VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

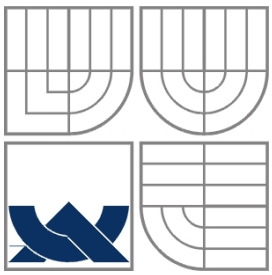
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ELEKTRONICKÁ PODATELNA VUT 2

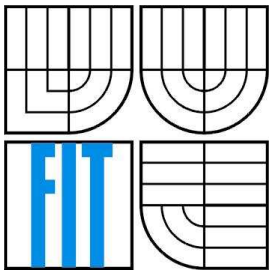
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE MARTIN BERAN
AUTHOR

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 VUT 2

ELECTRONIC MAIL ROOM OF THE BUT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — MARTIN BERAN
AUTHOR

VEDOUCÍ PRÁCE — ING. JAROMÍR MARUŠINEC, PH. D.
SUPERVISOR

BRNO 2007

Zadání diplomové práce/5610/2006/xbemn15

Vysoké učení technické v Brně - Fakulta informačních technologií

Centrum výpočetních a informačních služeb Akademický rok 2006/2007

Zadání diplomové práce

Řešitel: **Beran Martin**

Obor: Výpočetní technika a informatika

Téma: **Elektronická podatelna VUT 2**

Kategorie: Web

Pokyny:

1. Prostudujte problematiku elektronického podepisování emailů a problematiku osobních certifikátu.
2. Prostudujte a porovnejte dostupné komerční elektronické podatelny nabízející služby státním úřadům.
3. Navrhněte elektronickou podatelnu pro VUT. Kromě technické částí se také zaměřte na návrh organizačního zabezpečení na VUT.
4. Realizujte elektronickou podatelnu VUT ve spoluprácí s CVIS jako webovou aplikaci na PortáluVUT.
5. Vytvořte stručnou a názornou uživatelskou příručku pro podávající občany, pro zaměstnance podatelny a pro uživatele na VUT.
6. Zhodnoťte výsledky vaší práce a navrhněte další směr rozvoje podatelny pro potřeby VUT jako součást elektronické spisové služby.

Literatura:

- Literatura Oracle

Při obhajobě semestrální části diplomového projektu je požadováno:

- Splnění prvních 3 úkolu zadání.

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

Technická zpráva diplomové práce musí obsahovat formulací cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problému a specifikaci etap, které byly vyřešeny v rámci ročníkového a semestrálního projektu (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentací a zdrojové texty programu. 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 manipulací.

Vedoucí: **Marušinec Jaromír, Ing., Ph.D.,** CVIS VUT

Datum zadání: 1. listopadu 2006 Datum Datum odevzdání: 22. května 2007

prof. Ing. Tomáš Hruška, CSc.

děkan FIT

LICENČNÍ SMLOUVA

POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami:

1. Pan/paní

Jméno a příjmení: **Martin Beran**
Id studenta: 22646
Bytem: Jungmannova 81, 666 01, Tišnov
Narozen: 24. 8. 1982, Brno
(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“)

Čl. 1
Specifikace školního díla

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

Název VŠKP:	Elektronická podatelna VUT 2
Vedoucí/ školitel VŠKP:	Marušinec Jaromír, Ing., Ph.D.
Ústav:	Centrum výpočetních a informačních služeb VUT
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 pořizovaní 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

Tato práce se věnuje problematice elektronické podatelny pro VUT.
Rozebírá princip fungování elektronické podatelny, elektronického podepisování a porovnává nabídku komerčních podatelen. Věnuje se návrhu a realizaci e-podatelny pro VUT.
Od chvíle, kdy bylo uzákoněno používání e-podatelny na všech úřadech veřejné zprávy, nabízí občanům možnost osvobození od dlouhých front na úřadech a úředníka chrání od stresu, zažívajícího především před uzávěrkami odevzdání řady důležitých dokumentů.
Při komunikaci prostřednictvím elektronické podatelny hraje velkou roli elektronický podpis. Je téměř plnohodnotnou, zákonem uznávanou alternativou k fyzickému podpisu. Pro svoji bezpečnost a funkčnost využívá asymetrických šifer a hashovacích algoritmů. V současnosti se ve většině států, kde je elektronický podpis uzákoněn, využívá podpisu ve spojení se standardem X.509. Formát určený standardem definuje formát certifikátů, organizaci a jednání certifikačních autorit. Certifikační autorita zajišťuje důvěryhodné spojení osoby a veřejného klíče k využití pro elektronický podpis.

Klíčová slova

Elektronická podatelna, elektronický podpis, šifrování, certifikační autorita, certifikát, asymetrická kryptografie, algoritmus RSA, DSA, hashovací funkce, MD5, SHA-1

Abstract

This dissertation thesis attends to problems of electronic registry for VUT.
It deals with the principal of electronic registry functioning, electronic signature and it compares offer of the commercial registries. It goes in for the proposal and implementation of the electronic registry for VUT.
Since the using of the e- registry on all public service Office was legalized the people can avoid long queues and the employees are avoided from the stress before dead lines.
By the communication through the electronic registry is very important the electronical signature. It is almost a full-valued and lawful alternative to the physical signature. For its safety and utility this system employes asymmetric codes and hash algorithm. Presently in many states, where the electronical signature is legalized it is used together with standard X 509 which defines the format of certificates, organization and action of certification authorities. The certification autority ensures safe connection of the person and general key for using of the electronical signature.

Keywords

Electronic registry, electronic signature, cryptography, certification authority, certificate, asymmetric cryptography, algorithm RSA, DSA, hash function, MD5, SHA-1.

Citace

Beran Martin: Elektronická podatelna VUT 2. Brno, 2007, diplomová práce, FIT VUT v Brně.

Elektronická podatelna VUT 2

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením Ing. Jaromíra Marušince, Ph. D.
Další informace mi poskytli Ing. Marek Strakoš, Ing. Michal Jurosz a Edmund Kmeť.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Martin Beran
22.5. 2007

Poděkování

Děkuji vedoucímu mé diplomové práce panu Ing. Jaromíru Marušincovi, Ph. D., za jeho rady a odborné vedení.
Také děkuji pracovníkům vývojového centra CVIS Ing. Markovi Strakošovi a Ing. Michalovi Juristovi za pomoc a rady při vývoji na systému Portál VUT.
Mé poděkování patří též Edmundu Kmeťovi z databázového centra CVIS VUT za poskytnutí informací o části databáze využívané při implementaci.

Obsah

1 Úvod

Elektronická podatelna je nástroj, jehož využívání v posledních letech zažívá nárůst. Nařízením vlády, které bylo schváleno dne 25. 8. 2004, byla stanovena povinnost orgánů veřejné moci zřídit e-podatelny, vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací. Tímto zdánlivě bezvýznamným rozhodnutím se dostává občanům do ruky nástroj zjednodušující komunikaci mezi ním a orgány veřejné moci. Zajišťuje pravost doručených zpráv a schopnost zpětné kontroly nad poskytovanými informacemi.

Fenoménem, který má pomoci zajistit důvěryhodnost komunikace, je elektronický podpis. E-podpis se v posledních letech dostává stále více do povědomí obyvatelstva a vzrůstá i jeho používání při komunikaci.

Úkolem této práce bude vysvětlit pojem elektronická podatelna a pomocný nástroj elektronický podpis, analyzovat principy fungování elektronické podatelny a využívání elektronického podepisování emailů při komunikaci přes podatelnu, navrhnout a realizovat podatelnu jako modul do prostředí portálu VUT a zhodnotit její využitelnost v tomto prostředí.

Téma jsem si zvolil pro jeho praktičnost a možnost nasazení realizovaného produktu do praxe. Spojení informatiky a kryptografie, které má za cíl usnadnit společnosti život, je jistě téma hodné bližšího zájmu. Můj přínos spatřuji v prozkoumání možností e-podatelny a realizaci nástroje zjednodušujícího a zefektivňujícího komunikaci okolí nejenom s Vysokým učením technickým v Brně.

Práci jsem se snažil zpracovat stylem, který by umožňoval komukoliv s elementárními znalostmi z informačních technologií pochopit principy, na nichž elektronická podatelna stojí a utvořit si vlastní názor na současný stav i výhody jejího použití.

2 Vznik elektronického podpisu

Pohlédneme-li do historie, zjistíme, že podpis provází člověka již od nepaměti. V dávno minulých dobách měl podobu grafických značek a postupem času, kdy rostla gramotnost lidí, se začal používat podpis tak, jak jej známe dnes. S nástupem elektronické doby přichází i elektronický podpis.

Podpis je využíván ve všech právních systémech společnosti jako potvrzení souhlasu s dokumentem. Podepsáním pod dokument stvrzujeme, že jsme se podrobně seznámili s obsahem podepisovaného dokumentu a že jej bez výhrad akceptujeme.

Při používání papírového nebo jiného fyzického média, jsme vystačili s „klasickým“ podpisem. Doba se však mění. S obrovským rozvojem elektroniky a všeobecné digitalizace, s nimiž se dnes sekáváme na každém kroku a které výrazně ovlivňují naše životy, přichází i změna komunikace. Od papírové podoby se stále častěji ustupuje a přechází se na digitální, kde si již s „klasickým“ podpisem nevystačíme. Pro zaručení pravosti dokumentů v digitální podobě využíváme služeb elektronického podpisu. Kde se ale elektronický podpis vzal?

V průběhu 80. let se v důsledku velkých technologických inovací a poklesu cen informačních technologií začala rozvíjet i elektronická komunikace. Nejdříve sloužila pro posílání zpráv mezi technologickými ústavy a také ji využívalo několik „vyvolených“, kteří si mohli dovolit luxus zvaný počítač. S postupem doby, kdy nastala miniaturizace a zlevňování, se rozšířila i mezi širší vrstvy obyvatel a začala stále více nahrazovat papírovou komunikaci. V současnosti si většina z nás nedokáže představit běžný den bez kontroly své e-mailové schránky, také firmy nebo úřady bez e-mailových schránek nemohou v podstatě existovat. Hlavní důvody, proč elektronická pošta svým objemem přenosu předstihuje poštu papírovou, je nejen její rychlost, jednoduchost, dostupnost, ale i ekonomičnost.

Rozvoj elektronické komunikace nepřinesl pouze zasílání elektronické pošty. Dnes již naleznete snad veškeré informace v digitální podobě a za pomoci moderních vyhledávačů a několika kliků myši si je snadno zobrazíte. Stejně jako lidská vynalézavost a touha po zisku, tak i lenost přispěly ke vzniku elektronického obchodování. Firmy začaly vytvářet elektronické obchody, kde nabízejí své zboží. Tento způsob je velmi výhodný pro obě strany. Společnost uspoří značné prostředky na prostoru svých prodejen a přitom není omezena regionálním působením. Obchodování na internetu můžeme rozdělit do dvou nejvýznamnějších kategorií.

Prvním z nich je obchodování za účelem další distribuce. V tomto případě vzniká síť internetových obchodů, kde nalezneme veškerý možný sortiment, počínaje spínacími špendlíky a konče obráběcími stroji. Tento způsob je pro obě strany výhodný, a proto se dá očekávat jeho další rozvoj.

Druhým, co do objemu rostoucím, způsobem je zaměření se na koncového zákazníka. Tento způsob je využíván hlavně pro rozšíření odbytiště firmy. Pryč jsou časy, kdy množství prodeje bylo

úměrné počtu prodejen. Pro zákazníka tento způsob obchodování přináší ve většině případů nižší cenu, než kterou nabízejí „kamenné“ obchody. Zboží je mu do několika dnů doručeno až do domu.

Co by to bylo za obchod, kdyby se za něj neplatilo. Kde jsou doby, kdy se jeden druh zboží směňoval za druhý, dnes se za zboží platí penězi. Jak jinak platit při elektronickém obchodování než elektronicky. Na tento druh obchodování záhy reagovaly bankovní ústavy a přišli s řadou novinek. Dnes vám každý ústav k vašemu účtu nabízí řadu možností, jak je spravovat. Můžete zůstat věrni osobnímu kontaktu a navštěvovat pobočku nebo jste o něco prozíravější a nehodláte ztrácet čas stáním ve frontě a spravujete svůj účet pomocí internetu či mobilního telefonu. Tento způsob vás neomezuje na otevírací dobu, a tak máte svůj účet pod kontrolou 24 hodin denně.

Elektronické obchodování však přináší jistou anonymitu, a tudíž i nejistotu. Zajisté nepošlete peněžní obnos instituci či osobě, než si budete dostatečně jisti, že ten, s kým komunikujete je opravdu on, za koho se vydává. Tímto si musí být jisti naprosto všichni, kteří se pohybují v internetovém prostředí. Neradi byste zadali svá přístupová hesla nějakému hackerovi, který by se vydával za váš peněžní ústav. A stejně tak i banka si musí být zcela jista, že peněžní transakce prováděné s účtem, řídí jeho majitel. To samé platí i pro internetové obchodování.

V neposlední řadě zjistila i veřejná zpráva výhody elektronické komunikace a začala ji plně podporovat. Pomocí elektronických podatelen, jež dnes podle zákona musí provozovat všechny správní organizace, můžete podávat formuláře, vyřizovat žádosti, a to vše mnohem pohodlněji a rychleji. Tyto podatelny by měly pomoci od dlouhých front na úřadech a úřadům zase od přehlcení v posledních dnech termínu odevzdání například daňového přiznání. Kompletní elektronická dokumentace by rovněž měla zefektivnit a zprůhlednit průběhy řízení i způsob vykonávání veřejné moci. Aby byla elektronická komunikace mezi subjekty důvěryhodná a bezpečná, bylo třeba najít mechanismy, kterými to lze zaručit. Na pomoc přišla kryptografie. Jde o obor matematiky, podporovaný hlavně vojenskou a vládní sférou, který se zabývá zkoumáním a vývojem šifrovacích mechanizmů.

Možnost realizace elektronického podpisu přinesl až objev asymetrické kryptografie. Ten přišel v roce 1976 a začala tak nová éra kryptografie. Autory byli Whitfield Diffie, Martin Hellman a Ralph Merkle. V dřívějších dobách bylo nutné, aby dva subjekty, které si chtěly vyměňovat tajnou informaci, sdílely jedno tajemství tzv. šifrovací klíč. Pomocí něho bylo možno zprávu šifrovat i dešifrovat. V elektronickém podpisu se využívá dvojice klíčů. Jeden je soukromý a je držen pouze jeho majitelem a slouží k zašifrování zprávy. Druhou částí je veřejný klíč. Tento je veřejně přístupný a slouží k ověření pravosti zašifrované zprávy.

3 Objasnění pojmů

Všechny dříve zmíněné faktory přispěly ke vzniku elektronické podatelny a k využívání elektronického podpisu. O tom, k čemu takový elektronický podpis je, jakou má formu a jaké je v současnosti možné jeho využití, si řekneme dále. Nejprve se zaměříme na vysvětlení pojmů, které se budou v práci dále objevovat.

3.1 Elektronický podpis

Musíme začít tím, že si vysvětlíme, co to vlastně elektronický podpis je. Litera zákona nám říká toto:

„Pro účely tohoto zákona se rozumí elektronickým podpisem 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 podepsané osoby ve vztahu k datové zprávě.“ Převzato z [1]

Je důležité uvést, že elektronický podpis není pouhé převedení podpisu z papírové podoby do digitální, jak si řada čtenářů může myslet. Elektronický podpis je představován speciálně vygenerovanými daty, která jsou pro každý dokument unikátní a k datové zprávě se připojí.

„Datovou zprávou zákon rozumí elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou.“ Převzato z [2]

V naší legislativě platný zaručený elektronický podpis musí splňovat následující kritéria:

- 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. Převzato z [2]

Podmínkou pro chápání podpisu jako zaručeného je schopnost podepisující osoby udržet prostředky pro vytváření elektronického podpisu pod svou výhradní kontrolou. Prostředky rozumíme technické či programové vybavení, které je určeno k vytváření elektronického podpisu. Elektronický podpis by měl plnit jisté funkce. Lze rozeznávat čtyři funkce, kterými jsou:

- nepopiratelnost
- autentizace
- identifikace
- integrita

3.1.1 Nepopiratelnost

Použití elektronického podpisu zaručuje nemožnost popřít podepsanou osobou podepsání dokumentu stejně jako to platilo u papírové podoby.

Zákon uvádí toto:

„Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.“ Převzato z [3]

3.1.2 Autentizace

Autentizace představuje ověření, že osoba uvedená v certifikátu elektronického podpisu je skutečně osobou, která dokument podepsala. Jinými slovy, ověření proklamované identity. To zaručuje certifikační autorita.

3.1.3 Identifikace

Identifikací rozumíme jednoznačnou identifikaci osoby, která učinila právní úkon. Při použití elektronického podpisu musí být druhé straně jasné, kdo daný dokument podepsal. Neboli kdokoli musí být schopen zjistit jeho jméno a příjmení nebo jasně označený pseudonym, pokud je certifikát vydán na pseudonym.

3.1.4 Integrita

Po obdržení dokumentu, který byl elektronicky podepsán musí být zřejmé, zda-li se jeho obsah nezměnil od doby jeho podepsání. Mechanismus elektronického podpisu toto ověření umožňuje.

Poslední podmínkou pro uznání elektronického podpisu, kromě dříve zmíněných, je založení zaručeného elektronického podpisu na kvalifikovaném certifikátu vydaným akreditovaným poskytovatelem certifikačních služeb.

3.2 Poskytovatelé certifikačních služeb

Abychom mohli elektronickému podpisu důvěřovat, musí být vystaven některou z certifikačních autorit (v zákoně 227/2000 Sb. o elektronickém podpisu se nazývá *poskytovatel certifikačních služeb*). Vydáním certifikátu certifikační autorita stvrzuje, že subjekt, kterému byl certifikát vydán, skutečně vlastní daný pár klíčů (privátní a veřejný). Přirozeně certifikační autorita musí být dostatečně důvěryhodná organizace, protože jí důvěřují obě komunikující strany. Pokud certifikační autorita splní požadavky dané zákonem a zažádá o udělení akreditace, stává se po jejím udělení akreditovaným poskytovatelem certifikačních služeb.

3.3 Certifikát

Certifikát je datový soubor, uložený ve standardním, mezinárodně platném formátu. Je vydán poskytovatelem certifikačních služeb a umožňuje ověřit u certifikační společnosti identitu podepisující osoby.

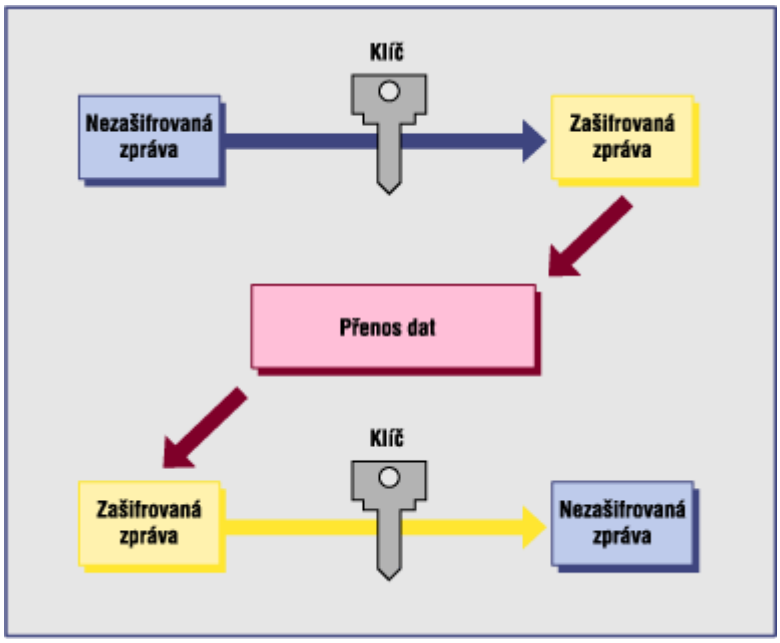
Certifikát je uznáván jako kvalifikovaný, pokud jej vydal akreditovaný poskytovatel certifikačních služeb a splňuje následující podmínky:

- nese označení, že je vydán jako kvalifikovaný certifikát
- v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen
- jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym
- zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu
- data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby
- elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává
- číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb.
- počátek a konec platnosti kvalifikovaného certifikátu
- případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití
- popřípadě omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít. Čerpáno z [4]

4 Kryptografie a elektronický podpis

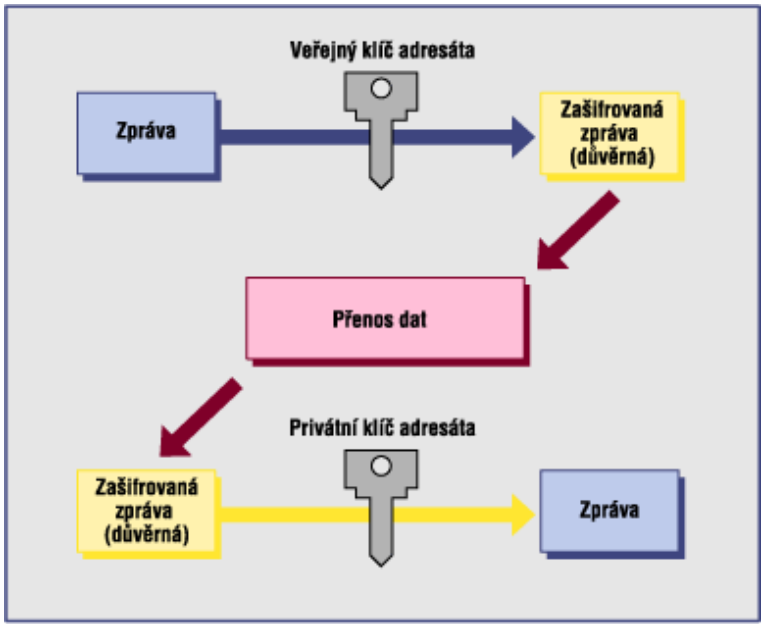
O kryptografii již zaslechl snad každý, kdo se v oblasti informačních a komunikačních technologií (ICT) pohybuje. Za to může jednak široké využití ICT v posledních desetiletích, ale především trend desetiletí posledního - využití otevřených sdílených sítí, a to zejména Internetu a telefonních sítí pro přenos informací. Kryptografie slouží k zajištění podpory mnoha aspektů bezpečnosti, nejčastěji je zmiňována důvěrnost (informace skryté v datech nezjistí nikdo nepovolaný) a integrita (nedojde k nepovolené změně dat), ale nelze nezmínit i dostupnost (data jsou k dispozici) a zodpovědnost (po manipulaci s daty se musí vědět, kdo s nimi vlastně manipuloval).

Při zašifrování dat si můžeme vybrat z řady algoritmů, které můžeme rozdělit do dvou hlavních skupin. První skupinou jsou algoritmy symetrické. Tyto využívají ke šifrování a dešifrování dat stejný klíč. Pokud tedy někomu zašleme zašifrovaná data, musí druhá strana znát klíč, aby je byla schopna dekódovat.



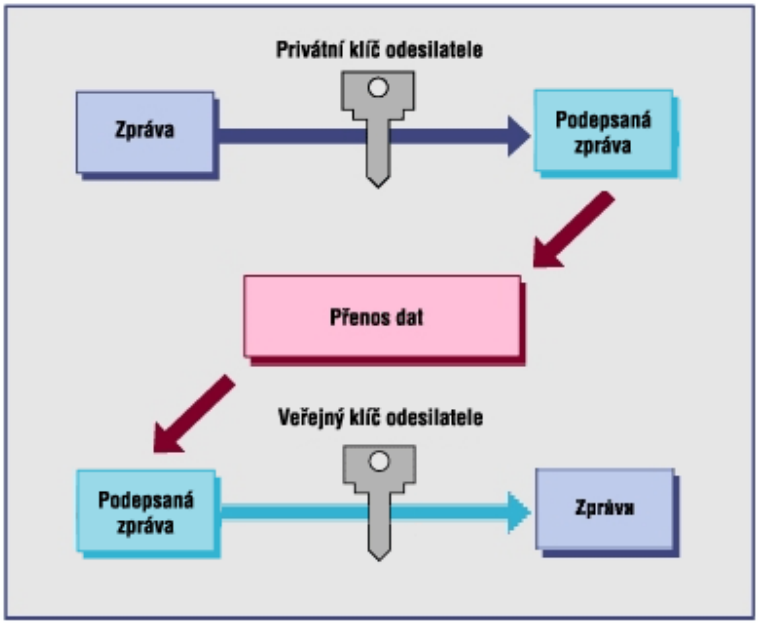
Obr. 1 -. Schéma vytvoření a přenosu symetricky zašifrované zprávy

Druhou skupinou jsou asymetrické algoritmy, jež jsou použity mimo jiné i pro tvorbu elektronických podpisů. Tyto procesy využívají dvou klíčů – veřejného a soukromého. Pro zašifrování dat se používá veřejný klíč subjektu a ten jediný na základě svého soukromého klíče je schopen zprávu rozšifrovat. Soukromý klíč vlastní pouze osoba, které byl vydán a je v jejím zájmu, aby zůstal utajen. Naproti tomu veřejný klíč si může kdokoli volně prohlédnout a zkontrolovat u certifikační společnosti, který pár klíčů vystavila.



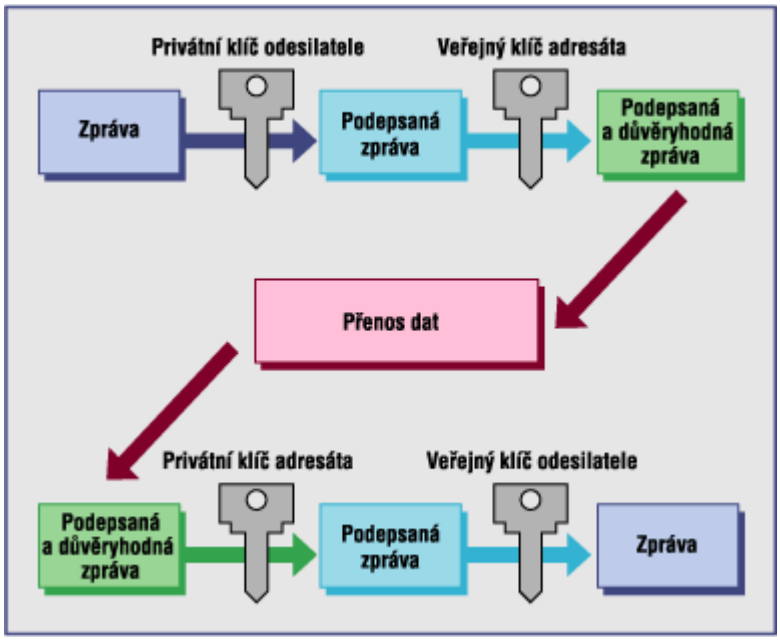
Obr. 2 – Schéma přenosu asymetricky zašifrované zprávy, ale neautorizované

Toto ovšem není způsob, který by byl využíván pro elektronický podpis. Ten totiž pracuje na opačném principu. Co je naším cílem při obdržení elektronicky podepsaného dokumentu? Zjistit, zda-li jej odepsal skutečně člověk uvedený jako odesilatel. I k tomuto můžeme využít zmiňované asymetrické kryptování s tím rozdílem, že obrátíme postup. Pokud někdo zašifruje dokument svým soukromým klíčem, jsou jej schopni dešifrovat naprosto všichni. To je naprosto nepřijatelné pro šifrovanou komunikaci, ale nám plně vyhovující. Položme si nyní otázku, kdo mohl zašifrovat zprávu, kterou jsme obdrželi a dešifrovali pomocí veřejného klíče? Nikdo jiný, než majitel soukromého klíče. A pokud je držen soukromý klíč v tajnosti, je to jediná osoba. Tím jsme se dostali k principu elektronického podpisu.



Obr. 3 – Schéma vytvoření a přenosu podepsané zprávy

Při práci s veřejným a privátním klíčem vzniká ještě jedna možnost vytvoření zprávy. Jednalo by se o zprávu, která je šifrovaná veřejným klíčem příjemce a zároveň podepsaná soukromým klíčem odesilatele.



Obr. 4 – Schéma zprávy zašifrované veřejným klíčem příjemce a podepsané odesilatelem

Nyní jsme si pouze nastínili obecné postupy při šifrování, dešifrování nebo podpisu zprávy. V dalším textu si přiblížíme některé algoritmy, jež jsou ve zmíněných procesech využívány.

4.1 Kryptografické algoritmy

Při studii problému šifrování a dešifrování dat, se seznámíme s řadou publikovaných algoritmů. Některé z nich byly již prolomeny a na jejich místo musely nastoupit algoritmy nové. O některých se tvrdí, že k jejich prolomení je zapotřebí desítky superrychlých počítačů, které by musely několik let provádět výpočty, než by se jim podařilo nalézt druhou část klíče. Obecně je ale známo, že vytvořený klíč je tím bezpečnější, čím delší je jeho řetězec. V současné době se považuje za nejbezpečnější používání algoritmů RSA či DSA založených na eliptických křivkách. Některé státy včetně České republiky mají dokonce ve svých zákonech nařízeno používání pouze těchto algoritmů.

4.1.1 Algoritmus RSA

Poprvé byl tento algoritmus publikován 4. dubna 1977. Vynalezli jej páni L. Rivest, A. Shamir a L. Adleman a posléze byl pojmenován podle počátečních písmen jejich příjmení - RSA. Algoritmus RSA je považován za jeden z nejlepších, jedinou jeho nevýhodou je značná časová náročnost. Tento problém je však řešen využitím hashovacích funkcí. Pokud tedy chceme podepsat nějakou zprávu, neprobíhá šifrování nad konkrétními daty zprávy, ale nejprve je vytvořen její „otisk“ pomocí některé

z hashovacích funkcí, který je pro každou zprávu jedinečný a při sebemenší změně zprávy musí byt vytvořen znovu, aby byl platný, a teprve poté je na získaný výsledek použit RSA algoritmus.

RSA je založen na faktu, že je velice obtížné rozložit čísla, kde každé je součinem dvou dostatečně velkých prvočísel. Nejprve tedy generujeme náhodně a nepredikovatelně dvě dostatečně velká prvočísla P a Q. Jejich minimální délka je 1024 bitů, což odpovídá dekadickému číslu o více než 100 cifrách. S těmito čísli se dále operuje, až vznikne veřejný a privátní klíč. Bližší podrobnosti o výpočtu klíčů lze získat v publikaci [5].

4.1.2 Algoritmus DSA

Druhým algoritmem, který je využíván v oblasti elektronického podpisu, je DSA (Digital Signature Algorythm) specifikovaný v DSS (Digital Signature Standard). Byl vyvinut organizacemi NIST a NSA jako alternativa k RSA, který byl tou dobou chráněn patentem. Bezpečnost tohoto algoritmu spočívá v obtížnosti výpočtu diskrétního logaritmu (obvykle je složitost této úlohy považována za ekvivalentní složitosti úlohy faktorizace - mějme dáno celé číslo n, cílem je nalézt jeho zápis ve tvaru: $n = p_1^{e1} p_2^{e2} ... p_k^{ek}$, kde p_i je prvočíslo a e_i je celé číslo). Obecná definice problému diskrétního logaritmu - mějme dánu konečnou cyklickou grupu G řádu r, její generátor α a prvek $\beta \in G$ cílem je najít celé číslo x, $0 \leq x \leq r-1$, takové, že $\beta = \alpha^x$, píšeme také $x = \log_\alpha \beta$. Doporučená délka klíče u DSA je rovněž 1024 bitů. Nevýhodou tohoto algoritmu je nemožnost jeho použití pro šifrování. Podrobnosti o algoritmu DSA lze získat v publikaci [6].

4.1.3 Hashovací funkce

Přímé používání asymetrického kryptování k šifrování zprávy není příliš vhodné vzhledem k časové náročnosti výpočtu. Jeho použití je značně pomalejší, než u jednodušších symetrických šifer. Při podepisování datově objemnějších zprávy, by odesilatel strávil značný čas čekáním na ukončení šifrování zprávy. Z tohoto důvodu se u elektronického podpisu přistupuje k mezikroku, který celý proces značně urychlí. Jedná se o využívání hashovacích funkcí.

Hashovací funkce je speciální jednocestná matematická operace. Na vstup funkce vložíme libovolný dokument, soubor či jakákoli jiná data. Výsledkem, který funkce vrátí, je soubor s přesně definovanou velikostí, tzv. hash (můžeme se setkat i s výrazem počeštěným – haš nebo otisk), který je unikátní pro daný hashovaný dokument. Provedeme-li sebemenší změnu ve vstupním souboru, promítne se tato změna i na výstupu. Na hashovací funkci jsou kladeny následující požadavky:

- výstup má jednoznačně danou pevnou délku
- pro rozdílné vstupy nesmí být stejný výstup
- při znalosti výstupu nesmí být možné zpětně dopočítat vstup

Pro potřeby elektronického podpisu se využívá v současnosti dvou funkcí. Jsou jimi MD5 (Message Digest) a SHA-1 (Secure Hash Algorithm). Funkce MD5 má výstup o délce 128 bitů. U funkce SHA-1 je výstup dlouhý 160 bitů.

4.1.3.1 MD5

Hashovací funkce vytvoří z velmi dlouhé zprávy M (soubor dat o délce a. 2^{64} bitů) hashovací kód o délce 128, resp. 160 bitů. Kompresi uvedených hashovacích funkcí zajišťuje tzv. kompresní funkce (f). U zmíněných funkcí je zpráva M před vlastním hashováním doplněna a zarovnána na celistvý počet 512 bitových bloků M_i, i=1..n, a dále je definována inicializační hodnota C (konstanta příslušné hashovací funkce). Proces hashování využívá kompresní funkci MD5 iterativně (opakovaně) takto:

$H_0=C$,
$H_i=f(H_{i-1},M_i)$, i=1..n,
$H(M)=H_n$ Čerpáno z [7]

Autorem hashovacích funkcí MD (Message Digest) je R. Rivest. Jako první z řady MD vznikla MD2 (1989), která je bajtově orientovaná a od svých 32 bitových následovníků se odlišuje i zjevnou pomalostí. V roce 1990 byla vytvořena hashovací funkce MD4 s otiskem o velikosti 128 bitů. Funkce byla rychlejší, avšak byla kolizní. Tento fakt byl dokázán na podzim roku 1991 pracovníkem německé informační služby Hansem Dobbertinem. Roku 1991 byla tedy vydána nová verze označená MD5. Funkce MD5 používá 128 bitový kód a je zhruba o 1/3 pomalejší, než byla MD4. V neprospěch této funkce přispívá i fakt, že Hans Dobbertin dokázal i v jejím případě nalézt kolizi (1996). V roce 1994 byl pány P. Oorschotem a M. Wienerem navržen stroj, realizující tzv. narozeninový paradox u 128 bitového kódu. V praxi znamená narozeninový paradox možnost nalezení kolize u 2d/2 zpráv s pravděpodobností 50%. Z této skutečnosti vyplývá, že hashovací funkce používající 128 bitové kódy jsou se současnou technologií prolomitelné. Po uveřejnění této skutečnosti sám autor doporučil nepoužívat hashovací funkci MD5 pro používání v digitálních podpisech.

4.1.3.2 SHA-1

SHA-1 byla vytvořena americkou tajnou službou NSA. Poté byla 17. 4. 1995 vyhlášena americkým úřadem pro normalizaci NIST jako standard v oficiálním dokumentu [8]. Je určena nejen pro potřeby algoritmu digitálního podpisu (DSA), ale i pro všechny aplikace ve státním sektoru, kde je požadována bezpečná hashovací funkce. SHA-1 tak nahradila svoji předchůdkyni SHA. Dokumenty jsou nazvány Secure Hash Standard (SHS), přičemž vlastní algoritmus se nazývá Secure Hash Algorithm (SHA). Rozdíl mezi definicí SHA-1 a SHA je nepatrný, ale rozdíl mezi jejich bezpečností je velký. Více v [8]. Funkce SHA-1 je považována za bezpečnou, zatímco SHA nikoli. SHA-1 byla

navržena jako standardní hashovací funkce se vstupem od 0 až do 2^{64}-1 bitů a výstupem 160 bitů. Myšlenkově vychází z návrhu algoritmu MD4, ale velmi posiluje jeho vnitřní funkce, takže zatímco u MD4 již byly nalezeny kolize, SHA-1 je vůči nim považována za rezistentní. Důležitou úlohu zde hraje také délka kódu. Jestliže jsme uvedli, že současná technologie je schopná v dosažitelném čase najít kolizi hashovací funkce, jejíž kód má délku 128 bitů, pak stejná technologie by našla kolizi u 160 bitového kódu až za 216 násobek (princip narozeninového paradoxu) této doby.

Algoritmus SHA-1 se sestává z několika hlavních kroků, které si v dalším odstavci popíšeme.

Nejprve dojde k doplnění zprávy M na délku, která je celočíselným násobkem 512 bitů. Výpočet hashovací hodnoty se provádí postupným zpracováním bloků M_1 až M_n:

1. Každé M_i rozdělíme na 16 slov W(0) a. W(15).
2. Provedeme expanzi na slova W(16) a. W(79).
3. Proměnné A až E nastavíme na konkrétní hodnoty konstant H_0 a. H_4.
4. V následujících 80 rundách přimícháváme dle vzorce slova W do konstant A až E.
5. Aktualizujeme hodnoty H_0 a. H_4 přičtením závěrečných hodnot A až E. Čerpáno z [8].

Po zpracování posledního bloku M_n je hashovací hodnota definována jako 160 bitový řetězec tvořený slovy H_0 až H_4.

5 Pravdivost informací

Nyní již máme představu jakým způsobem jsou vytvářeny soukromé a veřejné klíče, potřebné k elektronickému podepisování dokumentů a nebo k jejich šifrování. Kde ale vzít jistotu o pravdivosti podpisů?

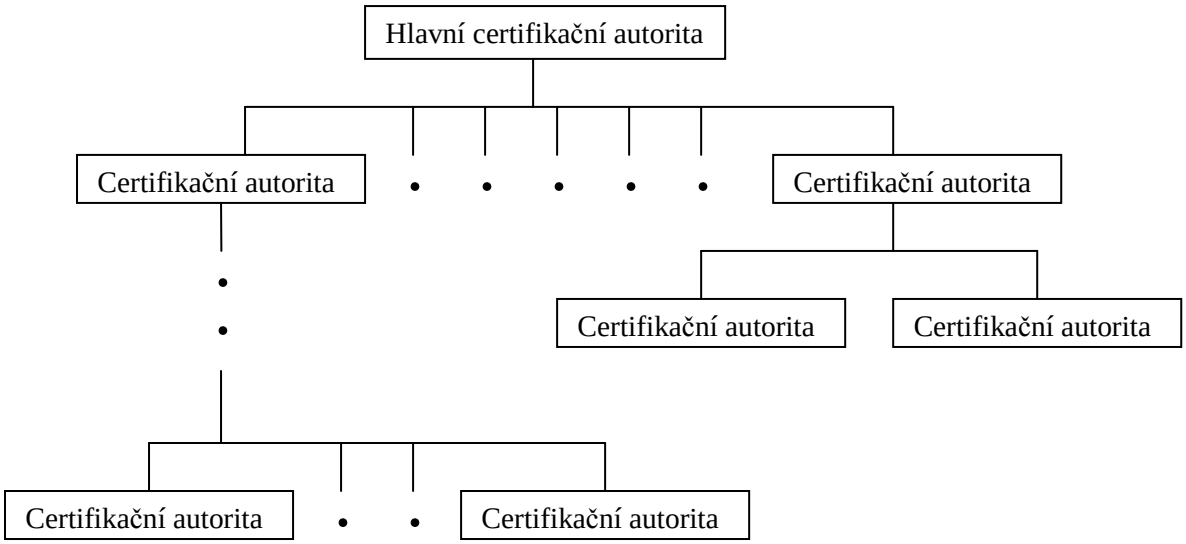
Je v podstatě nemožné v reálném čase ověřit identitu objektu na druhé straně komunikace. Musíme se tedy spolehnout, že to udělá za nás subjekt, který k tomu má prostředky. Způsobů, jak tohoto cíle dosáhnout je několik, ale já zde uvedu pouze dva nejznámější.

Prvním je systém certifikátů podle normy X.509, který se opírá o hierarchickou strukturu certifikačních autorit. Mezi země, který tento systém využívá se řadí i Česká republika. V naší zemi je využíván pro zmiňovaný elektronický podpis.

Druhým ze systému je PGP, který se pro elektronický podpis používá na úrovni komunikace mezi jedinci pomocí elektronické pošty. Tento způsob není akceptován českými úřady, neboť postrádá centrální autoritu, kterou by bylo možné dozorovat.

5.1 Standard X.509

Mezinárodně platným doporučením, které popisuje formu využití Public Key Infrastructure (PKI) je standard ITU-T X.509. PKI je soubor hardwaru, softwaru, lidí, metod a politik (vysvětleno níže v textu), které slouží k jednoznačnému přiřazení veřejného klíče konkrétnímu subjektu při využití elektronického podpisu. V současné době je využívána třetí generace. Čerpáno z [9]. Systém X.509 je na rozdíl od PGP centralizován. Na jeho strukturu lze pohlédnout jako na strom, nazývaný též stromem důvěry. Vychází se z hlavní certifikační autority (CA), která tvoří kořen stromu a je chápána jako důvěryhodná. Musí splňovat ty nejpřísnější podmínky. Její hlavní funkcí je plnit certifikační autoritu pro další poskytovatele certifikačních služeb. Nadřazená certifikační autorita certifikuje certifikační autoritu na nižší úrovní a tímto i se z níže postavené autority také stává certifikační autorita, mající možnost udělit certifikaci jiným autoritám, které o ni požádají. Tím způsobem se vytvoří strom, ve kterém se může uživatel dopracovat až k autoritě, kterou považuje za důvěryhodnou. Cesta od koncového certifikátu až k důvěryhodnému místu je nazývána certifikační cestou (certification path). Čím je cesta kratší, tím lépe systém v praxi pracuje.



Obr 5. – Náčrt stromu důvěry certifikačních autorit

Každá certifikační autorita vydává svou certifikační politiku. Jedná se o dokument, v němž CA specifikuje skutečnosti související s vydáváním osobních kvalifikovaných certifikátů, jejich další správou, použitím, akceptací, ukončením platnosti, zneplatněním a dalšími aspekty související s nakládáním s párovými daty. Dále by CA měla mít vypracovánu bezpečnostní politiku, plán pro zvládání krizových situací a plán obnovy. Tyto dokumenty značně ovlivňuje místní legislativa. Součástí standardu je i požadavek na pravidelné zpracovávání a uveřejňování CRL. Jeho vedení je rovněž jednou z funkcí CA. Nemusí ji však vykonávat sama, ale může ji delegovat na jinou instituci.

Certifikát založený na standardu X.509 má následující strukturu.

Držitel certifikátu	Identifikační údaje o osobě, které je certifikát vydáván. Ta je vlastníkem certifikovaného veřejného klíče .
Doba platnosti	Na sekundu určená platnost Od – Do, mimo tento interval je certifikát neplatný.
Název vystavitele	Identifikace CA, která vytvořila a podepsala certifikát.
Verze	Číslo, které charakterizuje použitou verzi. 0 pro v1, 1 pro v2 a 2 pro v3.
Sériové číslo	Unikátní číslo certifikátu přidělené certifikační autoritou.
Identifikace algoritmu	Určení, jaký algoritmus a s jakými parametry byl použit pro vytváření podpisu certifikátu.
Veřejný klíč	Veřejný klíč držitele certifikátu, určení pro jaké algoritmy je možné jej využít.

Další rozšíření Například umístění CRL, certifikační politiky, prohlášení, aj. Více o X.509 je možné najít přímo v normě ITU-T. Více v [9].

5.2 Systém PGP

PGP, z anglického Pretty Good Privacy, byl vyvinut primárně pro ověřitelnou e-mailovou komunikaci s bezpečným obsahem. PGP poprvé prezentoval Philip Zimmermann v roce 1991. Tento systém používá asymetrickou kryptografii pro podepisování a ověřování odesílaných zpráv. Podpis je nezávislý na zprávě, aby umožnil podepsání ostatními uživateli. Pro zachování bezpečnosti zprávy, může být šifrována za pomoci symetrického klíče, který je náhodně generován pro každou odesílanou zprávu. Následně je zpráva i klíč zašifrována veřejným klíčem příjemce. Elektronické podepisování je totožné se schématem, které jsme si popsali dříve (viz obr.3). Jako hashovací funkce používá PGP (v současném standardu OpenPGP) MD5, MD2 (dřívější verze), SHA-1 a RIPEMD-160. Pro transport speciálních znaků využívá PGP Radix-64 konverzi. Ta umožňuje převod zprávy v libovolném kódování, např. UTF-8, do ASCII a její přenos i přes starší typy kanálů. Příjemce po doručení odstraní konverzi a získá zprávu v originálním znění.

Specifikem systému PGP je nepřítomnost centrální certifikační autority. V decentralizovaném modelu každý uživatel vystupuje jako certifikační autorita. Svým podpisem pod certifikát někoho jiného mu vyjadřuje důvěru, a činí jej tak důvěryhodnějším pro ostatní. Toto je reálné, pokud se alespoň někteří z uživatelů osobně znají. V případě velkých vzdáleností mezi uživateli důvěryhodnost značně klesá.

Certifikát PGP má typicky následující strukturu:

Verze PGP	Označuje použitou verzi PGP.
Informace o držiteli klíče	Identifikační údaje – jméno, e-mail...
Certifikovaný klíč	Veřejný klíč držitele certifikátu.
Podpis držitele klíče	Ten je vytvořen soukromým klíčem držitele, který odpovídá certifikovanému klíči, tzv. self-signature.
Preferované šifrovací algoritmy	Seznam šifrovacích algoritmů, které preferuje držitel.
Doba platnosti	Časový údaj vytvoření klíče, doba jeho platnosti.
Podpisy	Podpisy ostatních uživatelů, kteří držiteli věří. Mohou být přidávány i dodatečně po vytvoření certifikátu.

V březnu roku 2001 se objevila zpráva, že bylo PGP prolomeno. Ukázalo se, že nešlo o prolomení šifrovacího algoritmu, ale o objevení bezpečnostní chyby při ukládání klíčů. Ta umožňovala úpravu souborů, které PGP program používá a následnou extrakci soukromého klíče s možností jeho zneužití pro falzifikaci podpisu.

6 Nabídka komerčních podatelen

Nařízením vlády, které bylo schváleno dne 25. 8. 2004, byla stanovena povinnost orgánů veřejné moci zřídit e-podatelny, vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací.

Pro příklad uvádím několik firem a jimi nabízené e-podatelny, které nalezl vyhledávač Google po zadání výrazu „elektronická podatelna“.

6.1 ICZ a.s.

Společnost ICZ a.s. se sídlem v Praze vyvíjí kompletní systém pro veřejnou správu. Mezi produkty, které nabízí, patří řešení pro podporu administrativních procesů, živnostenský informační systém, elektronické podpisy a podatelny a řadu dalších.

Jimi nabízená podatelna pracuje na principu klient-server. Jako serverovou technologii je využito J2EE.

Serverová část řešení zajišťuje kontrolu integrity dat od klienta včetně ověření elektronického podpisu zaslaného s daty. Podpis je přiložen buď samostatně v textovém formátu, nebo je zasílán spolu s daty v kryptografickém CMS formátu nebo XML Signatuře formátu.

V souvislosti s novelou zákona o elektronickém podpisu, která zavádí do právního řádu časová razítka a elektronické značky, nabízí také implementaci těchto nástrojů do J2EE řešení.

6.2 TOPSPIN Solutions, s.r.o.

Společnost TOPSPIN Solutions, s.r.o. vznikla na podzim roku 2006 sloučením několika fyzických osob z odvětví obchodu, ekonomiky a vývoje.

Hlavní cíl společnosti je poskytování komplexních, bezpečných a efektivních služeb. Snaží se nalézt optimální řešení mezi užitnou hodnotou a cenou poskytovaných služeb.

Jejich produkty jsou zaměřeny pro nasazení u orgánů státní moci. Firma nabízí produkt Informační systém TIS, jenž je tvořen řadou volitelných balíčků. Pro příklad uvádím některé z nich - správa ekonomiky, daní a poplatků, majetku, spisové služby, elektronického podání a další.

E-podatelna je jedním z volitelných balíčků a jde o automatizovaný serverový systém kompletně splňující požadavky vyhlášky 496/2004 Sb. o elektronických podatelnách, nařízení vlády č.495/2004, kterým se provádí zákon č.227/2000 Sb. o elektronickém podpisu a změně některých dalších zákonů, ve znění pozdějších předpisů.

6.3 ASI informační technologie s.r.o.

ASI informační technologie s.r.o je česká společnost, která již od roku 1994 poskytuje a rozvíjí odborné služby v oblasti ekonomických a informačních systémů, tvorby webových stránek a počítačových školení především pro organizace rozpočtové a příspěvkové.

Nabízí softwarový produkt určený zejména státní správě a samosprávě ke zpracování ekonomických a správních agend včetně vedení registrů nazvaný Gordic. Systém Gordic je tvořen řadou částí z nichž jedna je nazývána EPD – elektronická podatelna. E-podatelna zajišťuje:

- zpracování tzv. elektronických podání emailových zpráv obsahujících text, popř. soubory jako přílohy, obsahující digitální podpis
- ručních podání z média (disketa, CDROM), které obsahují podepsané soubory
- příjem a odesílání datových zpráv dálkovým přístupem i na technickém nosiči dat
- kontrolu, zda jsou zprávy čitelné a schopné zpracování
- ověření platnosti certifikátu náležejícího k elektronickému podpisu
- předání ověřeného podání k dalšímu vyřizování
- antivirová kontrola zpráv

Systém je provozován na počítačích vybavenými operačním systémem Windows NT nebo XP.

6.4 STUARE Post, s.r.o.

Společnost STUARE Post, s.r.o. byla založena v roce 1998. Stěžejním programem společnosti je vývoj aplikací pro klienty České pošty, s.p. včetně poskytování služeb technické pomoci uživatelům vlastních i externích aplikací. Od roku 2000 je dodavatelem klientských aplikací České pošty s.p. Důslednými pravidelnými analytickými úkony, vyhodnocováním výstupů z HOT LINE pracoviště a zpracováním požadavků České pošty, s.p. se produkty společnosti staly stěžejním komunikačním kanálem pro předávání dat mezi podavateli a pracovišti České pošty, s.p.

Společnost nabízí celkem 4 produkty. Jedním z nich je Post office. Hlavním posláním tohoto systému je zabezpečit přehlednou a úplnou evidenci práce se zásilkami. Kniha přijaté a odeslané pošty je jádrem aplikace. Novinkou systému je evidence elektronických zásilek prostřednictvím Elektronické podatelny včetně REP zásilek.

6.5 Alis spol. s r.o.

ALIS, spol. s r.o. je česká softwarová společnost bez zahraniční. Vznikla na konci roku 1990. Předmět činnosti je tvorba, údržba a distribuce SW produktů, školící a lektorské činnosti, poskytování metodicko-poradenského zázemí k distribuovaným produktům.

Mezi "vlajkové" firemní produkty patří originální a rozšířené databázové vývojové prostředí PC FAND, k němuž existují další užitečné produkty (ODBC ovladače, Tiskový manažer pro PC FAND). Rozsáhlý modulární systém ekonomicko - administrativních agend pro oblast místní samosprávy má název KEO - Komplexní evidence obce. Pro oblast školství dodává informační systém RELAX-KEŠ pro Windows. Nabízí též programy pro domácí využití.

V oblasti elektronické podatelny nabízí dva produkty. KEO – moderní kancelář a KEO-X – kancelářský systém. První ze zmiňovaných programů nabízí jednoduchou správy doručených a vlastních písemností, příloh, práce s elektronickým podpisem a jiné. Druhý program je co do počtu funkcí mnohem rozsáhlejší. Nabízí možnost běhu na operačním systému Windows i Linux, zajišťuje komplexní problematiku spisové služby, obsahuje části podatelna, referent a výpravna. Systém umí komunikovat s programy MS Office a Open Office, stejně jako s poštovními klienty Outlook a Outlook Express.

6.6 DIGNITA, s.r.o.

Rozhraní pro práci operátora nabízené podatelny je na bázi dynamických stránek HTML. Je použita technologie skriptů PHP (ver.4+), na straně MSIE pak JavaScript a pro komunikaci se serverem se částečně používá XML a RPC. Pro elektronický podpis se používá originální komponenta CAPICOM od Microsoft.

Na straně serveru je podporována platforma MS Windows a IIS (2000, XP) nebo Linux (Debian) v kombinaci s databázemi buď MS SQLServer, PostgreSQL, nebo MySQL. Nově je implementováno časové razítko a systémová značka.

Společnost nabízí na svých internetových stránkách možnost vyzkoušet si demo jejich produktu. O společnosti samotné na jejich internetových stránkách nejsou žádné bližší informace.

6.7 Porovnání nabízených produktů

Popis společností a jejich produktů, kterými jsem se zabýval v několika předešlých odstavcích, není zdaleka konečný a jistě existuje mnohem více společností, jež nabízejí elektronickou podatelnu buďto jako samostatný produkt jako v případě firem Dignita a Alis, nebo jako součást většího systému v případě ostatních firem.

Dalším kritériem pro výběr e-podatelny může být operační systém, který je provozován na serveru kupujícího. V nabídce je zastoupen jak operační systém Windows v případě produktů od firmy Alias, tak podpora Windows i Linux v případě firmy Dignita.

Rozdíly produktů jsou v podstatě minimální, protože aby mohly společnosti e-podatelny nabízet orgánům státní moci, musí splňovat zákonem definované požadavky.

7 Návrh e-podatelny pro VUT

Při zpracovávání návrhu na podatelnu pro potřeby Vysokého učení technického v Brně jsem vycházel ze struktury komerčních produktů. VUT v Brně nepotřebuje implementovat rozsáhlý systém podobný produktům nabízených firmami Asi, Topspin či Icz. Cílem projektu je vytvořit jednoduchý a funkční modul, který by se začlenil do již fungujícího systému využívaného na VUT.

Návrh elektronické podatelny počítá se dvěma částmi. Částí určenou pro veřejnost a s částí, která bude přístupná pouze zaměstnancům VUT.

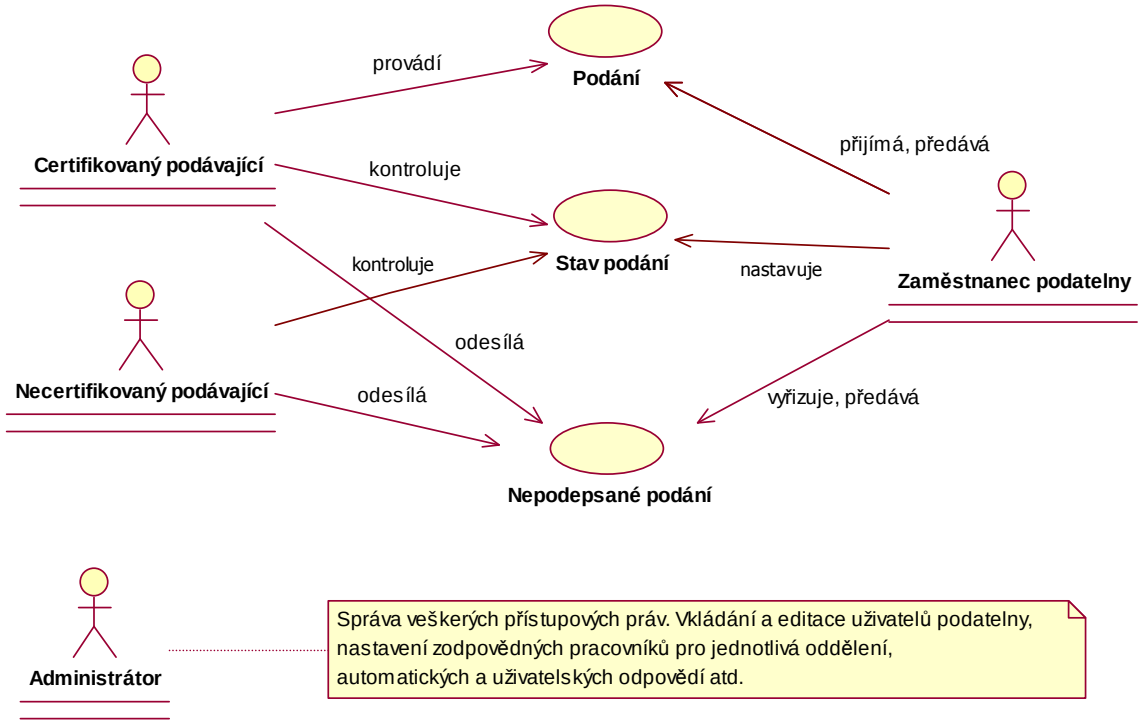
7.1 Veřejná část systému

Veřejná část podatelny bude mít dvě základní funkce. V první řadě se zde podávající dozví informace týkající se formální stránky podávané žádosti. Nalezne zde informace o formátu podání, jaké může obsahovat přílohy a kam žádost zaslat. Druhou funkcí veřejné sekce je možnost přihlášení podávajícího a následná kontrola stavu jeho zprávy. Tzn. zda byla řádně přijata, jestli se vyřizuje, nebo zda již byla vyřízena.

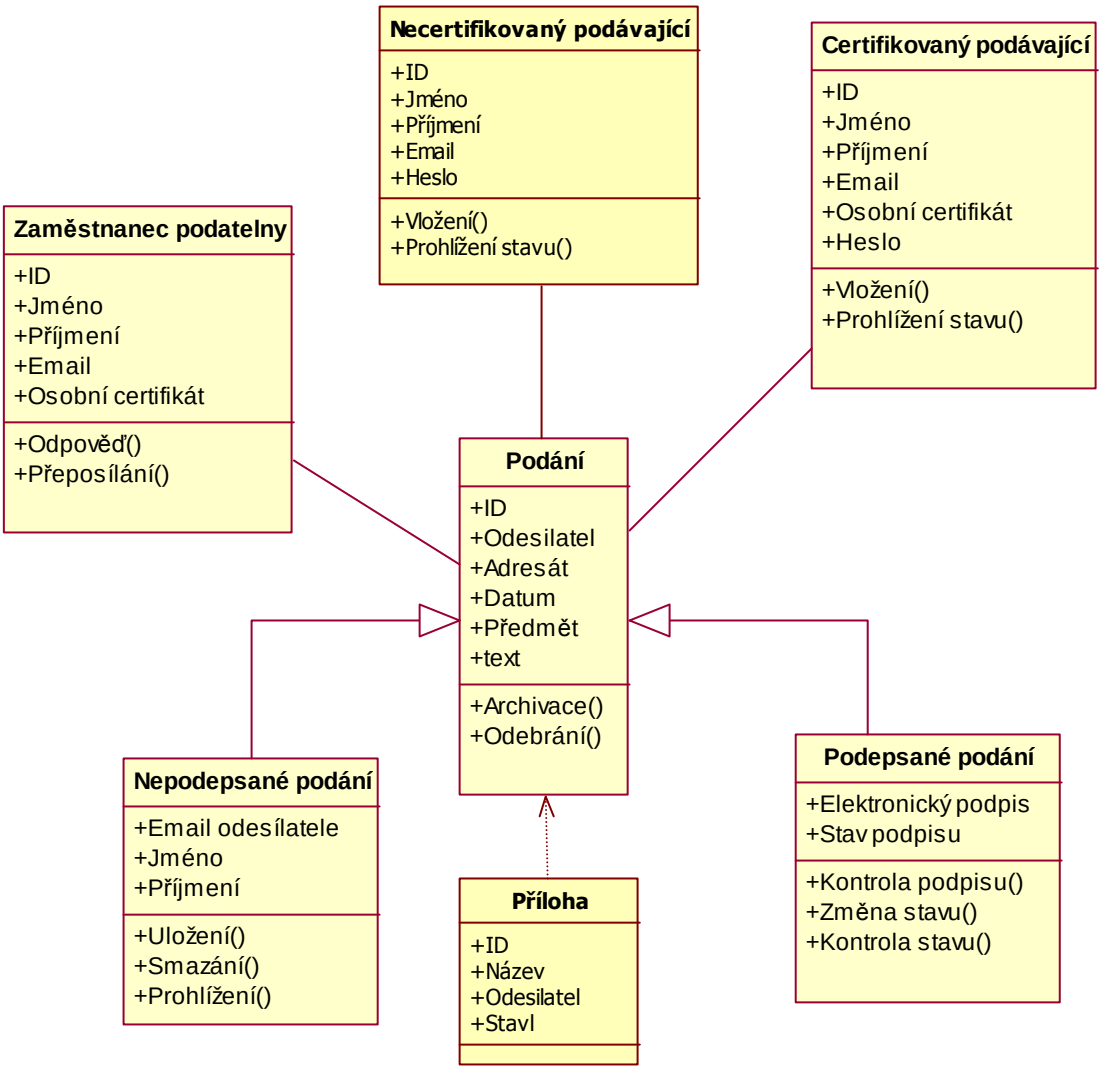
7.2 Vnitřní část systému

Vnitřní část systému bude sloužit zaměstnancům VUT nebo těm lidem, kteří budou mít v kompetenci zprávy zaslané na podatelnu zpracovávat či zodpovídat na ně. V této části budou moci pracovníci na zprávy odpovídat, popřípadě je přeposílat na jiné pracoviště či kompetentnějším osobám. Modul by měl umožňovat i přístup pro administrátora, který e-podatelnu bude spravovat. Každá osoba přistupující do systému bude mít zprávy rozděleny na nově příchozí, se kterými bude možno dále pracovat, a na sekci zpráv, na které již dotyčná osoba tazateli odpověděla. Zodpovězené zprávy bude moci uživatel pouze prohlížet včetně všech příloh. Samozřejmostí také bývá mazání zpráv. Zde je však nutno popřemýšlet, jestli tuto volbu bude mít běžný uživatel anebo pouze osoba s administrátorskými právy. Vzhledem k tomu, že by se nejednalo o soukromou korespondenci, ale o oficiální sdělení, přikláněl bych se spíše k názoru nechat volbu mazání aktivní pouze pro administrátora.

Následující obrázky ukazují návrh podatelny pro VUT.



Obr. 6 – Use case diagram návrhu e-podatelny



Obr. 7 –Diagram tříd návrhu e-podatelny

8 Implementace e-podatelny

V této kapitole se seznámíme s metodami a technikami, které byly použity při tvorbě elektronické podatelny. Budeme diskutovat důvody jejich použití a případné nedostatky. Všechny úvahy diskutované v této kapitole jsou implementovány v přiloženém programovém kódu.

Implementovaný systém je součástí většího celku, který je vyvíjen pro potřeby VUT a je využíván jako informační systém. Řekněme si tedy proto pár slov o tomto systému.

8.1 Informační systém VUT

Informační systém využívaný na Vysoké škole technické v Brně není žádným komerčním produktem, který by škola zakoupila od společnosti zabývající se tvorbou informačního systému. Jde o sytém, který je vyvíjen přímo zaměstnanci vysokého učení. Tento přístup systému, jenž škola zvolila, přináší značnou řadu výhod:

- je „šitý“ na míru potřebám školy
- neobsahuje žádné nevyužívané moduly, jako tomu bývá při zakoupení komerčních produktů
- možnosti přidávání dalších modulů jsou „prakticky neomezené“
- odezva na požadavky provádění úprav systému je okamžitá

Vývoj tohoto systému a jeho následnou správu mají na starosti oddělení CVIS (centrum vývoje informačního systému). Skládá se ze dvou částí - Vývojového centra a databázového centra. Jak je již z jejich názvu patrné, první z nich se stará o vývoj systému a druhé oddělení má na starost tvorbu a správu databází, které systém pro svoji činnost využívá.

Podíváme-li se na tento systém trochu podrobněji, lze jej rozdělit na tři funkční jednotky. První využívají učitelé a zaměstnanci, druhý je určen studentům a poslední jednotka slouží pro sdělení informací běžným návštěvníkům stránek VUT. Aplikace je vyvíjena pro část určenou zaměstnancům.

Navržený modul elektronické podatelny je určen pro zaměstnaneckou část systému.

8.2 Návrh databáze

Již při návrhu modulu bylo jasné, že část dat se bude čerpat z již vytvořených a používaných databázových tabulek a pro část dat bude nutno vytvořit tabulky nové. Při prvotním návrhu celého modulu bylo počítáno s více tabulkami, než kolik jich bylo při samotné implementaci použito. S vývojem aplikace se jejich počet postupně redukoval až se ustálil na počtu 3. Do první tabulky s názvem *mail* se ukládají informace o emailech a v druhé s názvem *attachment* se uchovávají

informace o přílohách zpráv. Hodnoty třetí tabulky podat_prac_os fungují jako nastavení pro přeposílání zpráv na jednotlivá oddělení VUT.

8.2.1 Struktura tabulky mail

Struktura tabulky *mail*, v níž se uchovávají data o příchozích zprávách či odpovědích na ně, vychází ze samotné struktury emailu. Každá mailová zpráva, aby nalezla adresáta a zároveň aby pro něj byla nějakým způsobem přínosná (tzn. neuvažujeme prázdnou zprávu), musí obsahovat vyplněné položky:

- emailová adresa odesilatele
- emailová adresa příjemce
- předmět zprávy
- tělo zprávy

Existují i další položky, které může zpráva obsahovat, např. kopie, skrytá kopie atd., tyto však pro adresáta nejsou již nikterak podstatné. Z těchto údajů jsme vyšli při tvorbě tabulky pro ukládání zpráv. V následující tabulce jsou uvedeny všechny položky tabulky i s jejich datovými typy.

NÁZEV SLOUPCE	DATOVÝ TYP
ID	NUMBER
SENT_FROM	VARCHAR(50)
SENT_TO	VARCHAR(50)
CC	VARCHAR(50)
SUBJECT	VARCHAR(200)
BODY	VARCHAR(10)
EL_SIGN	VARCHAR(256)
STATE	VARCHAR(10)
DATETIME	VARCHAR(50)
PSSW	VARCHAR(10)
ID_REF	NUMBER
ID_UZIV	NUMBER
CERT_INFO	NUMBER

Tab. 1 – Struktura databázové tabulky Mail

Podívejme se nyní na jednotlivé položky tabulky a přibližme význam hodnot, které jsou do nich ukládány.

ID – sloupec obsahuje číslo jednoznačně identifikující uložený mail v databázi

SENT_FROM – zde je uložena informace o emailu uživatele, který zprávu odeslal

SENT_TO –sloupec nese informaci o mailu příjemce

CC – prostor pro uložení emailu adresáta kopie

SUBJECT – ve sloupci je uložen text hlavička zprávy

BODY – vzhledem k tomu, že text posílaný mailem muže být dosti dlouhý, není uchováván přímo v databázi, ale je uložen do adresářové struktury a v tomto sloupci je uložen pouze název souboru s uloženým textem zprávy

EL_SIGN – je-li zpráva podepsána elektronickým podpisem, je tento soubor uložen v adresáři a do databáze je na vložen pouze název uloženého souboru

STATE – sloupec může nabývat pouze tří hodnot, PRIJATO, VYRIZOVANO, VYRIZENO, tato hodnota udává v jakém stavu zpracování se zpráva právě nachází

DATETIME – informace o odeslání emailu ve formátu „Mon, 14 May 2007 15:33:27 +0200“

PSSW – prostor pro uložení hesla, umožňujícího kontrolu stavu podání

ID_REF – obsahuje 0 jedná-li se o příchozí zprávu, jiná číselná hodnota udává, že se jedná o odpověď na zprávu číslo zde uložené

ID_UZIV – slouží k identifikaci uživatele, pro kterého je zpráva určena

CERT_INFO – číslo uvádí platnost jednotlivých složek certifikátu, 0 značí neplatnost, 1 platnost

Jak již bylo řečeno, tato tabulka slouží nejenom k ukládání příchozích zpráv, ale také odpovědí na ně. K rozlišení je využito hodnoty sloupce ID_REF.

8.2.2 Struktura tabulky attachment

Databázová tabulka *attachment* slouží k ukládání informací o přiložených přílohách k mailům. Vzhledem k tomu, že pomocí mailu lze poslat soubory i velikosti několik Mega-Bajtů, nebylo by rozumné ukládat je přímo do databáze z důvodu přílišné nabývání její velikosti. Pokud by administrátor nepromazával staré zprávy s případnými přílohami, mohlo by dojít k datovému nárůstu tabulky na Giga-Bajty a tato tabulka by zbytečně zatěžovala chod celého serveru, zpomalovala by vyhledávání a načítání hodnot z ní. V neposlední řadě by také vzrostl čas potřebný na její zálohovaní.

Z těchto důvodů se při realizaci podatelny přistoupilo k ukládání souborů příloh do adresářové struktury, jakož je tomu i v případě těla zpráv. Následující tabulka zobrazuje strukturu databázové tabulky *attachment*, včetně datových typů jednotlivých položek.

NÁZEV SLOUPCE	DATOVÝ TYP
UNIQ	VARCHAR(256)
NAME	VARCHAR(256)
SENT_FROM	VARCHAR(50)
ID_MAIL	NUMBER
STATE	VARCHAR(10)

Tab. 2 – Struktura databázové tabulky Attachment

Přibližme si nyní blíže význam hodnot, uložených v jednotlivých sloupcích tabulky.

UNIQ – v řádku tabulky je uložen název souboru přílohy, pod kterým jej nalezneme v adresářové struktuře

NAME – hodnota nese informaci o původním názvu souboru přiloženého ke zprávě

SENT_FROM – zde je uložen email odesilatele zprávy

ID_MAIL – číselná hodnota, odkazující na číslo z právy, ke které příloha náleží

STATE – řádek nabývá dvou hodnot, a to *sing* v případě jedná-li se o soubor elektronického popisu a *attachment*, jde-li o jakýkoli jiný soubor přiložený ke zprávě

8.2.3 Struktura tabulky podat_prac_os

Tato databázová tabulka neobsahuje žádné konkrétní údaje, ale jsou v ní uložena pouze metadata. Jinými slovy data v ní slouží k provázání řádků dvou jiných tabulek. A to sice tabulku *st01.mv_soucasti_vut* a *brutisadm.contact*. Z první jmenované tabulky jsou získávány informace o jednotlivých součástech VUT a k nim je přiřazena konkrétní osoba z tabulky druhé. Tabulka slouží jako nastavení odpovědné osoby pro jednotlivá pracoviště školy.

Podívejme se nyní na její strukturu.

NÁZEV SLOUPCE	DATOVÝ TYP
ID	NUMBER
ID_PRAC	NUMBER
ID_OSOBA	NUMBER

ID – číslo jednoznačně identifikující řádek v rámci tabulky

ID_PRAC – uložené číslo odkazuje na řádek tabulky *st01.mv_soucasti_vut*

ID_OSOBA – hodnota v řásku ukazuje na řádek v tabulce *brutisadm.contact*

Tabulky *mail*, *attachment* a *podat_prac_os* tvoří pilíř celého modulu elektronické podatelny. Ke své činnosti využívá podatelna i řadu jiných tabulek, které jsou součástí celého systému. Z těchto tabulek jsou čerpána data o zaměstnancích v podobě jména, příjmení, emailu a pracoviště, pod které jednotliví uživatelé spadají. Informace jsou brány z tabulek ze schématu *brutisadm* s názvy *pers_org* a *person*.

8.3 Adresářová struktura

Informační systém VUT, jehož součástí je i modul elektronické podatelny, je vyvíjen pomocí technologie PHP v kombinaci s databází vyvinutou firmou Oracle.

Původní návrh podatelny počítal s ukládáním veškerých dat do databáze. Při implementaci se však ukázalo toto řešení jako ne příliš rozumné, a tak bylo přistoupeno ke změně. Ukázalo se totiž, že při ukládání těla zprávy a příloh přímo do databáze, dochází k přílišnému toku dat mezi aplikací a databází a k nárůstu samotné databáze. Moderní databázové systémy počítají s ukládáním

objemnějších dat, avšak je vždy na zváženou, zda této možnosti využít, nebo raději data ukládat mimo databázi. Pokud by totiž nebyla data z tabulek podatelny pravidelně promazávána, došlo by po delším využívání systému k přílišnému datovému nárůstu databáze a tento jev by měl za následek zpomalení vyhledávání, čtení a zálohování databáze. Navíc by zbytečně zvětšoval datový tok mezi aplikací a databází. Z tohoto důvodu jsou do tabulek ukládány pouze informace z hlavičky mailu. Tyto textové řetězce nepřesahují velikost několika kilo-bajtů. Veškerá další data, jako je tělo zprávy a veškeré přílohy jsou ukládána do souboru v příslušných adresářích. Tento způsob s sebou nese jedno nebezpečí, které je třeba si uvědomit. Může nastat situace, kdy dva uživatelé pošlou zprávu s přílohou, která ponese stejný název. Zde by při ukládání do jednoho adresáře došlo k přepsání původního souboru, což je samozřejmě nežádoucí jev. Tento problém se dá vyřešit dvěma způsoby:

1. každá zpráva by měla vlastní adresář
2. přiřazení každému souboru jednoznačný prefix

První způsob ze zdá být řešením problému pouze ale do doby, než uživatel pošle ve zprávě dvě přílohy se stejným jménem. Došlo by opět k přepsání obsahu a místo dvou uložených souborů by vznikl pouze jeden. Z těchto důvodů byl při implementaci podatelny zvolen druhý způsob. Každému souboru je k originálnímu názvu přidán vygenerovaný pomocí systémových funkcí jednoznačný řetězec.

Tělo zprávy není tímto omezením nikterak zatíženo, a tak jsou texty v něm obsažené ukládány do souborů s názvem, skládajícím se ze dvou částí. První částí je statický řetězec *body*, druhou část tvoří číslo *id*, pod nímž je zpráva uložena v databázi. Jelikož je při ukládání zprávy zajištěna jednoznačnost *id* pro každou nově vkládanou zprávu, není důvodu se obávat, že by došlo nežádoucími přepsaní obsahu jiného souboru.

Následující tabulka ukazuje podrobně adresářovou strukturu pro ukládání souborů. Z názvů adresářů je patrné, jaká část zprávy je do nich ukládána.

Hlavní adresář	Podadresáře	Soubory
files		
├——→	attachment	veškeré přílohy emailů
├——→	body	těla zpráv
└——→	sign	elektronické podpisy

8.4 Implementace na základě návrhu

Elektronická podatelna implementovaná jako modul do informačního systému je brán z pohledu tohoto systému jako jeden celek. Při bližším pozorování je však nutno modul vnitřně rozdělit na dvě

téměř samostatné části. Jediná věc, kterou jsou spojeny v jeden celek, je práce nad společnými databázovými tabulkami (zmíněnými v předchozí kapitole) a daty s nimi souvisejícími.

8.4.1 Veřejná část systému

První část modulu by se dala nazvat „veřejnou“. Toto označení vyplývá ze skutečnosti, jaká data jsou zde zpracovávána a komu je k nim umožněn přístup. Základem je internetová stránka obsahující informace o funkčnosti podatelny. Uživatel přistupující na tyto stránky získává informace o tom, kam je možno podání zaslat. Na podatelnu může zaslat jak nepodepsané zprávy, tak i pro větší důvěryhodnost zprávy podepsané platným elektronickým podpisem. Dále je zde možno naleznout výpis s typy příloh, které elektronická podatelna přijímá. Podporovány jsou textové přílohy typu .doc, .pdf, .rtf a další. Z pochopitelných důvodů je zakázán příjem zpráv, jejichž součástí jsou přílohy ve spustitelném tvaru. Typicky se jedná o soubory s příponou .exe, .com a další.

Pokud osoba zasílající podání na mail podatelny dodrží všechna předepsaná kritéria, je zpráva podatelnou přijata. Příchozí zpráva je pomocí algoritmu rozložena na jednotlivé části (email odesilatele, tělo zprávy, přílohy, datum atd.) a tyto informace jsou posléze uloženy do databáze. Zároveň je této zprávě nastaven stav *PRIJATO*.

Jak již bylo zmíněno výše, tělo zprávy není uloženo přímo do databáze. Zde je pouze uložen název souboru, v němž se data nacházejí. K přijaté zprávě je vygenerováno heslo, sloužící podávajícímu ke kontrole stavu jeho podání. Heslo je zasláno společně s potvrzením o přijetí podání na schránku odesilatele.

Pokud zpráva obsahuje přílohy, jsou postupně zpracovány. Jedná-li se o běžnou přílohu ke zprávě, informace o ní jsou uloženy do tabulky *attachment* a samotný soubor je nahrán do adresářové struktury. Je-li však rozeznán soubor s informacemi o elektronickém podpisu, je tento soubor dále zpracováván. Provádí se kontrola na pravost certifikátu, tzn. zda-li byl vydán autorizovanou certifikační autoritou. Zjišťuje se informace o platnosti certifikátu podle data. Platnost na základě mailu odesilatele a mailu uvedeného v certifikátu a další. Soubor s certifikátem je posléze uložen stejně jako ostatní přílohy do adresářové struktury a informace o souboru uloženy taktéž do tabulky *attachment*, s tím rozdílem, že příznak ve sloupci *state* u tohoto souboru je nastaven na *sign*, aby došlo k odlišení od ostatních příloh. Získané informace z ověřování certifikátu jsou uloženy do tabulky *mail* k příslušné zprávě.

8.4.2 Vnitřní část systému

Druhou část systému nazvanou „vnitřní“ využívají zaměstnanci VUT pro přeposílání a zodpovídání příchozích podání. Označení vnitřní nese z důvodu omezených práv k jejímu přístupu a využívání. Toto právo se vztahuje pouze na zaměstnance školy.

Popišme si nyní princip chodu, funkcí a možností vnitřní části podatelny tak, jak byl implementován v rámci modulu.

Obsluhu podatelny lze hierarchicky rozřadit do tří nadřazeně uspořádaných stupňů. Na vrcholu pyramidy je jediná osoba z celého VUT. Ta zpracovává a dále distribuuje veškerá podání. Druhý stupeň tvoří jedna osoba z jednotlivých částí VUT. Na posledním stupni jsou zaměstnanci spadající pod dané pracoviště VUT.

8.4.2.1 Centrální zpracovatel podání

Veškerá nová podání, která projdou zpracováním a jsou uložena do databáze, se zobrazí osobě, určené jako centrální zpracovatel podání sídlící na vrcholu pyramidy. Tento uživatel vyhodnotí obsah zprávy a rozhodne o dalším postupu. Jedná-li se o dotaz (podání), na něž je schopen podat dostatečně kvalifikovanou odpověď, využije funkci programu *odpovědět* a pomocí částečně předvyplněného formuláře, zašle tazateli mail s požadovanými informacemi. Pokud nazná, že existuje pracoviště, kde znají přesnější údaje k řešení dotazovaného problému, použije funkci programu *přeposlat*. Jelikož osoba stojí na začátku zpracování, je prakticky nemožné, aby znala jmenovitě a profesně každého zaměstnance VUT, může tedy přeposílat zprávu pouze na některé pracoviště a nikoli konkrétní osobě.

8.4.2.2 Prostřední článek zpracování

Dostáváme se k prostřednímu členu v uskupení a tím je zaměstnanec určený pro konkrétní oddělení VUT. Při přeposlání od centrálního zpracovatele podání je daná osoba upozorněna na novou zprávu v elektronické podatelně. Zde jsou zaměstnanci k dispozici opět stejné možnosti funkcí jako nadřazenému článku řetězce zpracování.

Tazateli může na zprávu odpovědět, pokud by i on neznal řešení problému, využije taktéž možnosti *přeposlat*. V nabídce na přesměrování zprávy se mu však již nezobrazí seznam pracovišť, nýbrž pouze osoby, vztahující se danému pracovišti, na kterém je sám zaměstnán. Přesměruje-li zprávu na konkrétní osobu, je jí doručeno upozornění na novou zprávu, která čeká na vyřešení a zodpovězení.

8.4.2.3 Nejnižší článek zpracování

Nyní se již nacházíme na samém dně pyramidy. V tomto stádiu by se již zpráva měla nacházet u osoby určené k vyřízení daného podání, jež zná přesnou odpověď na dotaz. Může se však stát, že ani tato osoba nezná správné řešení otázky, a proto i na této úrovni je ponechána možnost předávání zpráv dalším osobám v systému, ale opět pouze v rámci daného pracoviště.

8.5 Podatelna z pohledu zdrojového kódu

Elektronická podatelna realizovaná rámci diplomové práce využívá technologie skriptovacího jazyka PHP (více na [10]) ve spojení s databází firmy Oracle (podrobnosti [11]). Jedná se tedy o webovou aplikaci běžící na serveru *appache* (více na [12]).

Aplikace je realizována jako samostatný modul pro portál VUT, pracující také na těchto technologiích. Zdrojový kód je rozdělen do čtyř souborů.

1. index.php – hlavní soubor aplikace
2. formulare.php – obsahuje formuláře pro práci se zprávou
3. mail_save.php – třída MailSave pro ukládání mailů
4. mime_mail.php - třída mime_mail pro posílání mailů

8.5.1 Soubor index.php

Při vývoji webových aplikací bývá zvykem, že obsah souboru index.php se uživateli zobrazí jako první a z tohoto důvodu je v něm uložena logika celé aplikace. I v tomto případě tomu není jinak. Celý chod programu je řízen jedním příkazem *switch*, který na základě řídící proměnné volá jednotlivé funkce definované v tomto souboru nebo v dalších souborech využívaných v rámci aplikace.

Řídící proměnná, definující stav aplikace, ve kterém se nachází, může nabývat těchto hodnot:

- cist – stav čtení mailu, volána funkce *obsah_mailu*
- vyrizena – v tomto stádiu jsou funkcí *vyrizene_maily* zobrazena zodpovězená podání
- preposlat – je zobrazen adresář pro výběr daného oddělení nebo osoby, které je zprávu možno postoupit
- odpovědět – řízení programu je předáno skriptu v souboru *formuláře.php*, který spravuje posílání odpovědí tazateli
- nova – stav, kdy jsou funkcí *prichozi_maily* zobrazeny všechny nezodpovězené zprávy
- default – stav, kdy řízení nepadlo ani do jedné z vyjmenovaných podmínek a opět je vyvolána funkce *prichozi_maily*

V dalších bodech se budeme podrobně věnovat jednotlivým funkcím ve skriptu, zajišťujícím chod podatelny.

8.5.1.1 Funkce prichozi_maily()

Funkce, jak je již z jejího názvu patrné, zajišťuje vypsání všech nevyřízených zpráv do tabulky, určených pro přihlášeného uživatele. Ke své činnosti využívá data z tabulky *mail*. Vstupem funkce jsou čtyři parametry:

1. ukazatel na spojení s databází

2. ID přihlášeného uživatele k aplikaci
3. počet zobrazovaných zpráv na stránce
4. číslo, od něhož jsou zprávy zobrazovány

8.5.1.2 Funkce vyrizene_maily()

Zvolením příkazu programu „Vyřízené zprávy“ se aktivuje tato funkce. Vstupní parametry jsou shodné jako v případě předchozí funkce a na jejich základě se vypíše seznam zpráv, na které v rámci provozu podatelny uživatel odpovídal.

Funkce pracuje s daty uloženými v tabulce mail. Jelikož je datum přijetí zpráv podatelnou v databázi uloženo v nepříliš uživatelsky přívětivém formátu, předávají funkce *vyrizene_maily()* a *prichozi_maily()* získaný řetězec z databáze na vstup funkce *Prevod_Datum()*. Ta řetězec zpracuje a výsledek vrátí ve formátu *dd.mm. rrrr*, což už je formát, na který je uživatel z denního života zvyklý.

8.5.1.3 Funkce obsah_mailu()

Předchozí dvě funkce slouží k výpisu pouze základních informací o zprávách uložených v databázi, a to ve formě tabulky. Z této tabulky si uživatel může vybrat zprávu, která ho zajímá a nechat si pomocí popisované funkce zobrazit kompletní zprávu včetně příloh k ní přiložených. Funkce *obsah_mailu()* čerpá data z tabulky *mail* (pro zobrazení informací o zprávě) a z tabulky *attachment*, (pro vypsání souborů přiložených ke zprávě). Vstupním parametrem je ID mailu, jehož detailní výpis uživatel požaduje. V kapitole 8.3 byl popsán způsob ukládání těl zpráv a příloh do externích souborů, tedy mimo databázi. Funkce *obsah_mailu* pro načtení těchto souborů využívá dvou dalších funkcí.

Pro načtení těla zprávy volá funkci *Body()*. Jako vstupní parametr je použit řetězec s názvem souboru, díky němuž funkce soubor otevře a vrátí jeho obsah.

Pro zobrazení interaktivního seznamu příloh je volána funkce *prilohy_mailu()*. Vstupním parametrem funkce je ID mailu, jehož přílohy chceme zobrazit. Funkce vypíše názvy souborů příloh s odkazy na jejich stažení.

8.5.1.4 Funkce Hlavicka()

Jde o poslední funkci definovanou v souboru *index.php*. Její výstup se skládá z části statické a dynamické. Statickou část tvoří nadpis systému a dva odkazy umožňující přepínání mezi zobrazením nevyřízených a vyřízených zpráv.

Dynamickou část tvoří navigační menu. Na základě počtu zpráv v každé kategorii funkce zobrazuje „rolovací“ tlačítka umožňující uživateli zobrazování seznamu novějších nebo starších zpráv. Druhou částí navigačního menu jsou akce vztahující se ke konkrétním zprávám. Jedná se o funkce odpovědět, přeposlat a zpět.

8.5.2 Soubor formulare.php

Funkce umístěné v tomto souboru přebírají řízení celé aplikace v případě přeposílání zprávy nebo vytváření odpovědi. V souboru jsou obsaženy dvě funkce:

1. odpovedni_form()
2. adresar()

8.5.2.1 Funkce odpovedni_form()

Funkce *odpovedni_form()* je volána v případě požadavku odesilatele na vytvoření odpovědi na nevyřízenou zprávu. Funkce zobrazí standardní formulář s předvyplněnými položkami Od, Komu, Subjekt a Tělo zprávy. Položka Od obsahuje email uživatele přihlášeného k aplikaci. Tento je získán z tabulky *brutisadm.contact* na základě ID uživatele. Ostatní položky jsou načteny z tabulky *mail* z řádku, kde je ID rovno parametru této funkce.

Formulář umožňuje přiložit až čtyři soubory jako přílohy k odpovědi. Při řádném vyplnění a odeslání formuláře jsou využity funkce ze tříd umístěných v souborech *mail_save.php* a *mime_mail.php*. Tyto třídy budou rozebrány později.

8.5.2.2 Funkce adresar()

Aktivace této funkce je spojena s uživatelským pokynem „přeposlat“ zprávu. Funkce zobrazí adresář s daty podle uživatelova zařazení. Jde-li o centrálního zpracovatele podání (viz odstavec 8.4.2.1), je v adresáři zobrazen seznam pracovišť, na která je možno příslušnou zprávu přeposlat. Předává-li zprávu jiná osoba než centrální zpracovatel, jsou v adresáři zobrazena pouze jména spolupracovníků z oddělení, ke kterému patří i osoba přeposílající zprávu.

8.5.3 Soubor mail_save.php

V předešlých dvou souborech byl kombinován zápis deklarace funkcí a provádění přímého kódu. Soubor *mail_save.php* obsahuje pouze třídu *MailSave* s konstruktorem a dvěmi metodami *SaveMail()* a *SaveAttachment()*.

Pomocí konstruktoru si třída uloží data vložená jako parametr při vytváření instance této třídy v programu. Konstruktor zpracovává celkem tři hodnoty. První z nich udává cestu k adresářové struktuře (viz odstavec 8.3). Druhá obsahuje data o položkách mailu, který se bude ukládat do databáze. Poslední nese informace o přiložených souborech k odpovědi. Tyto budou také uloženy do adresářové struktury.

Metoda s názvem *SaveMail()* zpracovává druhou položku uloženou konstruktorem. Jedná se o informace z odpovědního formuláře řádně vyplněného a odeslaného uživatelem. Metoda obdržená data uloží do databázové tabulky *mail* kromě těla zprávy. To je uloženo do souboru (viz kapitola 8.2.1). Zprávě, které odpověď patří, nastaví položku *state* na hodnotu VYRIZENO.

Druhá metoda s názvem *SaveAttachment()* zpracovává třetí položku uloženou konstruktorem. Jedná se také o data z odpovědního formuláře, ale obsažená informace se týká příloh přiložených k odpovědi. V cyklu se postupně zkontrolují informace ze všech čtyř polí formuláře, určených k přikládání souborů. Pokud byl ke zprávě nějaký soubor přiložen, proběhne kontrola na podporu typu souboru. Je-li výsledek v pořádku, soubor je uložen do adresářové struktury a informace o něm uloženy do databázové tabulky *attachment*.

8.5.4 Soubor mime_mail.php

Obsahem souboru je opět programový kód na tvorbu třídy. Kód v tomto souboru byl převzat z publikace [13]. Soubor obsahuje třídu s názvem *mime_mail.php*. Tato třída slouží k posílání mailů s přílohou. Obsahuje konstruktor a 5 metod. Názvy metod nalezneme v následujícím seznamu:

1. add_attachment()
2. build_message()
3. build_multipart()
4. get_mail()
5. sent()

Pomocí metody *add_attachment()* můžeme k budoucí zprávě poslané pomocí PHP funkce *mail()* vkládat soubory.

Metody 2 až 4 slouží k sestavení celé zprávy z jednotlivých částí. V první řadě je vytvořena hlavička. Tzn. informace o odesilateli, příjemci, předmětu zprávy. Poté jsou ke zprávě připojeny jednotlivé soubory.

Pomocí zavolání poslední metody s názvem *sent()*, odešle skript email s nastavenými parametry a obsahem.

9 Závěr

Hlavním předmětem zájmu tohoto projektu bylo fungování elektronické podatelny. Při tvorbě této práce jsem získal poznatky z oblasti elektronického podpisu, kryptografie, certifikátů a certifikačních společností. Toto všechno jsou prostředky využívané v komerčních podatelnách. Cílem projektu bylo vytvořit funkční modul elektronické podatelny pro prostředí Portálu VUT.

V průběhu práce byly analyzovány hlavní kryptografické algoritmy využívané při elektronické podepisování a šifrování. Byly rovněž rozebrány dva principy pro ověřování pravosti elektronických podpisů.

Za hlavní přínos této práce považuji praktičnost demonstrace elektronické podatelny v prostředí informačního systému VUT a její možné nasazení do běžného provozu. Elektronická podatelna a jí využívané podepsané dokumenty nebo zprávy jsou krokem na cestě za bezpečnější komunikací v otevřeném internetu, kde na neopatrného uživatele číhá nebezpečí na každém kroku.

Přestože se v současné době podepisování zpráv certifikáty nikterak hromadně nevyužívá, můžeme s jistotou říci, že tak jako byl počítač před dvaceti lety neznámý pojem a nyní jej využívají skoro všichni, tak věřím, že i budoucnost elektronického podpisu přijde. Již teď mohu říci, že elektronické podatelny v sobě skrývají obrovský potenciál, který společnost ocení v průběhu několika budoucích let se vzrůstající informační gramotností.

Další práci na tomto projektu spatřuji především ve větší práci s certifikáty na straně systému využívaného zaměstnanci VUT a zdokonalení komunikačního rozhraní s uživatelem, aby práce s programem přinášela potěšení a nikoli pouhou povinnost.

.

Seznam obrázků

Literatura

[1] Zákon 227/2000 Sb. o elektronickém podpisu § 2, Dokument dostupný na URL http://www.micr.cz/files/1540/UZ-227_2000.pdf

[2] Zákon 227/2000 Sb. o elektronickém podpisu § 2, Dokument dostupný na URL http://www.micr.cz/files/1540/UZ-227_2000.pdf

[3] Zákon 227/2000 Sb. o elektronickém podpisu § 3a, Dokument dostupný na URL http://www.micr.cz/files/1540/UZ-227_2000.pdf

[4] Zákon 227/2000 Sb. o elektronickém podpisu § 12, Dokument dostupný na URL http://www.micr.cz/files/1540/UZ-227_2000.pdf

[5] RSA Laboratories, *PKCS #1 v2.1: RSA Cryptography Standard*, 14 června 2002, Dokument dostupný na URL ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

[6] National Institute of Standards and Technology FIPS PUB 186-2, *Digital signature standard (DSS)*, Dokument dostupný na URL http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[7] Pinkava, J. *Hashovací funkce v roce 2004*, říjen 2004, Dokument dostupný na URL http://crypto-world.info/pinkava/clanky/hash_2004.pdf

[8] Federal Information, *Secure hash standard*, FIPS PUB 180-1, 17. dubna 1995, Dokument dostupný na URL http://www.niatec.org/pdf/fips180-1.pdf

[9] Chokhani, S., Ford, W., Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, březen 1999, Dokument je dostupný na URL http://www.ietf.org/rfc/rfc2527.txt

[10] Manuálové stránky skriptovacího jazyka PHP, www.php.net

[11] Internetové stránky společnosti Oracle, www.oracle.com

[12] Manuálové stránky serveru Apache, httpd.apache.org

[13] Castagnetto, J., Schumman, S., Rawat, H., Scollo, Ch., Veliath, D., T., *Proffesional PHP Programming*, Wrox Press 1999

Seznam příloh

Příloha 1 – Manuál

Aplikace elektronická podatelna je vytvořena jako webová aplikace. Proto při jejím ovládání platí stejná pravidla jako při pohybu na internetu. Fungují zde klávesové zkratky

- *CTRL+P* – tisk zobrazené stránky
- *CTRL+S* – uložení zobrazené stránky
- *Pravé tlačítko myši* – zobrazení místní nabídky

Po přihlášení do aplikace je zobrazena tabulka s nevyřízenými zprávami. Viz obrázek P1

Elektronická podatelna VUT			
Nové zprávy Vyřízené zprávy			
« předchozí další »			
Nové zprávy			
#	Datum	Od	Předmět
17	07.04. 2007	terka7@seznam.cz	zprava 13
16	07.04. 2007	cviceni4@centrum.cz	zprava 12
15	07.04. 2007	terka3@seznam.cz	zprava 11
14	07.04. 2007	cviceni2@centrum.cz	zprava 10
13	07.04. 2007	terka1@seznam.cz	zprava 9
12	07.04. 2007	smk@seznam.cz	zprava8
11	07.04. 2007	terka@seznam.cz	zprava7
10	07.04. 2007	cviceni@centrum.cz	zprava6
9	07.04. 2007	karel@post.cz	zprava5
8	07.04. 2007	petr@seznam.cz	zprava4
7	07.04. 2007	tom@seznam.cz	zprava3
6	07.04. 2007	nekdo@vonlny.cz	zprava 2
5	07.04. 2007	pokus@tiscali.cz	zprava 1
4	14.05. 2007	majlon@email.cz	podepsana zprava
3	07.04. 2007	epodatelna@centrum.cz	pokus1

Obr. P1 – Výpis nevyřízených zpráv

Na jeden výpis je zobrazeno maximálně 15 zpráv. Pokud je v databázi více nevyřízených zpráv, přepínáte mezi jejich zobrazením pomocí tlačítek *předchozí*, pro zobrazení novějších zpráv a *další*, pro výpis starších zpráv.

Detail zprávy zobrazíte po kliknutí na email odesilatele, nebo předmět zprávy. Na obrázku P2 je zobrazen detail příchozí zprávy. Výpis zprávy je rozdělen do tří částí.

1. Hlavička zprávy – informace o odesilateli, příjemci, datu odeslání a předmětu zprávy
2. Tělo zprávy – zde je zobrazen obsah doručené zprávy
3. Přílohy – pokud zpráva obsahuje přílohy, jsou vypsány v této sekci.

Nad hlavičkou je umístěn seznam akcí, které je možno se zprávou provádět

1. Odpovědět – tlačítko slouží k zobrazení formuláře pro odeslání odpovědi na zprávu

2. Přeposlat – funkce vyvolá zobrazení adresáře s výpisem osob nebo oddělení, kterým je možno zprávu přeposlat
3. Smazat – funkce na smazání zprávy
4. Zpět – návrat do výpisu zpráv

Elektronická podatelna VUT	
Nové zprávy Vyřízené zprávy	
	odpovědět | přeposlat | smazat | zpět
Datum:	14.05. 2007
Od:	majlon@email.cz
Komu:	epodatelna@centrum.cz
Předmět zprávy:	podepsana zprava
Tělo zprávy:	
telo telo	
Přílohy	
smime.p7s	

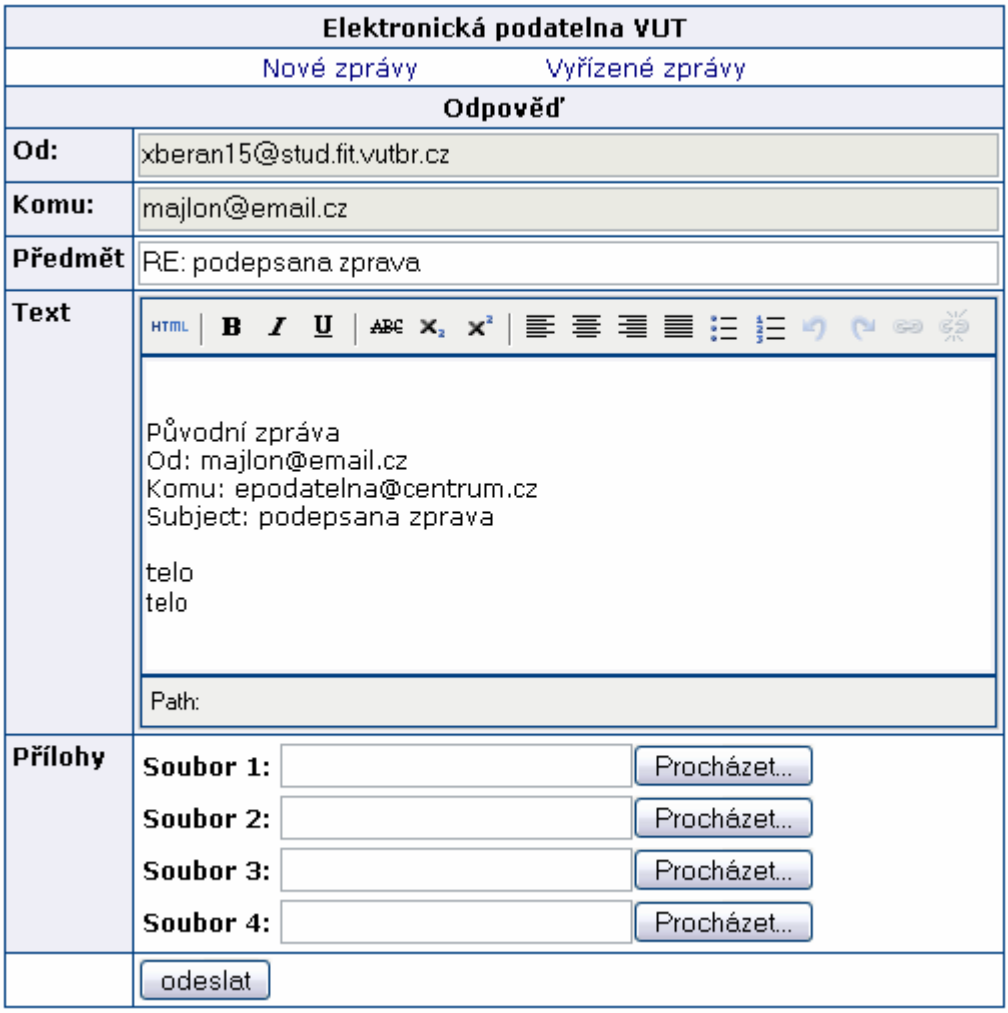
Obr. P2 – Detailní zobrazení nové zprávy

Při zvolení volby odpovědět je zobrazen částečně předvyplněný formulář (viz obrázek P3). Opět je rozčleněn na tři sekcí. Hlavička, kde jsou informace o odesilateli, příjemci a předmětu zprávy. Tělo, sloužící k napsání obsahu zprávy. Poslední část tvoří vstupní pole, umožňující přiložit ke zprávě až čtyři soubory. Soubory přiložíte po kliknutí na „Procházet..“. Zobrazí se diskový manažer, v němž vyberete soubor který chcete ke právě přiložit. Vložení souboru dokončíte pomocí talčítka „Otevřít“. Po vyplnění formuláře a kliknutí na tlačítko odeslat, dojde k odeslání zprávy tazateli.

Program e-podatelny v tuto chvíli přejde k zobrazeni seznamu vyřízených zpráv (viz obrázek P4). Zde je vždy zobrazena hlavička původní zpráva a pod ní hlavička odpovědi. Po kliknutí myší na email nebo předmět u zprávy nebo odpovědi ke zprávě, se zobrazí detailní výpis zprávy a odpovědi na ni. Ukázka výpisu je na obrázku P5.

V detailu zodpovězené zprávy můžete použít dvě tlačítka. „Smazat“ pro odstranění zprávy a volbu „Zpět“ pro návrat do výpisu zodpovězených zpráv.

Pro přecházení mezi výpisem nevyřízených a vyřízených zpráv slouží tlačítka „Nové zprávy“ a „Vyřízené zprávy“.



Obr. P3 – Předvyplněný odpovědní formulář

Obr. P4 – Výpis vyřízených zpráv

Elektronická podatelna VUT	
Nové zprávy	Vyřízené zprávy
	smazat | zpět
Datum:	07.04. 2007
Od:	epodatelna@centrum.cz
Komu:	epodatelna@centrum.cz
Předmět zprávy:	ýěšíýěčěšč
Tělo zprávy:	
body body body	
Odpověď	
Datum:	22.05. 2007
Od:	xberan15@stud.fit.vutbr.cz
Komu:	epodatelna@centrum.cz
Předmět zprávy:	RE: ýěšíýěčěšč
Tělo zprávy:	
odpověď s přílohou Původní zpráva Od: epodatelna@centrum.cz Komu: epodatelna@centrum.cz Subject: ýěšíýěčěšč body body body	
Přílohy	
05101315.zip	

P5 – Detailní výpis zprávy a odpovědi na ni