkách podatelny. Většinou se jedná o běžně používané formáty. Akceptované formáty mohou být:

- HTML (hypertextový dokument)
- DOC (soubory softwarového produktu Microsoft Word)
- XLS (soubory softwarového produktu Microsoft Excel)
- PDF (soubory softwarového produktu Adobe Acrobat)
- RTF (rich text format)
- TXT (prostý text)
- JPG (grafický formát)

Kromě výše uvedených se samozřejmě mohou zasílat i další běžně používané formáty. Je důležité řídit se pokyny uvedených na stránkách konkrétní podatelny [5].

2.3.3 Velikost datových zpráv

Dalším omezením při přijímání datové zprávy je její velikost. Datová zpráva včetně všech svých příloh pak nesmí tuto hodnotu přesáhnout. Informace o maximální přípustné velikosti je opět uvedena na internetových stránkách podatelny (obvykle se maximální hodnota kapacity pohybuje mezi 4 až 8 MB).

2.3.4 Typy datových zpráv

Datové zprávy, resp. příchozí podání doručené do systému elektronické podatelny, mohou být několika typů [6]:

- Nepodepsaná zpráva s jednou, nebo více podepsanými přílohami.
- Podepsaná zpráva s jednou nebo více podepsanými či nepodepsanými přílohami.
- Podepsaná a šifrovaná zpráva obsahující jednu nebo více příloh, které mohou být podepsané a šifrované.
- Nějaká z výše popsaných kombinací opatřená navíc jedním nebo více časovými razítky.

2.3.5 Doručovací zprávy

Jak již bylo zmíněno, doručovací zprávy (doručenky) slouží jako informace pro odesílatele, že jeho elektronické podání bylo přijato do systému elektronické podatelny. Orgán veřejné správy má povinnost neprodleně zaslat tuto doručovací zprávu při přijetí podání.

2.3.5.1 Požadavky na doručovací zprávu

Ze zákona [2] musí být součástí každé zprávy o potvrzení minimálně tyto údaje:

- Datum a čas, kdy byla datová zpráva doručena do systému elektronické podatelny.
- Uznávaný elektronický podpis oprávněného zaměstnance orgánu veřejné moci nebo uznávanou elektronickou značku orgánu veřejné moci.
- Identifikátor datové zprávy, který mu byl přidělen systémem elektronické podatelny.
- Připojený ověřený platný a důvěryhodný digitální podpis.

3 Elektronický podpis

3.1 Co je elektronický podpis

S využíváním elektronických podatelen úzce souvisí tzv. elektronický (digitální) podpis. Elektronický podpis je jedním z hlavních nástrojů identifikace (zjišťování totožnosti) a autentizace (ověřování totožnosti) osob v prostředí internetu.

Jelikož je elektronická podatelna založena na principu přijímání datových zpráv (elektronických dokumentů) bez toho, aby musel být odesílatel zprávy fyzicky přítomen na úřadě, je potřeba zajistit, aby byla přijímaná zpráva nezpochybnitelná a nepopiratelná a mohlo být jednoznačně určeno, která osoba daný elektronický dokument poslala. Zároveň je nutné zajistit skutečnost, že obsah přijímaného dokumentu je skutečně takový, který občan schválil a odeslal. To znamená, že dokument nebyl později nějakou neoprávněnou osobou jakkoliv modifikován a je tedy ověřena jeho pravost. K zajištění těchto výše uvedených požadavků se výborně hodí a je v praxi používána právě technologie elektronického (digitálního) podpisu.

Aby mohl mít elektronický podpis stejnou váhu (byl tedy právně akceptovatelný) a byl funkčně ekvivalentní ke klasickému vlastnoručnímu podpisu, musí být legislativně ošetřen. Pojem elektronický podpis byl v České republice uveden v zákoně č. 227/2000 Sb., o elektronickém podpisu. Podle výkladu tohoto zákona se *elektronickým podpisem rozumí údaje v elektronické podobě, jenž jsou připojené k datové zprávě, nebo jsou s ní logicky spojené a slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*.

Z litery zákona jasně vyplývá, že elektronický podpis nepředstavuje vlastnoručně napsaný podpis převedený digitální podoby. Jde o speciálně vygenerovanou množinu dat, která je pro každý elektronický dokument jedinečná a která se k této datové zprávě připojuje, tzn. podpis a podepisovaná zpráva jsou dvě samostatné jednotky [3].

3.1.1 Elektronický podpis X digitální podpis

Ačkoliv mohou pojmy elektronický podpis a digitální podpis splývat v jedno (a v některých pramenech se mezi nimi vskutku příliš rozdíl nedělá), ve skutečnosti bychom měli porozumět jejím rozdílům, protože se nejedná o zcela ekvivalentní záležitosti.

Pod pojmem elektronický podpis rozumíme obecný termín pro prokazování totožnosti elektronickou formou. V podstatě se jedná o široké spektrum kontroly identity jedince. Pod elektronický podpis tak spadá například snímání oční duhovky, snímání otisků prstů nebo jim podobných technik.

Digitální podpis je naopak termín, který spadá pod elektronický podpis (tzn. je jeho podmnožinou, jeho složkou). Technologie digitálního podpisu je postavená na bázi šifrování dokumentů (záznamů) v digitální formě.

Jak jsem již zmínil, jsou oba pojmy (digitální a elektronický podpis) v praxi velice často zaměňovány a považovány v podstatě za totožné. Proto hovoří-li se o elektronickém podpisu, bývá obvykle myšlen právě podpis digitální [6].

3.1.2 Elektronická značka

Elektronická značka funguje podobném principu jako elektronický (digitální) podpis. Hlavním rozdílem je právní charakter věci. Zatímco elektronický podpis je určen pro používání fyzickou osobou, elektronickou značku může navíc používat i osoba právnická či orgán státní správy pro automatické hromadné označování dokumentů. Elektronická značka tak může být v praxi využitá například právě v elektronických podatelnách při automatickém generování odpovědí ze strany podatelny, které probíhají bez zásahu oprávněné označující osoby.

Elektronická značka je v podstatě automatem vytvářený elektronický podpis a lze ho chápat jako úřední razítko. K vytváření elektronické značky je zapotřebí systémového certifikátu, který definuje identitu označující osoby. Tato osoba nese zodpovědnost za používání takové techniky, jenž zaručí veškerou bezpečnost, zejména ochranu dat sloužících pro vytváření elektronické značky [7].

3.1.3 Časové razítko

Časové razítko slouží jako doplněk k digitálnímu podpisu. Jelikož samotný digitální podpis v sobě nenese žádný údaj o době jeho vytvoření, používá se časové razítko k jednoznačnému potvrzení, že daná označovaná datová zpráva existovala minimálně v době před uvedeným časovým údajem.

Vydávání časových razítek má na starosti důvěryhodná autorita časových razítek, fungující na obdobném principu jako certifikační autorita. Žadatel o časové razítko odešla žádost autoritě společně s otiskem datové zprávy, k níž má být údaj o čase vložen. Autorita zkontroluje správnost dat a pokud vše souhlasí, posílá zpátky digitálně podepsaný původní otisk zprávy doplněný o časový údaj.

Ověření časového razítka je založeno na stejné bázi jako kontrola digitálního podpisu. Vypočítá se otisk (hash) daného souboru a zjistí se hash hodnota dešifrovaná z časového razítka (k tomu je zapotřebí certifikát autority časových razítek). Jsou-li oba otisky shodné, znamená to, že nedošlo k porušení časového razítka a časový údaj je tak platný [8].

3.2 Technologie tvorby digitálního podpisu

Abychom mohli pochopit princip elektronického podepisování, musíme nejdříve zabrousit a ve stručnosti popsat oblasti, které s touto problematikou souvisejí a na nichž je vše postaveno.

3.2.1 Šifrování

Základním stavebním prvkem a vůbec podstatou elektronického (digitálního) podepisování je šifrování resp. šifrování dokumentů (zpráv). Věda zabývající se touto oblastí se nazývá kryptologie. Kryptologie jako taková zahrnuje dvě podtřídy - kryptografii (šifrování zpráv, utajování) a kryptoanalýzu (dešifrování, luštění šifrovaných zpráv).

Šifrování obecně pojednává o ukrytí informací před jejich nevyžádaným únikem a případným zneužitím, ve smyslu převedení prostého (tedy běžně čitelného) textu do podoby šifrovaného textu (běžným způsobem nečitelného). Jako prostředek, kterým dosahujeme těchto požadavků, slouží šifra, neboli matematická metoda (algoritmus), jejíž pomocí (a v součinnosti s šifrovacím klíčem) jsme schopni zprávu znečitelnit. K tomu abychom následně mohli dešifrovat, musíme znát nejen onen matematický algoritmus, ale rovněž šifrovací klíč [9].

3.2.2 Šifrovací metody

Metody sloužící pro šifrování dělíme do několika celků. Tím prvotním rozdělením je možné chápat metody jednosměrné a obousměrné. Pod termínem jednosměrná šifrovací metoda rozumíme postup, kterým je možné zašifrovat určitou zprávu, ovšem bez možnosti zpětného procesu, tedy dešifrování zprávy. U tohoto typu šifrování zpravidla nepotřebujeme žádný klíč. Jednosměrná šifrovací metoda se obvykle používá pro ukládání přístupových hesel (nelze je tedy zjistit, ale je možné je porovnávat a následně ověřovat). Na druhé straně obousměrné šifrování již probíhá za účasti šifrovacího klíče a díky tomu, že jsme schopni provést zpětný chod (dešifrovat), používáme ji všude tam, kde potřebujeme získat původní podobu zprávy. Obousměrné metody v zásadě rozlišujeme na symetrickou a asymetrickou [10].

3.2.2.1 Symetrické šifrování

Metoda symetrické šifry je postavena na myšlence vlastnit jediný šifrovací klíč. V praxi to znamená, že pro zašifrování nějaké zprávy použijeme tento klíč a ten samý klíč poté uplatníme i při následném dešifrování. Již na první pohled má tento způsob šifrování jednu velkou nevýhodu a to nutnost zajistit bezpečný přenos šifrovacího klíče mezi dvěmi koncovými entitami (odesílatelem a příjemcem). Jakmile totiž dojde k úniku šifrovacího klíče, je vysoce pravděpodobné, že zašifrovaná zpráva může být kdykoliv přečtena třetím nežádoucím subjektem. Je proto nutné zajistit nějaký důvěryhodný a bezpečný kanál pro předání klíče. Díky uvedeným faktům nastává další problém a to ten, že nejde

jednoznačně splnit požadavek nezpochybnitelnosti, protože nelze vždy jednoznačně určit, kdo zprávu poslal a kdo ji převzal.

Výhodou symetrické šifry je její rychlost (vhodné pro šifrování objemnějších dat) a skutečnost, že i při relativně malé délce klíče je časově velmi náročné tento klíč odhalit (doba potřebná k dešifrování roste s délkou klíče velice rychle).

V současné době k nejznámějším symetrickým šifrovacím algoritmům řadíme DES (vyvinut v laboratořích IBM v sedmdesátých letech, používá 56 bitový klíč), Triple-Des (řeší bezpečnostní nedostatky DESu, používá taktéž klíč o délce 56 bitů), IDEA (je patentován, využívá 128 bitového klíče) a BlowFish (délka klíče v rozmezí 32 až 448 bitů, obvykle pracuje se 128 bitovým klíčem). V dnešní době se díky výraznému nárůstu výkonu výpočetní techniky stal algoritmus DES z pohledu bezpečnosti již nedostačující [10, 11].

3.2.2.2 Asymetrické šifrování

Metoda asymetrického šifrování je poněkud sofistikovanější. Mezi nejpodstatnější rozdíl oproti symetrickému šifrování se řadí přítomnost dvojice šifrovacích klíčů. Jeden z nich je klíč soukromý (nebo též privátní) a druhý klíč veřejný. Oba tyto klíče jsou spárovány, takže zprávu, která je zašifrována jedním z této dvojice klíčů, je možné dešifrovat pouze s pomocí druhého klíče z páru (pro dešifrování zprávy šifrované privátním klíčem použijeme klíče veřejného a naopak).

Oba tyto klíče si generuje uživatel pomocí k tomu určených a běžně dostupných softwarových produktů (např. SSL). Dnes se standardně používají klíče o délce 1024 nebo 2048 bitů. Podstata spočívá v tom, že soukromý klíč vlastní pouze jeho majitel a ten má za povinnost učinit veškerá bezpečnostní opatření, která zabrání jeho úniku. Na druhé straně klíč veřejný je již podle svého názvu veřejně přístupný a kdokoliv si jej tak může zjistit. Díky tomuto můžeme v reálu uplatnit skutečnost, jenž říká, že u zprávy, kterou dešifrujeme něčím veřejným klíčem, můžeme prohlásit, že známe jejího odesílatele (tím je vlastník privátního klíče). Takovou zprávu pak lze v jistém slova smyslu brát jako podepsanou.

Jelikož asymetrická metoda šifrování pracuje se dvěmi klíči, je výhodou absence vytváření bezpečnostního kanálu pro přenos šifrovacího klíče. Privátní klíč se nikam neposílá a veřejný lze bez obav poskytnout komukoliv, protože je takřka nemožné v rozumném časovém období odvodit z veřejného klíče privátní.

Nevýhodu této metody je její rychlost. Asymetrická je oproti té symetrická až tisíckrát pomalejší. To jí dělá prakticky nepoužitelnou pro šifrování velkého objemu dat. Další věcí, kterou je potřeba brát v úvahu, je ověření pravosti klíče, tedy jednoznačné určení identifikace vlastníka veřejného klíče. K tomu nám slouží tzv. certifikáty a certifikační autority.

Mezi nejvýznamnější asymetrické algoritmy patří RSA (iniciály autorů Rivest, Shamir, Adleman, vznik v roce 1977) a DSA (Digital Signature Algorithm, vznik v roce 1991) [10, 11].

3.2.3 Hashovací funkce

Abychom mohli přejít k problematice tvorby digitálního podpisu, je potřeba se ještě zastavit u pojmů hash a hashovací funkce.

Hashem rozumíme otisk nějaké datové zprávy (zjednodušené schéma principu vytváření otisků z datové zprávy je znázorněno na obrázku 1). Hashovací funkce má tedy za úkol vytvořit ze vstupních dat jejich otisk, který jednoznačně popisuje a je spjat s onou množinou dat. Obecně je hashovací funkce jakási speciální jednosměrná matematická metoda, která z proměnných vstupních veličin určité délky vygeneruje výstupní hodnotu pevně dané délky, která je považována za jedinečný otisk vstupních dat.

Důležitou podmínkou hashovací funkce je právě jednosměrnost. Z toho jednoznačně vyplývá, že k takovéto funkci neexistuje funkce inverzní, díky níž by se dalo zpětně zjistit podobu vstupních dat (například obsah dokumentu).

Obrázek 1: Schéma principu tvorby otisku zprávy

Dalším podstatným faktorem, který musí hashovací funkce splňovat, je odolnost vůči nalezení kolize. Nemělo by tedy být možné najít k jednomu dokumentu (vstupním datům), u něhož známe otisk, rozdílný dokument, jenž by měl stejný otisk. Šance na existenci dvou rozdílných textů se stejným otiskem proto musí být takřka nulová. U hashovacích algoritmů (funkcí) platí, že byť jen nepatrná změna ve vstupních datech znamená zcela odlišný výstup, resp. otisk dat.

Mezi nejznámější hashovací algoritmy patří SHA-1 (Secure Hash Algorithm) a MD5 (Message Digest, vytvořen v roce 1991). V případě algoritmu SHA-1 je vygenerován výstup o délce 160 bitů (40 znaků), zatímco u funkce MD5 se jedná o výstup délky 128 bitů (32 znaků). V roce 2004 došlo k prolomení algoritmu MD5, což znamená, že byla nalezena kolize dvou různých zpráv vedoucích na stejnou hash (MD5 již tedy není považováno za bezpečné). Rovněž byla v roce 2005 snížena náročnost při hledání kolizí v algoritmu SHA-1 [7, 10, 12].

3.2.4 Vytvoření digitálního podpisu

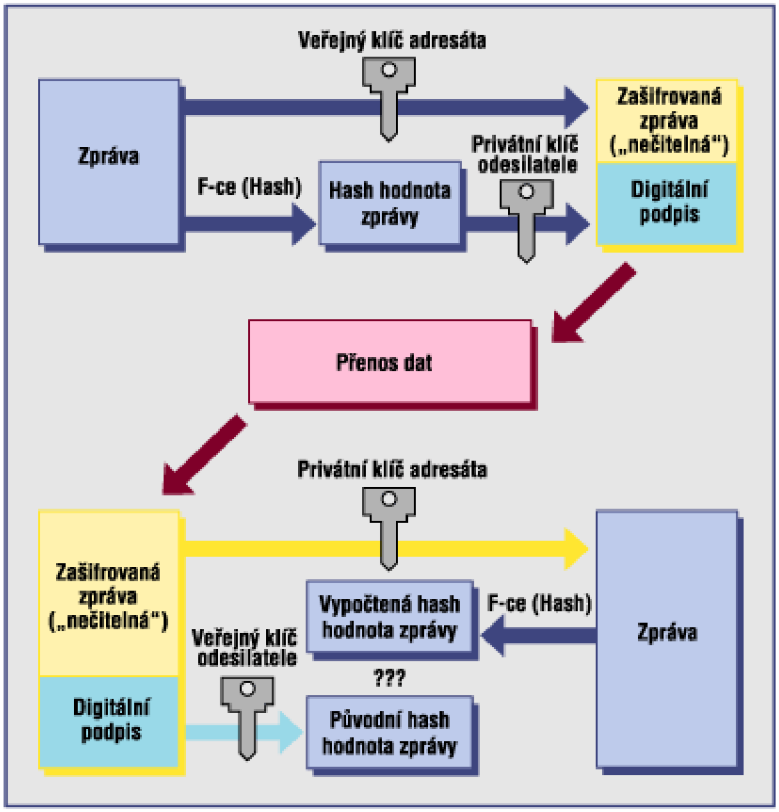
Nyní se podíváme na samotné vytváření digitálního podpisu, kterým se podepisují elektronické dokumenty a datové zprávy obecně. Tvorba digitálního podpisu je postavena na bázi použití metody asymetrického šifrování a hashovací funkce.

Máme-li nějaký soubor (datovou zprávu), kterou chceme digitálně podepsat, musíme nejprve z daného souboru vygenerovat jeho hash. Tento hash zašifrujeme za použití asymetrického algoritmu a svého privátního klíče. Tím vznikne šifrovaný hash daného souboru – digitální podpis. Příjemci pak zasíláme tento šifrovaný hash společně s datovou zprávou a certifikátem [9].

3.2.5 Ověření digitálního podpisu

Kontrolu digitálního podpisu se provádí na straně příjemce. Ten obdrží „balíček“ dat (původní podepisovanou zprávu, digitální podpis, certifikát). Nejprve by měl ověřit platnost certifikátu. Z původní podepisované zprávy musí vypočítat svůj hash (použije stejnou hashovací funkci jakou použil odesílatel). Poté si „přečte“ digitální podpis, tedy odšifruje jej za použití stejného šifrovacího algoritmu a veřejného klíče odesílatele (algoritmus a veřejný klíč zjistí z certifikátu). Příjemce tak získává v dešifrované podobě přijatý hash a ten porovná s hashem, který si sám vypočítal. Pokud oba hashe souhlasí, nebyla původní podepisovaná zpráva od doby podepsání nijak pozměněna a byla podepsána osobou, jíž náleží veřejný klíč. Tím je zkontrolována integrita obsahu [11].

Schéma principu komunikace s využitím digitálního podpisu je zobrazeno na obrázku 2.



Obrázek 2: Bezpečná komunikace s využitím digitálního podpisu

3.3 Využití e-podpisu při komunikaci se státní správou

3.3.1 Zaručený elektronický podpis

Chce-li občan komunikovat s orgány veřejné správy, tedy kupříkladu podávat elektronická podání, musí dokumenty podepisovat tzv. zaručeným elektronickým podpisem.

3.3.1.1 Požadavky na zaručený elektronického podpisu

- Je jednoznačně spojen s podepisující osobou.
- Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
- Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
- Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

3.3.2 Certifikáty a certifikační autority

Abychom mohli používat zaručeného elektronického podpisu, musíme si nechat vystavit tzv. kvalifikovaný certifikát. Jedná se o elektronické potvrzení, které spojuje nějaký subjekt s jeho veřejným klíčem. Aby mohl žadatel získat certifikát, musí si vygenerovat dvojici klíčů (privátní a veřejný) a podat žádost o vydání certifikátu. Tu podepíše vygenerovaným privátním klíčem (tím potvrzuje vlastnictví obou klíčů) a doručí certifikační autoritě. Ta ověří údaje a pošle žadateli certifikát, který může začít používat.

Certifikáty vydávají nezávislé a důvěryhodné organizace, které se nazývají certifikačními autoritami. Ty ověřují totožnost žadatele a na tomto základě mu vydávají certifikát. Aby mohla certifikační autorita vystavovat kvalifikované certifikáty, musí od státu získat akreditaci (splňuje podmínky stanovené zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty). U nás mezi tyto akreditované poskytovatele certifikačních služeb patří například První certifikační autorita a.s., nebo Česká pošta s.p..

Certifikát je v praxi datový soubor, jenž je uložený ve standardním mezinárodně platném formátu. Strukturu certifikátu jednoznačně popisuje norma X.509. Každý certifikát musí obsahovat tyto údaje:

- Sériové číslo (unikátní pro každý certifikát).
- Datum počátku a konce jeho platnosti.
- Identifikační (osobní) údaje subjektu, kterému je certifikát vydáván

- Veřejný klíč (nejčastěji o délce 1024 bitů) a typ algoritmu, který bude pro podepisování používán.
- Identifikační údaje subjektu (certifikační autority), která certifikát vydala a podepsala.

Jelikož je certifikát běžný datový soubor, je potřeba zabránit jeho zfalšování. Proto certifikační autorita podepíše vydávaný certifikát vlastním privátním klíčem a podpis připojí k certifikátu. Pomocí certifikátu veřejné autority (ten by měl být veřejně přístupný na stránkách autority) pak můžeme ověřit platnost podpisu a tím i pravost vydaného certifikátu [13].

4 Návrh ukázkového systému elektronické podatelny

V této kapitole je popsán návrh mnou implementované ukázky systému elektronické podatelny pro obecní úřady, kterou jsem vytvořil v rámci zadání této bakalářské práce.

4.1 Specifikace systému e-podatelny

- Navrhovaný informační systém (elektronická podatelna pro obecní úřady) je určen pro potřeby orgánů veřejné správy, které chtějí tímto způsobem zmodernizovat svou činnost a usnadnit tak práci občanům (fyzickým osobám) při jejich komunikaci s úřadem.

- Informační systém elektronické podatelny zprostředkuje uživateli (podávajícímu) přes webové rozhraní (bez nutnosti osobní přítomnosti na úřadě) elektronickou formou podávat obecnímu úřadu dokumenty v digitální podobě na základě registrace a uložení osobního certifikátu do sytému. Dokumenty v digitální podobě se rozumí soubory s formulářovými vzory, funkčně ekvivalentními s klasickými papírovými předtisky.

- Uživatel bude moci pomocí webového rozhraní informačního systému sledovat stav vyřízení svých již učiněných podání.

- Systém automaticky zkontroluje příchozí podání (korektnost podacích informací, pravost digitálního podpisu, duplikaci podacích čísel) a přijatá podání uloží (eviduje) do interní databáze.

- Informační systém zajistí automatizované generování potvrzovacích zpráv (tzv. doručenek) pro přijatá podání, jejich digitální podepsání a následné poslání formou e-mailové zprávy na odesílatelovu adresu e-mailové schránky.

- Pracovník úřadu (dále jen úředník) umožní tento informační systém přijatá podání zpracovávat (kontrolovat správnost samotného obsahu podávaných elektronických formulářů a přeposílat je k finálnímu vyřízení konkrétnímu odboru). Úředník má možnost o nesrovnalostech v obsahu podání informovat odesílatele formou informační e-mailové zprávy a pozastavit tím vyřizování daného podání.

- Pracovníci jednotlivých odborů si budou moci přes informační systém stáhnout jim určené (úředníkem ověřené) podání k vyřízení.

- Informační systém poskytne automatické provádění evidence (uložení do databáze) všech došlých podání, odeslaných potvrzovacích zpráv a úředníkem poslaných informačních zpráv.

- Systém bude obsahovat rozhraní pro správce, umožňující nahlédnout do interní databáze a vkládat, či odstraňovat některé z údajů.

4.2 Příjem podání elektronickou poštou

Součástí informačního systému elektronické podatelny má být možnost přijetí podání přes elektronickou poštu. Tato schopnost však není v ukázkové elektronické podatelně implementována. Příjem elektronickou poštou proto nechávám pouze v rovině návrhu.

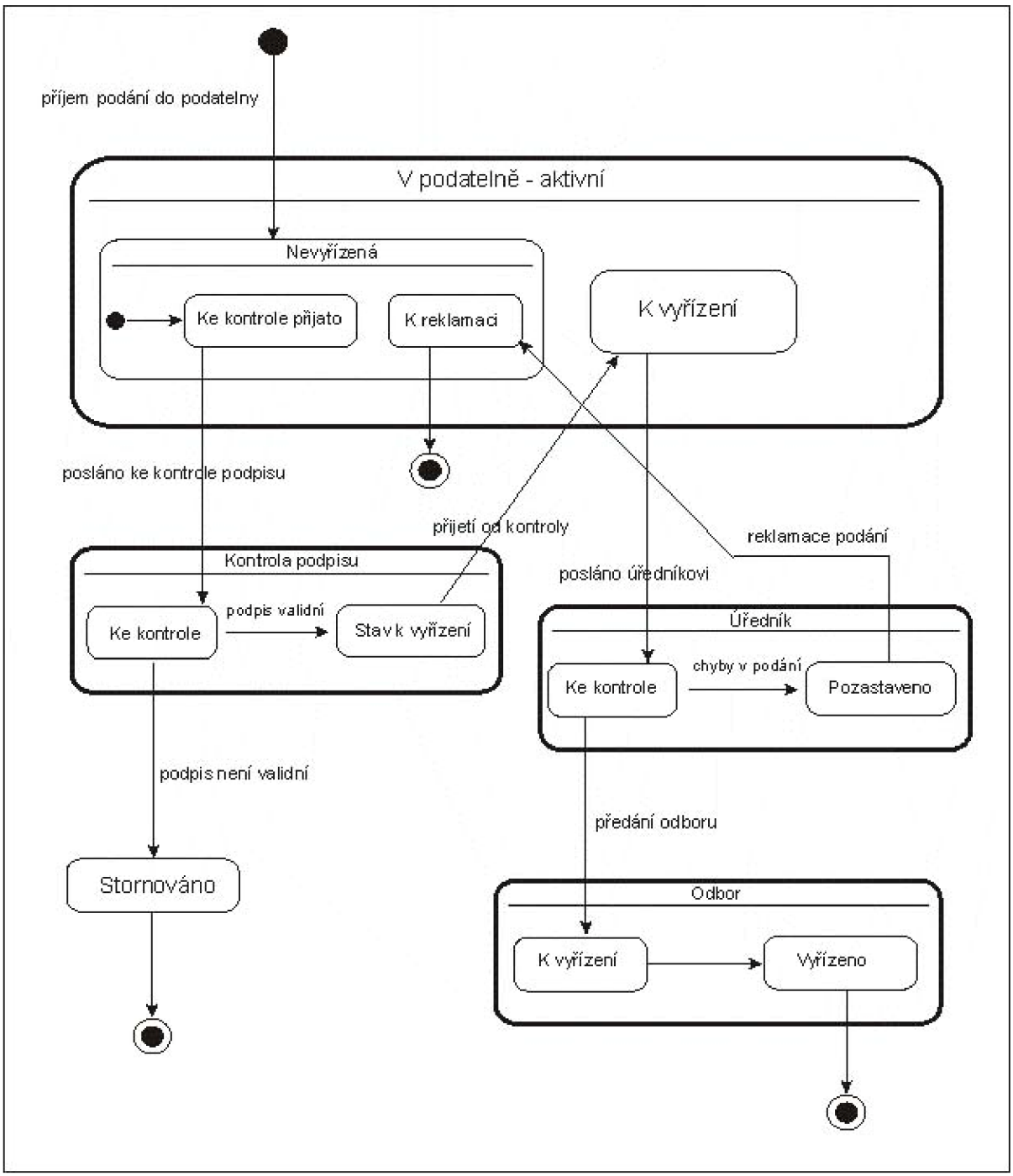
Jednou z možností, jak do systému zakomponovat příjem e-mailem, je vytvoření emailové schránky úřadu (mailbox), která bude sloužit pouze pro příjem zpráv (podání). Každý uživatel, který chce odeslat e-mail s podáním, musí splnit všechny náležitosti, které jsou požadovány při odesílání přes webové rozhraní. Každá příchozí zpráva musí obsahovat dvě přílohy. Jedna příloha je archiv ve formátu `zip` se soubory s podacími formuláři a podacím lístkem a druhá představuje textový soubor s digitálním podpisem archivu. Mailbox úřadu se automaticky za určitý časový úsek (např. každou hodinu) prověřuje a v případě, že obsahuje nově příchozí zprávy, začíná se s jejich postupným zpracováním. Každá nová zpráva je stažena do systému a následně dochází k její kontrole. Kontrola je obdobná jako při posílání přes webový formulář. Analyzuje se soubor s podacím lístkem a na základě údajů v něm obsažených se s podáním dále nakládá. V případě, že je vše v pořádku, uloží se podání do databáze (pokud jsou nějaké nesrovnalosti, je odesílatel informován e-mailem a podání se systémem dále nezpracovává). Následná kontrola digitálního podpisu už funguje zcela stejně, jako kdyby bylo podání učiněno přes webové stránky podatelny.

Jelikož součástí každého podání v implementované ukázce systému elektronické podatelny musí být soubor s podacím lístkem, bylo by i při posílání přes elektronickou poštu nutné jej vygenerovat přes webové rozhraní na stránkách podatelny. Podací lístek totiž obsahuje, kromě jiného, důležité údaje o identifikačním čísle uživatele, čísle podání a datumu podání (jistá neoficiální forma časového razítka, protože pod toto datum se odesílatel podepisuje). Funkce generování podacího lístku je dostupná výhradně přihlášeným uživatelům, takže i pro odesílání přes e-mail je nutná registrace a přihlášení se do systému.

Díky těmto skutečnostem nespatřuji v mnou implementované elektronické podatelně žádné výhody a přílišné uplatnění této formy odesílání podání.

4.3 Životní cyklus podání

Životní cyklus podání je znázorněn stavovým diagramem na obrázku 3. Prezentuje, kterými stavy podání po přijetí do systému elektronické podatelny prochází.



Obrázek 3: Stavový diagram podání

4.4 Role účastníků v systému

V této kapitole je prezentována role jednotlivých účastníků, kteří do systému elektronické podatelny přistupují.

4.4.1 Uživatel

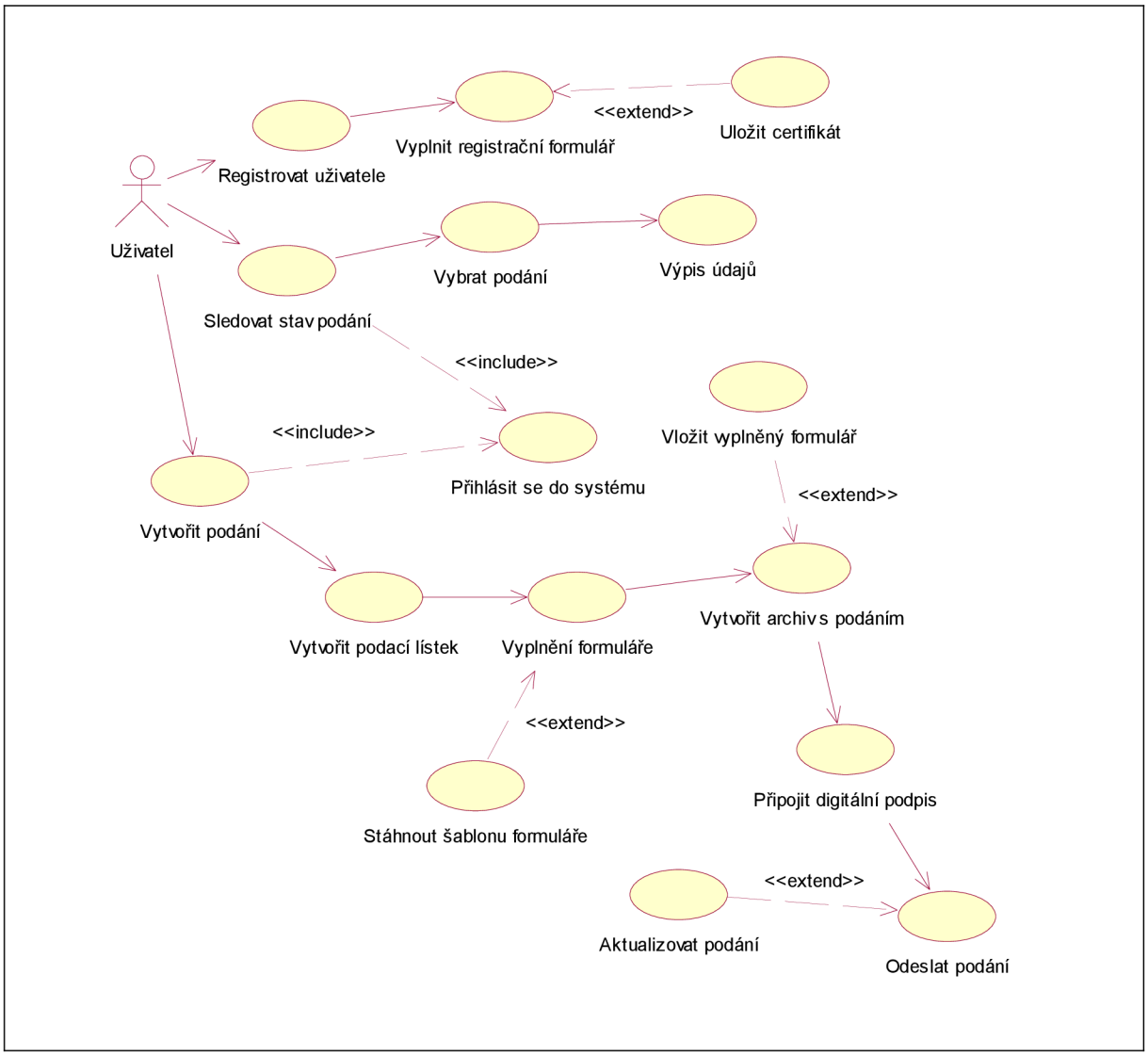
Uživatel (občan) přistupuje k systému přes uživatelské webové rozhraní přístupné na síti (internetu). Schématicky je jeho role zobrazena v diagramu případů použití na obrázku 4. Možnosti práce uživatele jsou v zásadě rozděleny do tří hlavních kategorií:

- **Registrace**. Při prvním přístupu do systému (resp. před prvním odesláním podání) musí uživatel provést zaregistrování a vytvořit si tak svůj uživatelský účet. Registrace spočívá ve vyplnění požadovaných údajů do připraveného registračního formuláře. V rámci tohoto úkonu si zvolí svůj uživatelský login a přístupové heslo. Důležitou položkou formuláře je vložení platného (z hlediska datumu platnosti) osobního certifikátu (bez něj nelze úspěšně zpracovat elektronické podání). Uživateli je systémem přiděleno identifikační číslo. Osobní údaje lze podle potřeby kdykoliv změnit (vyjma loginu).

- **Vytvoření podání**. Chce-li uživatel vytvořit a odeslat nové podání, je nutné se nejprve přihlásit do systému (přes logovací formulář na stránkách e-podatelny). Tím se dostává do své osobní sekce. Tvorba nového podání je tvořena několika dílčími úkony. Tím prvním je vytvoření podacího lístku. Uživatel vyplní potřebné údaje náležící do podacího lístku (formou vyplnění formulářových políček na webu) a nechá si podací lístek systémem vygenerovat (stáhne si nabízený textový soubor). Další krok spočívá ve vytvoření archivu ve formátu `zip`, například pomocí programu `Zip`. Do něj uloží veškeré soubory potřebné pro konkrétní podání (např. vyplněné formuláře v digitální podobě, jejichž šablony jsou přístupné na webových stránkách podatelny), včetně vytvořeného souboru s podacím lístkem. Celý archiv digitálně podepíše. Do webového formuláře pro odesílání podání poté vloží soubor s archivem a soubor s digitálním podpisem archivu. Posledním krokem je již pouze odeslání souborů s archivem a s digitálním podpisem (pomocí příslušné volby). Při aktualizaci dřívějšího odeslaného podání novým podáním se postupuje stejně, pouze se do odesílacího formuláře uvede informace o identifikačním čísle podání, jehož se aktualizace týká a pro samotné odeslání se zvolí volba pro aktualizaci podání.

- **Sledování stavu podání**. Pokud chce uživatel sledovat stav svých podání, musí být opět přihlášen. V příslušné sekci na stránkách podatelny vloží identifikační číslo sledovaného

podání (číslo buď napíše, nebo jej vybere z nabízeného seznamu) a odešle požadavek. Výstupem je vypsání informací vyžádaného podání.



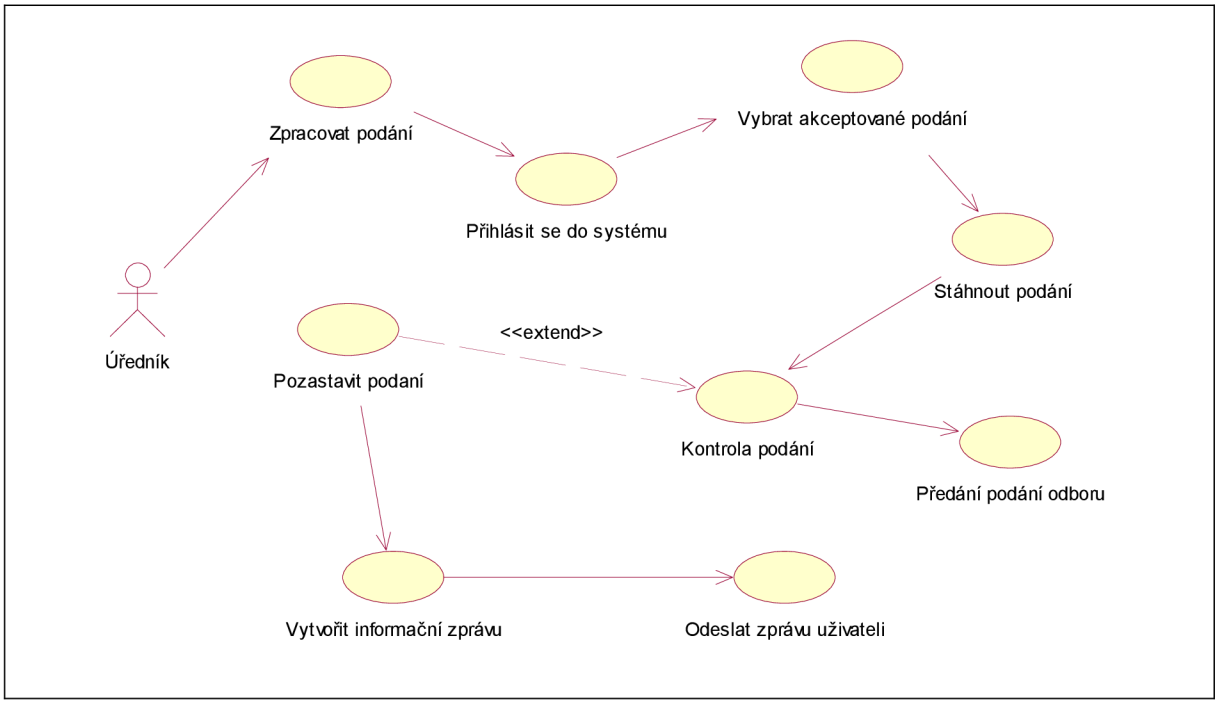
Obrázek 4: Diagram případů použití (uživatel)

4.4.2 Úředník

Úředník (pověřený pracovník úřadu) plní kontrolní funkci a přistupuje do systému přes webové rozhraní určené pro úředníky. Schématicky je role úředníka zobrazena v diagramu případů použití na obrázku 5. Jeho úkolem je zpracovávat a kontrolovat systémem akceptovaná podání.

Aby se úředník mohl dostat do své sekce, ze které je možné přistupovat k podáním a zpracovávat je, musí se přihlásit do systému (pomocí svého loginu a hesla). Úředník si vybere podání (resp. systém mu nabídne volné podání, na němž momentálně nepracuje jiný úředník) a zvolí možnost stažení archivu s podáním. Archiv se zkopíruje na disk do úředníkovy složky a zde si jej úředník rozbalí patřičným, běžně dostupným softwarem.

Kontrola podání spočívá v ověřování údajů zapsaných v přiložených formulářích (obecně v dodaných souborech). Pokud jsou všechny požadavky na správnost vyplněných údajů ve formulářích v pořádku, předává podání ke konečnému vyřízení tomu odboru, jemuž podání náleží (do databáze je k danému podání uložena informace o tom, že podání je zkontrolováno). V případě, že úředník zjistí v podání nesrovnalosti, vytvoří obsah informační zprávy (s popisem všech náležitostí, které je potřeba aktualizovat a uvést tak do korektní podoby) a zvolí její odeslání na e-mailovou schránku odesílatele podání. Tímto podání automaticky pozastaví a může začít zpracovávat další dostupné podání.



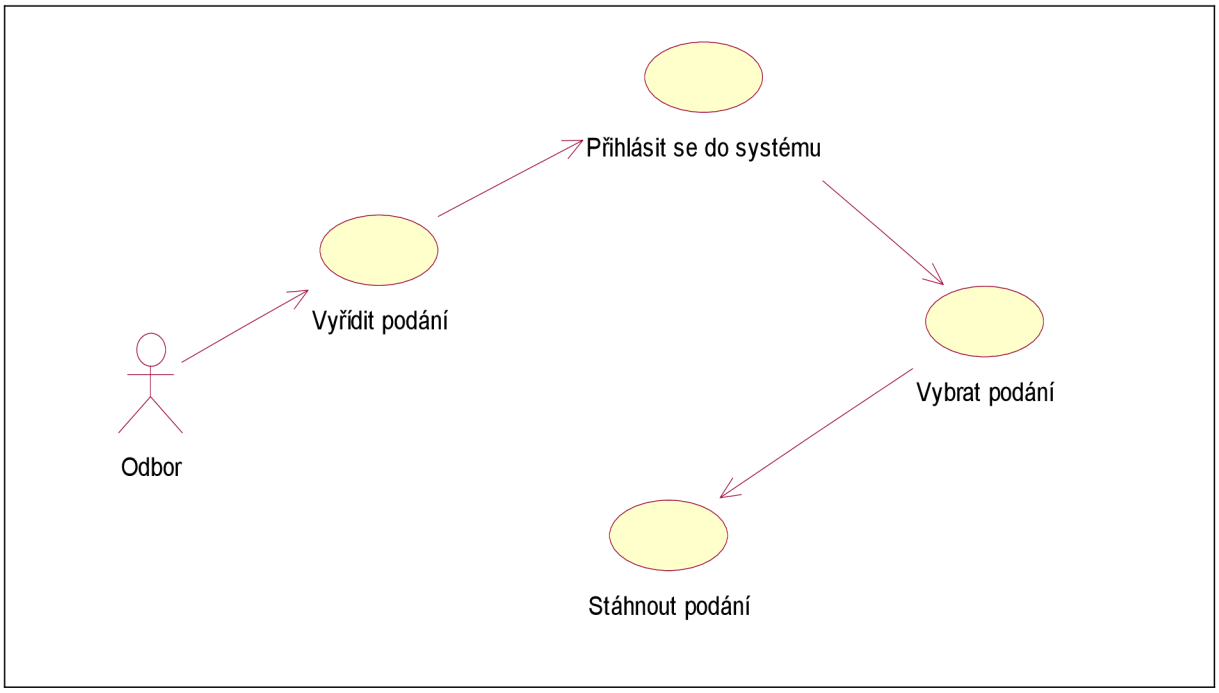
Obrázek 5: Diagram případů použití (úředník)

4.4.3 Odbor

Odbor je v implementovaném systému elektronické podatelny jakýmsi konečným elementem procesu zpracovávání podání (schématicky je úloha odborů znázorněna v diagramu případů použití na obrázku 6). Jeho úkolem je „fyzicky“ vyřídit konkrétní podání (tzn. provést činnost, kterou uživatel učiněním elektronického podání inicializoval). Odbor tak v podstatě nevyřizuje pouze elektronická podání, ale i běžná papírová podání.

Odborů je několik druhů, dle svého zaměření (sociální, pozemkový, apod.) a v rámci zjednodušení každý odbor do systému vstupuje jako jeden celek. To v praxi znamená, že systém nerozlišuje jednotlivé pracovníky v daném odboru. Každý odbor tak vlastní svůj jeden účet a kdokoli kompetentní (zná login a heslo) z daného odboru se může přes jim určené webové rozhraní přihlásit.

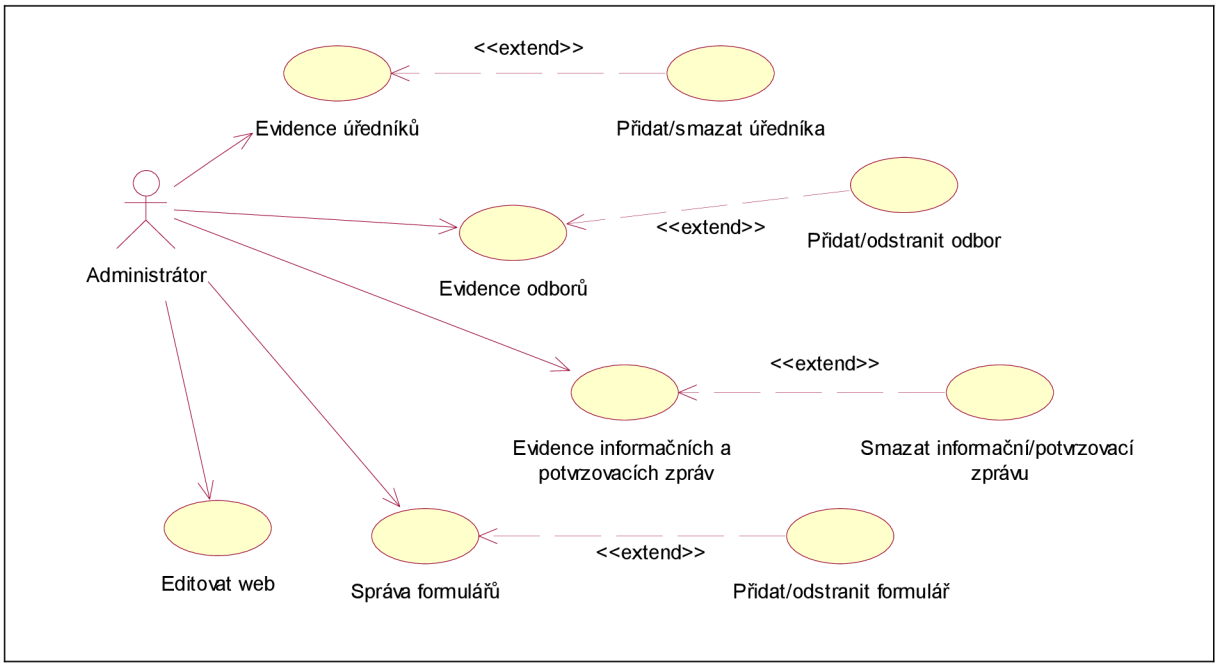
Samotnému vyřízení předchází zkopírování archivu s podáním do složky odboru (podobně jako u úředníka). Na disku se opět k tomu určeným softwarem archiv rozbalí, formuláře (resp. všechny obsažené soubory) například vytisknou a dále zpracovávají stejným způsobem, jako by bylo podání učiněno klasickým způsobem na úřadě.



Obrázek 6: Diagram případů použití (odbor)

4.4.4 Administrátor

Administrátor (správce systému) má na starosti chod celého informačního systému. Stará se o internetové stránky podatelny, o aktualizaci dat, formulářových šablon a běžných věcí související s provozem. Zároveň má přístup do celé databáze. Může přidávat či mazat ze systému pracovníky úřadu, jednotlivé odbory, nebo odstraňovat podání a informační či potvrzovací zprávy. Úlohy administrátora schématicky popisuje diagram případů použití na obrázku 7.



Obrázek 7: Diagram případů použití (administrátor)

5 Implementace ukázkového systému elektronické podatelny

Tato kapitola zahrnuje popis konkrétních stěžejních záležitostí, které bylo nutné při samotné implementaci vyřešit, včetně popisu schématu relační databáze.

5.1 Použité technologie

Informační systém elektronické podatelny je implementován pomocí skriptovacího jazyka PHP (verze 5), databázového systému MySQL (verze 5), hypertextovým značkovacím jazykem HTML (verze 4.01) a kaskádovými styly CSS.

Značkovací jazyk HTML a kaskádové styly jsou použity pro vzhled webového rozhraní, databázový systém MySQL pro vytvoření relační databáze a jazyk PHP pro naprogramování a vykonávání operací v informačním systému.

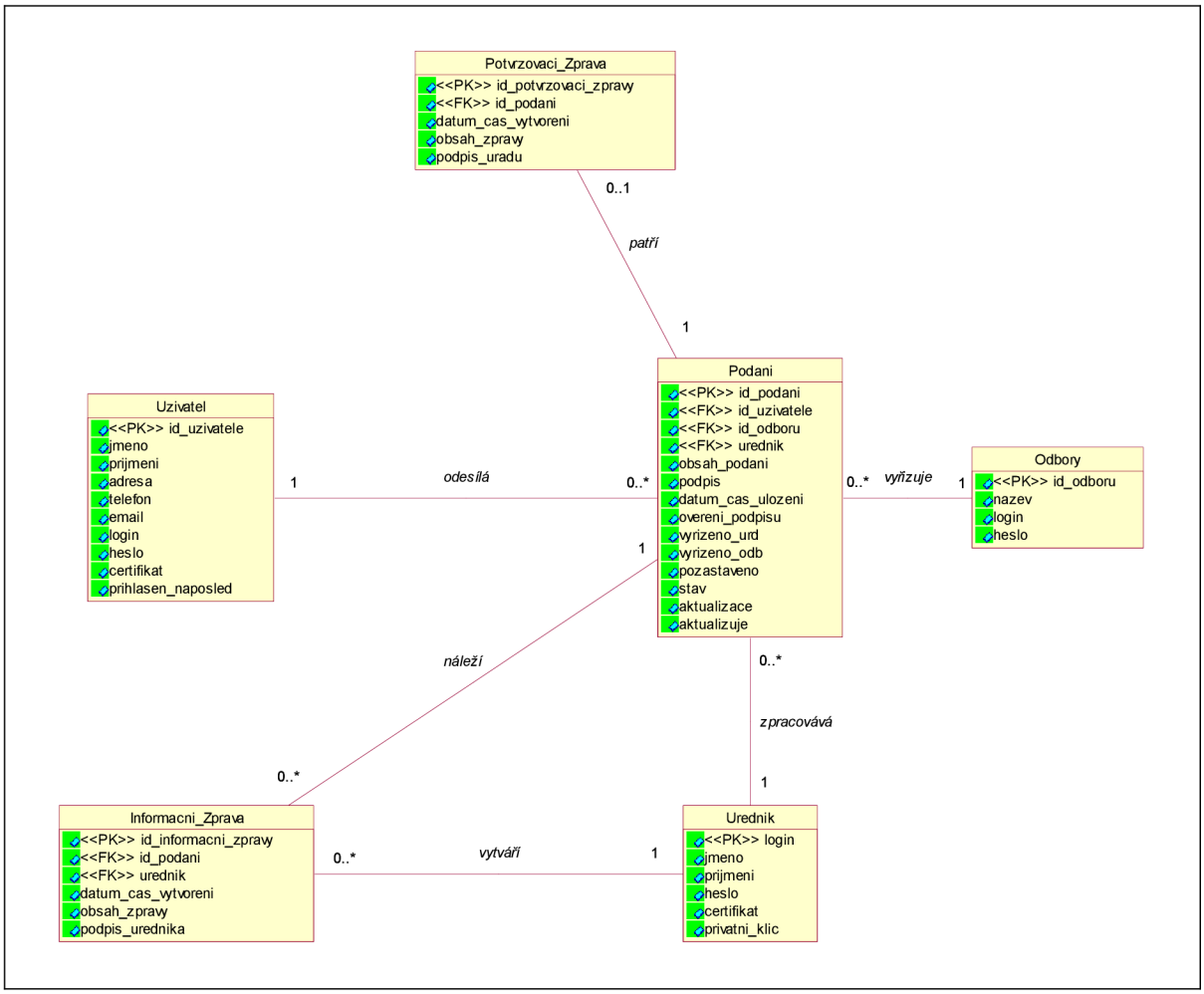
5.2 Databázové schéma

Relační databáze implementovaní v systému elektronické podatelny se skládá z několika entit. Realizace databáze v systému je znázorněna ER diagramem na obrázku 8.

5.2.1 Entity databáze

5.2.1.1 Uživatel

`Uzivatel` je entitou, která v databázi vystupuje jako odesílatel podání. Mezi jeho atributy patří identifikační číslo `id_uzivatele`, které slouží jako jednoznačná identifikace v rámci informačního systému elektronické podatelny. Toto číslo je uživateli automaticky přiděleno při úspěšném zaregistrování. K dalším atributům patří různé osobní údaje (např. jméno, příjmení, emailová adresa), přihlašovací jméno a heslo (`login` a `heslo`) a rovněž informaci o cestě k souboru s jeho osobním certifikátem (atribut `certifikat`), který je uživatel povinen v rámci registračního procesu vložit (uložit) do systému. Atribut `prihlasen_naposled` obsahuje časový údaj o posledním přihlášení uživatele do systému.



Obrázek 8: ER diagram databáze e-podatelny

5.2.1.2 Úředník

Entita `Urednik` představuje pověřeného pracovníka úřadu, který má na starosti kontrolu přijatých podání (ve smyslu prověřování údajů samotného obsahu podání). Zpracovává tak v podstatě entitu podání. Pracovník úřadu je v systému jednoznačně identifikován atributem `login`, který zároveň s heslem (atribut `heslo`) slouží jako jeho přihlašovací údaj. Stejně jako uživatel, obsahuje entita `Urednik` atributy udávající jméno a příjmení pracovníka (`jmeno` a `prijmeni`) a taktéž cestu k souborům s osobním certifikátem (`certifikat`) a privátním šifrovacím klíčem (`privatni_klic`). Jednotlivé pracovníky úřadu přidává a odstraňuje ze systému administrátor.

5.2.1.3 Odbory

`Odbory` jsou entitou, která v systému reprezentuje jednotlivá oddělení úřadu (odbory), které finálně vyřizují jednotlivá jim určená příchozí a úředníkem prověřená podání. Atribut `id_odboru` je číselná identifikace jednotlivých odborů. Každý z odborů do systému přistupuje pod svým přihlašovacím

jménem a heslem (atributy `login` a `heslo`). Poslední zbývající atribut `nazev` obsahuje údaj o názvu daného oddělení. Jednotlivé odbory jsou do databáze vkládány (popřípadě odstraňovány) administrátorem.

5.2.1.4 Podání

Entita `Podani` představuje v systému jednotlivá příchozí podání. Každé podání má své jedinečné identifikační číslo, představované atributem `id_podani`. Zároveň nese údaje o uživateli, který podání odeslal (`id_uzivatele`), o loginu úředníka, který obsah podání kontroloval (`urednik`) a o odboru, kterému je podání k vyřízení určeno (`id_odboru`). Atribut `obsah_podani` obsahuje cestu k souboru (archivu) s podáním, stejně tak `podpis` v sobě nese údaj o cestě k souboru s digitálním podpisem podání. Dalšími atributy jsou `datum_cas_ulozeni` (datum a čas přijetí podání), a `overeni_podpisu` (určuje, zda-li kontrola digitálního podpisu byla validní).

Atribut `vyrizeno_urd` stanovuje, jestli bylo podání zkontrolováno úředníkem. To stejné platí o `vyrizeno_odb`, s tím rozdílem, že atribut se vztahuje k informaci o vyřízení daným odborem. Dále entita obsahuje údaj o aktuálním stavu podání (`stav`) a atribut `pozastaveno` určující, jestli je podání zastaveno (v případě nalezení chyb úředníkem) a čeká na aktualizaci. Poslední dva atributy jsou `aktualizace` (obsahuje číslo nového podání, které toto podání aktualizuje, resp. nahrazuje) a `aktualizuje` (číslo předchozího podání, kterým je toto podání aktualizací).

5.2.1.5 Potvrzovací zpráva

Entita `Potvrzovaci_zprava` znázorňuje odeslanou potvrzovací zprávu (tzv. doručenku), jenž je při každém přijetí podání do systému automaticky generována a poslána odesílateli. Obsahuje identifikační číslo (`id_potvrzovaci_zpravy`) a číslo podání, ke kterému tato zpráva patří (`id_podani`). Atribut `datum_cas_vytvoreni` je údaj o čase vytvoření potvrzovací zprávy, `obsah_zpravy` je cesta k textovému souboru s obsahem potvrzovací zprávy a `podpis_uradu` značí cestu k souboru s digitálním podpisem potvrzovací zprávy.

5.2.1.6 Informační zpráva

Entita `Informacni_zprava` je obdobou potvrzovací zprávy s tím rozdílem, že informační zprávu odesílá úředník v případě, že nalezne nedostatky v podání a informuje tak odesílatele o náležitostech, které je potřeba pozměnit. Každá informační zpráva má své identifikační číslo (`id_informacni_zpravy`), číslo podání ke kterému se vztahuje (`id_podani`) a údaj o úředníkovi, který zprávu vytvořil a odeslal (`urednik`). Atributy `datum_cas_vytvoreni`, `obsah_zpravy` a `podpis_urednika` jsou obdobné jako u potvrzovací zprávy, tedy čas

vytvoření zprávy, cesta k textovému souboru s obsahem informační zprávy a cesta k souboru s podpisem této zprávy.

5.3 Nástin řešení problémů

5.3.1 Podací lístek

Podací lístek je nezbytnou součástí každého učiněného podání. Jedná se o systémem vygenerovaný textový soubor, který musí být přiložen do `zip` archivu s podáním. Je nutné, aby byl přiložený soubor s podacím lístkem pojmenován tak, jak byl vygenerován (tedy `podaci_listek.txt`). Tento soubor si přihlášený uživatel generuje na stránkách podatelny, v sekci pro odesílání podání, kde si jej rovněž může stáhnout do svého počítače. Důležitým údajem, který podací lístek obsahuje, je číslo podání. Toto číslo je systémem automaticky generováno. Aby bylo číslo jedinečné, je poslední číslice vložena ze souboru `citac_podani.txt`, který je uložen na disku podatelny. Po každém vytvořeném souboru s podacím lístkem je číslo čítače inkrementováno.

Může se stát, že odesílatel podání nabídnuté (vygenerované) podací číslo v souboru `podaci_listek.txt` přepíše na jiné a poté podání pod tímto číslem odešle. Proto když se vytváří číslo podání, prochází systém databázovou tabulku s příchozími podáními a kontroluje, zda-li neexistuje číslo podání, které je shodné s právě vytvářeným číslem. V případě že je shoda nalezena, vytvoří se číslo nové, které znova prochází ověřením. Další údaje v podacím lístku jsou jméno a příjmení odesílatele, jeho identifikační číslo a datum vygenerování lístku (tento údaj je chápán jako datum vyplnění lístku). Navíc má uživatel možnost zapsat do podacího lístku doplňující informace pro úřad (formou poznámek).

5.3.2 Kontrola příchozího podání

Každé podání se skládá ze dvou částí. První je archiv se soubory s podacími formuláři (včetně podacího lístku) a druhá část je textový soubor s digitálním podpisem archivu. Obě části si vytváří uživatel mimo systém podatelny svými prostředky, vyjma tvorby podacího lístku.

První kontrola uživatelem odeslaného podání spočívá v ověření přítomnosti obou částí (archiv s podáním + soubor s podpisem). Pokud jsou odeslány obě části, uloží se podání do dočasného souboru a následuje kontrola velikosti archivu (podání je omezeno svou maximální velikostí, v případě této implementované podatelny se jedná o 4MB). Dalším krokem je rozbalení archivu s podáním do dočasného adresáře. Rozbalení probíhá externím programem `Unzip` (je proto nutná jeho instalace, pokud není na provozované sestavě přítomen). Pokud se rozbalení nezdaří, je automaticky formát archivu označen za nesprávný. V rozbaleném archivu se analyzuje soubor s podacím lístkem `podaci_listek.txt` (pokud není nalezen, je formát podání neplatný).

V podacím lístku se ověřuje podací číslo. Pokud již existuje v databázi podání se stejným číslem, podání není akceptováno. Dále se prověřuje datum, které musí být platné s aktuálnímu kalendářním měsíci a rokem. Nesmí se jednat o datum v budoucnosti a nemůže být údaj o měsíci starší než současným měsíc. Současně s tím nelze mít uvedené datum v podacím lístku, které je v rozporu s platností uživatelova osobního certifikátu. Pokud jsou všechny podmínky splněny, je podání přijato a uloženo na disk podatelny pod názvem svého podacího čísla spolu s podpisem (podání se ukládají do adresáře `prichozi_podani` a podadresáře udávající den uložení).

5.3.3 Ověření digitálního podpisu

Poté co je podání uloženo, přichází fáze ověření digitálního podpisu. Získá se cesta k souboru s podáním, podpisem a uživatelově certifikátu a vše se předá funkci pro ověření podpisu. Funkce z certifikátu zjistí potřebná data (použitý hash algoritmus, veřejný klíč), vytvoří ze souboru s archivem svůj hash a volá další funkci, která dokáže rozšifrovat digitální podpis a získat tak původní hash. Této funkci se předává nově vytvořený hash a veřejný klíč. Funkce vrací úspěšnost porovnání obou hashů.

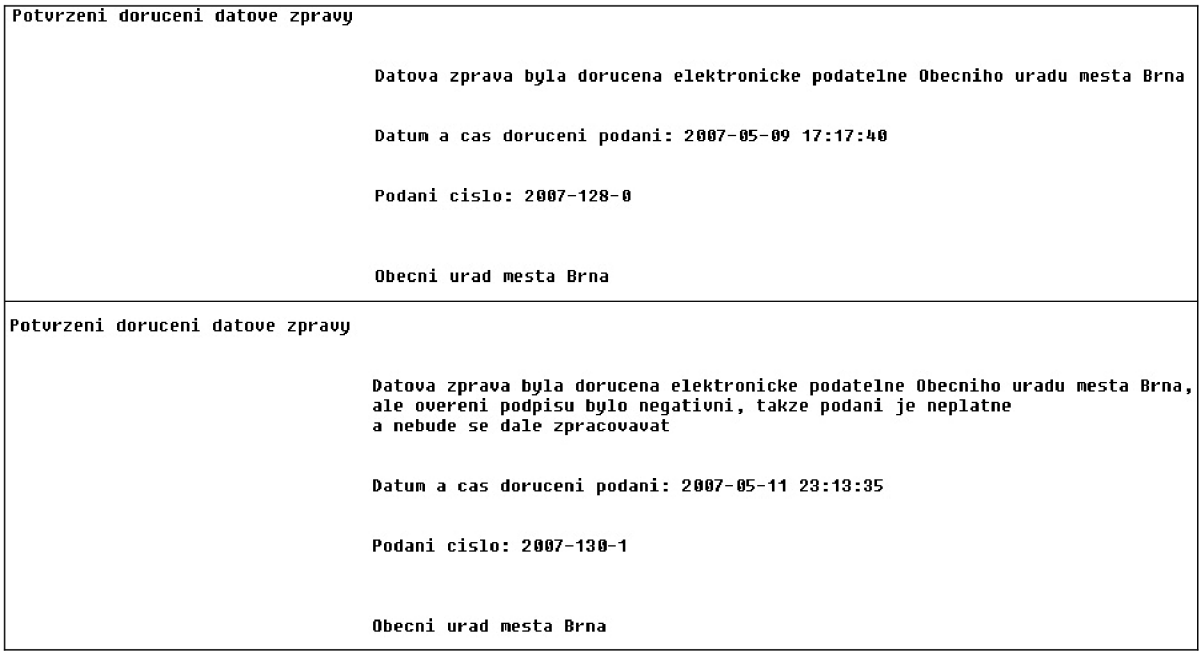
Po provedené kontrole podpisu se provede uložení záznamu o podání do databáze. Pokud je podpis validní, je do tabulky k podání uložena informace o platnosti podpisu. Tím je řečeno, že podání se bude dále zpracovávat.

5.3.4 Odesílání potvrzovací zprávy

V případě přijetí podání a jeho uložení podání do databáze, se odesílateli odesílá potvrzovací zpráva. Vytvoří se textový soubor s obsahem potvrzovací zprávy (potvrzovací zprávy jsou dvojího druhu) a ten se digitálně podepíše (vznikne soubor s podpisem zprávy). Ukázka obou druhů potvrzovacích zpráv (pro úspěšnou i neúspěšnou kontrolu podpisu) je zobrazena na obrázku 9.

Oba tyto soubory se archivují a informace o potvrzovací zprávě se uloží do databáze (potvrzovací zprávy se fyzicky ukládají na disk do adresáře `potvrzovaci_zpravy`). Posléze se volá funkce pro odeslání e-mailové zprávy, která obsahuje text potvrzovací zprávy a dvě přílohy (textový soubor s obsahem potvrzovací zprávy a soubor s digitálním podpisem souboru s obsahem).

Každá potvrzovací zpráva je jednoznačně identifikována svým číslem, jehož generování probíhá stejným principem jako tvorba číslo podání. Jako čítač je v tomto případě použit soubor `citac_pz.txt`. Pokud je odstraněno podání, kterému potvrzovací zpráva náleží, je tato zpráva smazána.



Obrázek 9: Ukázka potvrzovacích zpráv

5.3.5 Zpracování podání úředníkem

Každý úředník kontroluje podání přes své webové rozhraní. Před jednotlivým zpracováním si úředník přes webové rozhraní načte nezpracované podání z databáze. Každé podání v sobě nese informaci o tom, který úředník jej kontroluje (popřípadě zkontroloval). Na počátku (při uložení do databáze) je tento údaj vždy implicitní (hodnota `xurednik00`), což značí, že podání je volně dostupné ke zpracování.

Poté co je úředníkem podání načteno, je tento údaj změněn na hodnotu loginu vyřizujícího úředníka. Úředník si stáhne (opět přes webové rozhraní) obsah podání, čímž si zkopíruje archiv s podáním do své osobní složky (v adresáři `urednici`). Zde si již mimo rozhraní podatelny archiv rozbalí a ručně zkontroluje obsažené informace ve formulářích. Jestliže vše souhlasí, předá toto podání přes webové rozhraní určenému odboru (úředník jej zvolí, vybere jej ze seznamu). Tím se změní údaje o podání v databázi a podání se stane přístupným pro určený odbor.

5.3.6 Odesílání informační zprávy

Informační zprávu odesílá úředník na základě zjištěných nesrovnalostí při jeho zpracovávání podání. Odesílání informační zprávy funguje na stejném principu, jako odesílání potvrzovací zprávy. Obsah zprávy, určení příjemce a odeslání má na starosti úředník. Vše se děje přes jeho webové rozhraní. Pokud úředník odešle informační zprávu, vytvoří se soubor s obsahem zprávy a soubor s úředníkovým podpisem této zprávy.

Tvorba podpisu se děje automaticky (načte se úředníkův certifikát i jeho privátní klíč a vytvoří se soubor s podpisem) bez úředníkova zásahu. V případě že je odeslána zpráva, ukládá se do databáze

informace o pozastavení podání a vyřizování podání je pozastaveno (a očekává se jeho aktualizace). Současně je informační zpráva odeslána příjemci (v příloze je zaslán soubor s obsahem zprávy a soubor s podpisem této zprávy).

Také informační zpráva se archivuje v databázi pod svým identifikačním číslem (číslo se opět vytváří za pomocí čítače z externího souboru, stejně jako číslo podání a číslo potvrzovací zprávy). Jako čítač je využit soubor `citac_iz.txt`. Informační zprávy jsou fyzicky uloženy v adresáři `informacni_zpravy`. Informační zpráva je z disku i databáze automaticky odstraněna, pokud je smazáno podání, ke kterému se zpráva váže.

5.3.7 Aktualizace podání

Aktualizace podání je implementována následujícím způsobem. Aby šlo podání aktualizovat, musí být podání pozastaveno. Odesílatel při aktualizaci postupuje stejně jako při odesílání nového podání, pouze před samotným odesláním napíše do patřičné kolonky číslo podání, jenž chce aktualizovat, a namísto odeslání zvolí možnost aktualizovat.

Podání prochází stejným ověřovacím procesem. Pokud je takové podání akceptováno a uloženo do databáze, je k údajům o podání zapsáno číslo podání, které toto podání aktualizuje (nahrazuje). Stejně tak je do podání, jenž je aktualizováno, uloženo číslo o jeho „následovníku“ (tedy číslo tohoto nového podání). Aktualizovat podání může pouze uživatel, který to předchozí odeslal (systém tuto skutečnost ověřuje).

5.3.8 Vyřízení podání odborem

Přístup odboru k vyřízení podání je obdobný jako přístup úředníka ke kontrole. Odbor si webové rozhraní nahraje jemu určené podání, to si stáhne do své osobní složky v adresáři `odbory` a může jej začít „fyzicky“ vyřizovat. Po stažení je z hlediska systému podání bráno jako vyřízené.

5.3.9 Sledování stavu podání

Když podání prochází v systému různými stupni zpracování, je k podání do databáze automaticky zapisován údaj o jeho aktuálním stavu. Stav si může uživatel kdykoliv zjistit zadáním patřičného čísla podání na webových stránkách podatelny v jeho osobní sekci.

5.3.10 Implementace odesílání e-mailů

Funkce pro odesílání e-mailů v systému elektronické podatelny využívá hotové knihovny HTML Mime Mail 5 (dostupné na <http://www.phpguru.org/downloads/html.mime.mail/>). Tuto knihovnu používám pro vkládání příloh do e-mailové zprávy a následného odeslání celé zprávy.

5.3.11 Implementace tvorby digitálního podpisu

Funkce v implementovaném systému elektronické podatelny, které vytvářejí a ověřují digitální podpis, využívají již hotové PHP knihovny Crypt_RSA-1.0.0 (dostupné na <http://www.pear.php.net/package/Crypt_RSA/>), která mimo jiné umí šifrovat algoritmem RSA. Využívám ji pro šifrování otisku souboru (tedy vytvoření řetězce představující digitální podpis) a pro dešifrování řetězce s digitálním podpisem (získání otisku souboru). Tato knihovna zároveň umožňuje generování dvojice klíčů (privátní/veřejný).

Avšak během implementace se ukázalo, že knihovna korektně pracuje pouze s klíčí, které sama generuje. Bohužel jsem nedokázal přijít na to, jakým způsobem knihovna klíče vnitřně upravuje (optimalizuje), což znemožňuje použít v mnou vytvořené elektronické podatelně jiné klíče, než ty vytvořené touto knihovnou.

S tímto problémem úzce souvisí práce s certifikáty. Jelikož nelze používat běžné certifikáty (protože ty obsahují veřejný klíč nespolupracující s knihovnou Crypt_RSA), přikládám k systému několik mnou vytvořených testovacích certifikátů. Certifikáty mají formát textového souboru (avšak pro lepší orientaci jsou s příponou `.cer`) a je do nich vložen veřejný klíč (velikost klíče je 1024 bitů) vygenerovaný knihovnou Crypt_RSA. Tyto testovací certifikáty byly vytvořeny z existujícího certifikátu, takže struktura je shodná se skutečnými. V implementovaném systému elektronické podatelny je tak funkce pro získávání dat z certifikátu navržena tak, aby dokázala přečíst data i ze skutečného certifikátu.

6 Zhodnocení a další vývoj

6.1 Naplnění požadavků

Účelem a očekávaným přínosem zřízení elektronické podatelny je komunikace (podávání formulářů k vyřízení) občana s úřadem elektronickou formou, bez jeho osobní přítomnosti v kamenné podatelně.

Implementovaný systém tento způsob komunikace umožňuje. Zároveň do jisté míry ukázkovým způsobem splňuje základní a stěžejní požadavky kladeny na systém elektronických podatelen. Na základě uloženého certifikátu a přihlášení se do systému jednoznačně určuje, kdo podání odeslal, resp. kdo jej podepsal. Systém podle požadavků automaticky odesílá úřadem podepsanou potvrzovací zprávu a zjednodušenou formou splňuje požadavek na veškerou archivaci došlých podání a poslaných potvrzovacích a informačních zpráv.

Jako klad mého řešení považuji nutnost mít ke každému podání podepsaný podací lístek (což je zaručeno podepsáním celého archivu s podáním). Výhodu spatřuji v tom, že v podacím lístku je možné mít řadu podacích informací (jako např. datum), které uživatel svým podpisem stvrzuje. Samozřejmě v systému, který jsem vytvořil je práce s podacím lístkem značně zjednodušená, ale domnívám se, že při vylepšení tohoto systému by se mohlo jednat a cenný zdroj doplňujících a odesílatelem nezpochybnitelných údajů. Stejně tak je podle mého užitečné komprimovat veškerý obsah do jednoho archivu (a ten pak podepsat). Díky tomu se nemusí každý dokument podepisovat zvlášť a s podáním se jednodušeji manipuluje.

6.2 Další vývoj a rozšíření systému

Vzhledem k tomu, že je implementovaný systém pouhou ukázkou, vyhovuje požadavkům na elektronické podatelny pouze částečně. Řada věcí není do řešení zahrnuta a jiné, které tato podatelna obsahuje, by potřebovaly další rozpracování, popřípadě změnu.

Jak již bylo výše zmíněno, znatelným nedostatkem, který by si zasloužil předělání, je nekompatibilita s běžnými certifikáty, přesněji řečeno s privátními a veřejnými klíči. Řešení tohoto problému by spočívalo buď v nalezení způsobu jak upravit použitou knihovnu Crypt_RSA, tak aby uměla pracovat se všemi klíči, nebo nepoužívat tuto knihovnu a vytvořit vlastní funkce pro aplikování šifrovacího algoritmu RSA, popřípadě nalézt jinou vhodnější knihovnu. V praxi by se také měla kontrolovat pravost certifikátu při jeho ukládání, tedy ověření podpisu certifikační autority (to se v implementovaném systému vzhledem k používání testovacích ukázek certifikátů neděje)

Další věcí, kterou by měl systém elektronické podatelny umět a v implementaci chybí, je přijímání podání přes elektronickou poštu. Tento problém je nastíněn v kapitole návrhu, kde je rovněž popsán jeden ze způsobů, jak na stávající implementaci „napojit“ příjem pomocí e-mailu.

Dále by měl systém elektronické podatelny kontrolovat v příchozích podáních přítomnost škodlivého softwaru. V ukázkové implementaci taková kontrola není. Toto se dá do budoucna vyřešit s využitím současných antivirových a antispamových softwarů. Před uložením podání do podatelny by se každý příchozí soubor automaticky nechal zkontrolovat nějakým externím antivirovým programem.

Další rozšíření určitě vyžaduje odesílání e-mailových zpráv, zejména těch potvrzovacích (doručenky). Systém posílá zprávu pouze jednou, v případě že z jakýchkoliv důvodů nelze zprávu doručit, zpráva se k uživateli nedostane. Možným řešením by bylo ověřování, zda-li byla zpráva úspěšně doručena a pokud ne (třeba z důvodu zaplněnosti schránky uživatele), tak se do databázové tabulky s potvrzovacími zprávami zadá informace o nedoručení. Po určité časové době by systém procházel tabulku se zprávami a ty které nebyly doručeny se znovu pokusí doručit (počet opakovaných doručení by mohl být omezen kupříkladu na 5 pokusů).

Jedním z možných rozšíření systému by mohlo také spočívat ve vytvoření služby, která by umožňovala odesílateli nahlédnout do svých učiněných podání. V praxi by to mohlo fungovat jako zpětné poslání archivu s podáním uživateli na základě jeho žádosti.

Významnou oblastí, která není v ukázkovém systému řešena a pro praktický provoz patří k nezbytnostem, je bezpečnost systému ve smyslu zabránění vnějších útoků a zneužití citlivých dat. To znamená, že soubory na disku podatelny by byly uloženy takovým způsobem, který by eliminoval známé možnosti průniku do databáze a systému jako takového.

7 Závěr

Cílem této bakalářské práce bylo nastínit problematiku elektronických podatelen v ČR, navrhnout systém elektronické podatelny pro obecní úřady, který umožní přijímat datové zprávy a nakonec implementovat ukázku takovéhoto systému jako webovou aplikaci.

Práci jsem rozdělil na dvě části. Tu první, teoretickou, jsem pojal jako průvodce současným stavem elektronických podatelen u nás a přidružených oblastí, které s provozováním elektronických podatelen přímo souvisejí. Začal jsem stručným popisem příslušných právních předpisů, jenž stanovují minimální legislativní požadavky pro fungování elektronických podatelen ve státní správě. Poté jsem se zabýval principem fungování podatelen, popsal problematiku datových zpráv pro podatelny a teoreticky rozebral elektronický podpis (principy jeho tvorby a jeho ověřování), elektronickou značku a certifikáty a jejich smysl a použití v komunikaci v rámci e-podatelny.

V druhé, praktické, části jsem se věnoval oblasti popisu týkající se samotné problematiky tvorby ukázkového systému elektronické podatelny. Specifikoval jsem konkrétní požadavky, sestavil návrh systému a popsal řešení některých stěžejních bodů, tak jak jsem je ve vytvořeném systému implementoval. Zároveň jsem se zabýval následným rozšířením a možností budoucího vývoje vytvořeného systému.

Domnívám se, že elektronické podatelny jsou značným přínosem pro současnou společnost. Díky nebývalému rozmachu internetu se jedná o vynikající způsob, jak si může každý občan ušetřit dnes tak ceněný čas při vyřizování věcí na úřadech. Ovšem skutečné naplnění cíle, jenž si zřízení elektronických podatelen klade, vidím až v budoucnu. Je totiž potřeba znatelně zvýšit povědomí široké veřejnosti o možnostech a výhodách nejen při posílání formulářů úřadům, ale o využití elektronického podpisu obecně, protože početná část lidí o této oblasti takřka nic netuší a proto se tyto technologie nesnaží využívat.

Pro mě osobně měla tato práce významný přínos v tom, že jsem měl možnost hlouběji se seznámit se současnými možnostmi elektronické komunikace s úřady, o kterých jsem předtím příliš nevěděl. Stejně tak jsem měl dříve velmi neucelenou představu o fungování elektronických podpisů a certifikátů. Během této bakalářské práce jsem s touto oblastí podrobněji seznámil a podstatně si v této oblasti rozšířil obzory.

Literatura

[1] Nařízení vlády č. 495/2004 Sb. ze dne 25. srpna 2004 o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších přepisů. URL: <http://www.micr.cz/files/1603/Narizeni_vlady_495.pdf>

[2] Vyhláška č. 496/2004 Sb. ze dne 29. července 2004 o elektronických podatelnách. URL: < http://www.micr.cz/files/1705/Vyhlaska_496.pdf>

[3] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb. a zákonem č. 440/2004 Sb. URL: <http://www.micr.cz/files/1540/UZ-227_2000.pdf>

[4] Peterka, J.: Elektronické podatelny. *Veřejná správa online*, ročník II, č.5, 2001. URL: <http://vsol.obce.cz/clanek.asp?id=2001501>

[5] Plhoň, P.: Legislativa a řešení elektronických podatelen. [online], rev. 17.března 2006, [cit. 2007-05-11]. URL: <http://connect.zive.cz/?q=node/226>

[6] Urbánková, K.: E-podatelna, elektronický podpis a jejich využití v digitálních knihovnách. [bakalářská práce]. Masarykova univerzita v Brně, Fakulta filozofická, 2006.

[7] Štěpánek, L.: Elektronický podpis ve státní správě. [bakalářská práce]. Masarykova univerzita v Brně, Fakulta informatiky, 2006.

[8] Vrabec, V.: Elektronické časové razítko, doplněk elektronického podpisu. [online], rev. 3.června 2003, [cit. 2007-05-11]. URL: <http://interval.cz/clanky/elektronicke-casove-razitko-doplnek-elektronickeho-podpisu/>

[9] Doležal, D.: Jak funguje digitální podpis. [online], rev. 23.října 2002, [cit. 2007-05-11]. URL: <http://interval.cz/clanky/jak-funguje-digitalni-podpis/>

[10] Rybák, M.: Elektronický podpis v legislativě a v praxi v ČR. [bakalářská práce]. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, 2006.

[11] První certifikační autorita, a.s.: Šifrovací metody. [online], [cit. 2007-05-11]. URL: <http://www.ica.cz/home_cs/?acc=teorie_symetricke_a_asymetricke_kryptografie>

[12] Klíma, V.: Hašovací funkce MD5 a další prolomeny. [online], rev. 25.srpna 2004, [cit. 2007-05-11]. URL:<http://www.root.cz/clanky/hasovaci-funkce-md5-a-dalsi-prolomeny/>

[13] Doležal, D.: Co to je digitální certifikát. [online], rev. 23.ledna 2003, [cit. 2007-05-11]. URL: <http://interval.cz/clanky/co-to-je-digitalni-certifikat/>

Seznam příloh

Příloha 1. Manuál pro zprovoznění e-podatelny.

Příloha 2. CD se zdrojovými texty, ukázkovou aplikací elektronické podatelny a dalšími náležitostmi.

Příloha 1

Manuál pro zprovoznění e-podatelny

Ukázková implementace systému elektronické podatelny se na přiloženém CD nachází ve složce Elektronicka_podatelna. Tuto složku je zapotřebí zkopírovat do adresáře, který je na lokálním provozovaném počítači určen pro spouštění souborů se skripty skriptovacího jazyka PHP. Název a místo tohoto adresáře závisí na konkrétní instalaci PHP a nastavení lokálního serveru (např. Apache). Lokální server je nutné mít pro provozování systému zapnutý, stejně jako databázový systém MySQL.

Vytvoření databáze

Prvním krokem je vytvoření databáze. Databáze se vytvoří vložením následující cesty k souboru, se skriptem pro tvorbu databáze, do webového prohlížeče:

```
http://localhost/Elektronicka_podatelna/vytvoreni_databaze.php
```

Předtím je ovšem nutné podle potřeby změnit v souboru `mysql_konst.php` (cesta k souboru je `Elektronicka_podatelna/include_files/mysql_konst.php`) změnit následující konstanty:

- `define("SERVER", 'localhost')` – server, implicitně `localhost`.
- `define("USER", 'root')` – jméno uživatel pro přístup do MySQL, implicitně `root`.
- `define("PASSWORD", '')` – heslo pro přístup do MySQL, implicitně prázdná hodnota.
- `define("DATABASE_NAME", 'epodatelna')` – název vytvářené databáze, implicitně `epodatelna`.

Odstranění databáze

Databáze se odstraní vložením následující cesty k souboru, se skriptem pro odstranění databáze, do webového prohlížeče:

```
http://localhost/Elektronicka_podatelna/odstraneni_databaze.php
```

Vytvoření tabulek databáze

Tabulky databáze včetně jejich naplnění ukázkovými daty se vytvoří vložením následující cesty k souboru, se skriptem pro vytvoření tabulek, do webového prohlížeče:

```
http://localhost/Elektronicka_podatelna/vytvoreni_tabulek.php
```

Odstranění tabulek databáze

Smazání tabulek z databáze se provede vložením následující cesty k souboru, se skriptem pro odstranění tabulek, do webového prohlížeče:

```
http://localhost/Elektronicka_podatelna/odstraneni_tabulek.php
```

Nastavení odesílacího e-mailu

Aby mohl systém korektně odesílat e-maily, je zapotřebí nastavit e-mailovou adresu, z níž je možné odesílat e-mailové zprávy přes Internet.

V souboru `Elektronicka_podatelna/include_files/email_konst.php` je nutné změnit obsah následující konstanty:

- `define("EMAIL_ODESILATELE", '10762223@karneval.cz')` – implicitně je nastavena jako odesílající adresa `10762223@karneval.cz`

Spuštění systému

Pro snadnou navigaci v celém systému je možné použít rozcestník. Ten spustíte vložením následujícího odkazu do webového prohlížeče:

```
http://localhost/Elektronicka_podatelna/rozcestnik.html
```

Rozcestník je seznam odkazů, díky nimž se můžete dostat na indexovou stránku webového rozhraní pro uživatele, pro úředníky, pro správce systému a pro odbory. Zároveň obsahuje odkazy na skripty pro vytvoření a odstranění databáze a pro vytvoření a odstranění tabulek databáze. Posledním odkaz je odkazem na skript umožňující digitální podepsaní dokumentů a ověřování podpisů.

Podepisování a ověřování dokumentů

Pro podpis podání a ověřování podpisů slouží skript pro digitální podepisování. Spustit ho lze přes rozcestník, nebo zadáním následující cesty do webového prohlížeče:

```
http://localhost/Elektronicka_podatelna/e_podpis.php
```

Při podepsání dokumentu se vždy vytvoří textový soubor `podpis.txt`, který obsahuje digitální podpis daného dokumentu. Cesta k vytvořenému textovému souboru s digitálním podpisem je následující: `Elektronicka_podatelna/podpisy/podpis.txt`

Popis adresářů systému

V kořenovém adresáři `Elektronicka_podatelna` je obsaženo několik podadresářů, které implementovaný systém využívá. Následuje jejich výčet a popis.

- `certifikaty` – Zde jsou uloženy osobní certifikátu registrovaných uživatelů. Každý certifikát je uložen v podadresáři (název podadresáře je odvozen od loginu uživatele).
- `certifikaty_urad` – Zde je uložen certifikát úřadu, jehož pomocí se podepisují potvrzovací zprávy. Současně s ním se zde nachází také textový soubor s privátním klíčem, jenž tvoří dvojici k veřejnému klíči obsaženém v certifikátu.
- `certifikaty_urednici` – Zde jsou v patřičných podadresářích jednotlivých úředníků (podle jejich loginu) uloženy certifikáty úředníků a soubory s privátním klíčem k danému certifikátu.
- `formulare` – Zde jsou uloženy formulářové předtisky a certifikáty úřadu a úředníků pro stažení. Navíc jsou zde i skripty umožňující jejich stažení.
- `informacni_zpravy` – Do této složky se ukládají vytvořené soubory s informačními zprávami a k nim související soubory s podpisy těchto zpráv.
- `odbory` – Toto je osobní složka odborů (každému odboru je při stažení vytvořen vlastní podadresář), do kterých si stahují archivy s podáními.
- `podaci_listky` – Adresář pro dočasné uložení vytvářených souborů s podacími lístky (každému uživateli je během vytváření lístků je automaticky vytvořen jeho vlastní podadresář).
- `potvrzovaci_zpravy` – Složka pro ukládání souborů s potvrzovacími zprávami a k nim příslušných souborů s podpisy.

- `prichozi_podani` – Zde se ukládají příchozí archivy s podáními a k nim patřičné soubory s podpisy. Soubory se ukládají do jednotlivých automaticky vytvářených podadresářů podle data příchodu do podatelny.
- `tmp_podani` – Adresář pro dočasné uložení archivu s podáním během analýzy podacího lístku. V adresáři vznikají automaticky podadresáře pro jednotlivé uživatele.
- `urednici` – V této složce vznikají automaticky osobní adresáře jednotlivých úředníku, které slouží pro stažení archivu s podáním a jejich následnou „ruční“ kontrolu.

Testovací certifikáty

Na přiloženém CD se nachází adresář `Testovaci_certifikaty`, ve kterém je uloženo několik testovacích certifikátů v textovém formátu (pro snadnější rozeznání však mají soubory příponu `.cer`) a k nim příslušné soubory s privátními klíči. Tyto certifikáty je možné použít v systému, protože se jedná o upravené certifikáty v tom smyslu, že obsahují veřejné klíče, se kterými implementovaný systém dokáže komunikovat, resp. jsou akceptovány knihovnou `Crypt_RSA`, která je v systému používaná pro šifrování.

Příklad: Soubor `karel_stransky.cer` je certifikát, soubor `karel_stransky_pk.txt` je příslušný privátní klíč.