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

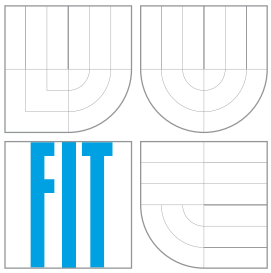
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

MILAN TOMÁŠEK

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

ELECTRONIC MAIL ROOM OF THE BUT

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — MILAN TOMÁŠEK

AUTHOR

VEDOUCÍ PRÁCE — Ing. JAROMÍR MARUŠINEC, Ph.D.

SUPERVISOR

BRNO 2007

Zadání

1. Prostudujte problematiku elektronického podepisování emailů a problematiku osobních certifikátů.
2. Prostudujte a porovnejte dostupné komerční elektronické podatelny nabízející služby státním úřadům.
3. Navrhněte elektronickou podatelnu pro VUT. Kromě technické části se také zaměřte na návrh organizačního zabezpečení na VUT.
4. Realizujte elektronickou podatelnu VUT ve spolupráci s CVIS jako webovou aplikaci na Portálu VUT.
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.

Licenční smlouva

Licenční smlouva je uložena v archivu Fakulty informačních technologii Vysokého učeni technického v Brně.

Abstrakt

Hlavním cílem této práce je vytvořit elektronickou podatelnu pro VUT. V první řadě jsem popsal problematiku týkající se elektronického podpisu, jeho použití, bezpečnosti a s elektronickým podpisem také úzce související oblast kvalifikovaných certifikátů a způsobu jejich vydávání certifikačními autoritami. Další část této práce se zabývá systémy umožňujícími podání v elektronické podobě (tzv. elektronická podatelna). Zaměřil jsem se na dostupné aplikace poskytující službu elektronické podatelny státním úřadům a následně analyzoval funkce, které jednotlivé aplikace nabízejí jak klientům podatelny, tak zaměstnancům daného úřadu. Na základě získaných znalostí a požadavků CVIS jsem vytvořil návrh elektronické podatelny pro potřeby VUT v Brně. Výsledkem této práce je vytvořená aplikace elektronické podatelny, implementovaná do portálu VUT v Brně.

Klíčová slova

Elektronický podpis, osobní certifikát, certifikační autorita, certifikace, elektronická podatelna, elektronické podání.

Abstract

The main purpose of this master's thesis is to create electronic mail room of The BUT. First of all I described problems concerning a digital signature, its use and safety, and as well as sphere of qualified certificates and method of their issuing by certification authority. The next part of the thesis deals with systems enabling electronic submission (so-called "Electronic Mail Room"). I have focused on available applications providing electronic submission service to civil offices, and subsequently analyzed functions that individual applications offer to the Mail Room clients as well as to authority staff. On the basis of gained knowledge and according CVIS requirements I created project of electronic submission for needs of the Brno University of Technology. Result of this thesis is the application of electronic mail room, implemented in BUT portal.

Keywords

Digital signature, personal certificate, certification authority, certification, electronic mail room, electronic submission.

Citace

Milan Tomášek: Elektronická podatelna VUT, diplomová práce, Brno, FIT VUT v Brně, 2007

Elektronická podatelna VUT

Prohlášení

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

.....

Milan Tomášek

21. května 2007

Poděkování

Chtěl bych tímto poděkovat panu Ing. Jaromíru Marušincovi, Ph.D., Ing. Marku Strakošovi a Ing. Michalu Juroszovi, za užitečné podněty a rady při práci na mé diplomové práci.

Obsah

Kapitola 1

Úvod

Hlavním cílem této práce je vytvoření systému elektronické podatelny pro potřeby VUT v Brně. V první řadě se budu zabývat problematikou elektronického podpisu, jeho využitím a způsobem realizace. Také se zaměřím na bezpečnostní kritéria při používání této technologie.

Dále bude následovat kapitola zabývající se osobními certifikáty, kde se budu zabývat jejich strukturou, informacemi v certifikátech obsaženými, k čemu se certifikáty vlastně používají a způsobem, jakým je možné vytvořit si svůj vlastní kvalifikovaný certifikát. V souvislosti s osobními certifikáty se také zaměřím na organizace, které mají oprávnění je vydávat a rušit jejich platnost.

V kapitole věnované elektronickým podatelnám se pokusím vybrat několik subjektů poskytujících službu elektronické podatelny úřadům a veřejnoprávním institucím v České republice a porovnat jejich funkce.

V závěru se zaměřím na vytvoření elektronické podatelny pro VUT. Rozeberu požadavky na funkce podatelny a pokusím se vytvořit model systému, jednak pomocí ER diagramu tříd a poté pomocí diagramu případů užití.

Kapitola 2

Elektronický podpis

Elektronický podpis je jedna z hlavních možností identifikace uživatele při komunikaci na internetu. Stejně jako klasický podpis slouží k ověření totožnosti konkrétní osoby k datové zprávě. Nutnou podmínkou pro používání elektronického podpisu jsou kvalifikované certifikáty, které jsou v České republice vydávány akreditovanými poskytovateli (akreditace těmto společnostem uděluje Ministerstvo informatiky) [1].

2.1 Realizace elektronického podpisu

Pro realizaci elektronického podpis se využívají kryptografické algoritmy s privátním a veřejným klíčem. Základní princip spočívá ve vytvoření dvojice různých, matematicky vázaných klíčů (tzv. asymetrický kryptografie). Jedná se o veřejný klíč, který se využívá k zašifrování zpráv, a privátní klíč, určený k dešifrování přijaté zprávy, který musí zůstat před ostatními utajen. Zašifrujeme-li danou zprávu veřejným klíčem příjemce, pak pouze on s pomocí svého privátního klíče může tuto zprávu dešifrovat a přečíst. Dvojice klíčů musí být navržena tak, aby nebylo možné ze známého veřejného klíče odvodit klíč privátní.

U elektronického podpisu se používá opačného postupu, než u šifrování datové zprávy. Uživatel tak pomocí svého privátního klíče připojí k odesílané zprávě elektronický podpis a každý, kdo zná veřejný klíč může pomocí něj ověřit, zda jde opravdu o konkrétního uživatele.

Při ověření elektronického podpisu postupuje příjemce tak, že nejdříve vypočte pomocí stejné hash funkce kontrolní vzorek zprávy, poté s využitím veřejného klíče osoby, která datovou zprávu podepsala, dešifruje elektronický podpis čímž získá druhý kontrolní vzorek. Oba vzorky se následně porovnají a jsou-li shodné, je potvrzena pravost elektronického podpisu.

Tento postup zaručuje, že zprávu mohl podepsat pouze ten, kdo má k deklarovanému veřejnému klíči odpovídající privátní klíč. Kromě toho také dává příjemci zprávy jistotu integrity dat (zpráva nebyla modifikována v průběhu přenosu).

Samozřejmě je velmi důležité, aby privátní klíč uživatele zůstal opravdu privátním a

nezískala ho nepovolaná třetí osoba. V takovém případě by byl elektronický podpis velice jednoduše zneužitelný.

Schéma elektronického podepisování zpráv a následného dešifrování s kontrolou integrity dat je znázorněno na obr. 2.1.

2.1.1 Asymetrická kryptografie

Asymetrická kryptografie (ASK) je jedním ze základních prostředků pro zajištění bezpečnostních požadavků při komunikaci elektronickou cestou po veřejných sítích, kde je kladen důraz na zvýšenou ochranu dat a autentizaci všech komunikujících stran.

Na rozdíl od symetrické kryptografie využívající pro fáze šifrování i dešifrování zprávy tajný klíč, se asymetrická kryptografie vyznačuje použitím dvojice klíčů a je také často označována za kryptografii s veřejným klíčem.

Infrastruktura veřejných klíčů

Proto aby bylo možné ASK efektivně využívat je potřeba zajistit důvěryhodné zveřejňování veřejných klíčů. K tomu slouží tzv. Infrastruktura veřejných klíčů PKI (Public Key Infrastructure) [7]. Jde o prostředí, které umožňuje ochranu informačních systémů, elektronických transakcí a komunikace. Je v něm zahrnuto veškeré softwarové vybavení a technologie, které jsou určeny pro šifrování s veřejným a privátním klíčem.

2.1.2 Šifrovací algoritmy

Základními algoritmy, které se používají k podepisování datových zpráv, jsou algoritmy RSA a DSA. Jedná se o asymetrické algoritmy, využívající principu dvojice klíčů.

Pomocí těchto algoritmů dochází k vytvoření elektronického podpisu ve dvou krocích. V první fázi se z datové zprávy pomocí hash funkce vytvoří kontrolní vzorek. Tento vzorek je následně zašifrován a vzniká tak elektronický podpis, který se připojí k původní zprávě. Při dešifrování dochází opět k vytvoření kontrolního vzorku pomocí hash funkce a k dekódování elektronického podpisu. Oba dva kontrolní vzorky musí být shodné (obr. 2.1).

Algoritmus RSA

Tento kryptovací algoritmus vznikl v roce 1977 a je pojmenovaný podle svých tvůrců (Ron Rivest, Adi Shamir, Leonard Adleman). Jeho princip spočívá v obtížnosti rozkladu velkých čísel na součin prvočísel (faktorizace). V současné době se nejvíce používají RSA klíče dlouhé 1024 – 2048 bitů.

Algoritmus DSA

Digital Signature Algorithm je systém vyvinutý v USA a je součástí Digital Signature Standard (DSS). Nedá se využít k šifrování dat podle normy. Jako hashovací algoritmus pro DSA se v současné době využívá SHA-1 (Secure Hash Algorithm).

Hashovací funkce

Podle doporučení NBÚ by se již v případě bezpečnostních aplikací neměly využívat hashovací funkce s výstupem menším než 160 bitů, jako jsou například MD5, RIPEMD, HAVAL-128, atd.

Předpokládaná doba, do kdy bude dostačující hashovací funkce SHA-1, je rok 2010. Po tomto roce by měla být nahrazena silnějším a bezpečnějším algoritmem SHA-2 [2].

Na základě vyhlášky č. 378/2006 Sb. nesmějí například akreditovaní poskytovatelé certifikačních služeb využívat hashovací funkci MD5. V souvislosti s touto vyhláškou byl zveřejněn odkaz na tzv. ALGO paper, ve kterém jsou stanoveny požadavky na kryptografické algoritmy a jejich parametry, které mohou být použity v aplikacích vyžadujících zvýšenou bezpečnost.

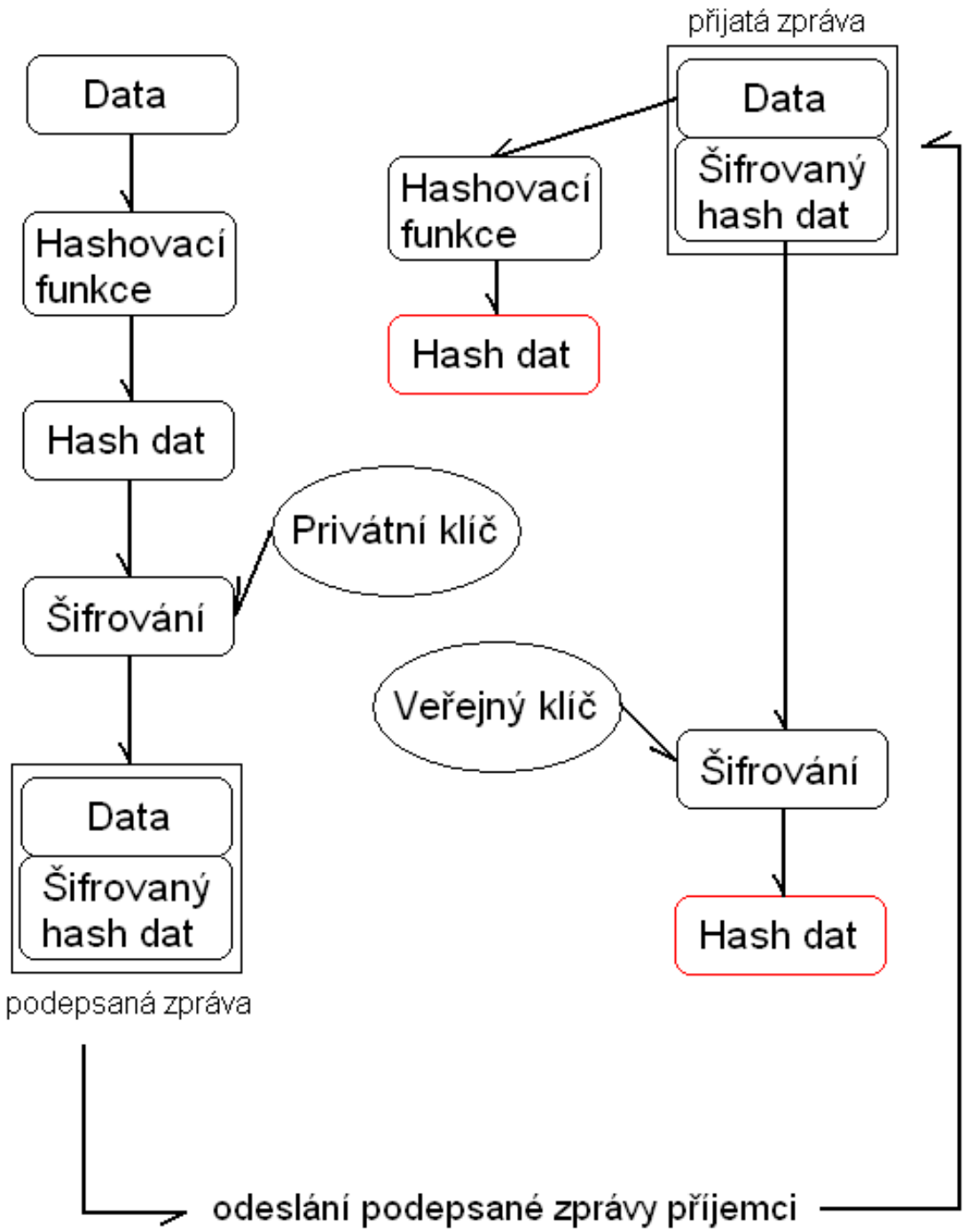
V současné době je nejvyužívanější kombinací kryptovací algoritmus RSA společně s hashovací funkcí SHA-1.

2.2 Bezpečnost elektronického podpisu

Pro zaručení bezpečnosti elektronického podpisu je potřeba zajistit, aby nemohlo dojít k získání privátního klíče a nebyl prolomen algoritmus použitý pro tvorbu elektronického podpisu. Také musí být jasné, že veřejný klíč opravdu náleží k osobě, která zprávu podepsala. Proto existují nezávislé instituce vydávající osobní certifikáty (certifikační autority).

Je-li elektronický podpis využíván pro operace vyžadující nejvyšší míru zabezpečení, jako jsou například finanční transakce, je obzvláště potřeba věnovat zvýšenou pozornost souboru doporučení týkajících se osob, jež tento podpis používají. Tato doporučení jsou zveřejněna ministerstvem informatiky České republiky.

Každá osoba využívající elektronický podpis za použití kvalifikovaných certifikátů (vydaných všeobecně uznávanou certifikační autoritou) by se rovněž měla řídit zákonem o elektronickém podpisu (z roku 2000), který definuje jak zacházet s prostředky a daty pro vytváření zaručeného elektronického podpisu tak, aby nemohlo dojít k jejich neoprávněnému použití. V případě podezření na možnost zneužití elektronického podpisu je nutné o této skutečnosti neprodleně informovat vydavatele příslušného kvalifikovaného certifikátu, aby mohlo dojít k jeho zneplatnění [3].



Obrázek 2.1: Schéma elektronického podepisování dat

Kapitola 3

Osobní certifikáty

Osobní certifikáty jsou důležitým nástrojem, jak ověřit příslušnost uživatele ke konkrétnímu veřejnému klíči (který je pro každého uživatele jednoznačný), aby bylo možné s jistotou určit, zda danou zprávu skutečně odeslala osoba uvedená v certifikátu. Jedná se o datový soubor, uložený v mezinárodně platném formátu daném normou X.509, popisující strukturu certifikátu [9].

Existuje několik typů certifikátu podle toho, k jakému účelu a jakému subjektu jsou vydány (fyzická osoba, firma).

Doba, po kterou je certifikát platný, je z bezpečnostních důvodu omezená. Obvykle jsou certifikáty vydávány s dobou platnosti 6 až 12 měsíců. Vzhledem k rychlému zvyšování výkonu výpočetní techniky by se totiž certifikáty mohly stát v delším časovém období nespolehlivé.

3.1 Struktura certifikátu podle mezinárodní normy X.509

Jde o normu z roku 1988, která přesně definuje strukturu certifikátu a pravidla pro jeho vystavení certifikační autoritou (v současné době je aktuální verze 3).

- Certifikát:
  - Verze certifikátu (Version)
  - Unikátní sériové číslo certifikátu (Serial Number)
  - Typ šifrovacího algoritmu (Signature Algorithm)
  - Vydavatel certifikátu - Certifikační autorita (Issuer)
  - Datum začátku a konce platnosti certifikátu (Validity)
  - Identifikační údaje vlastníka certifikátu (Subject)
  - Informace o veřejném klíči (Subject Public Key Info)

        * Algoritmus veřejného klíče (Public Key Algorithm)
        * Veřejný klíč certifikátu - většinou 1024 bitů (Public Key)
    - Volitelné součásti certifikátu:
        * Unikátní identifikátor certifikační autority
        * Unikátní identifikátor vlastníka certifikátu
        * Další rozšíření

- Algoritmus digitálního podpisu certifikátu (Certificate Signature Algorithm)
- Digitální podpis certifikátu (Certificate Signature)

Kromě těchto údajů mohou být v certifikátu obsaženy i další informace, jako je třeba omezení účelu použití certifikátu (například pokud je certifikát vydán pouze pro účely testování, není příliš důvěryhodný), cesta k certifikátům dané certifikační autority, cesta k seznamu zneplatněných certifikátů, atd.

Na obrázku 3.1 je zobrazen certifikát, na kterém jsou vidět základní údaje certifikovaného subjektu [6].

3.1.1 Struktura osobního certifikátu - příklad

Na následujícím příkladu je vidět struktura skutečného certifikátu standardu X.509 verze 3, v textové podobě. Tento certifikát jsem si vytvořil pro testovací účely u První certifikační autority a.s.

Certifikát používá ke kódování algoritmus RSA, společně s hashovací funkcí SHA-1. Platnost certifikátu je 14 dní a to od 9.4.2007 a času 12:39:38 do 23.4.2007 a času 12:39:38.

V rozšiřujících poznámkách jsou uvedeny ještě dodatečné informace o tom, že je certifikát určený pouze pro testovací účely, odkaz na seznam zneplatněných certifikátu První certifikační autority a.s. a možnosti použití certifikátu.

V závěru je mezi značkami BEGIN CERTIFICATE a END CERTIFICATE uveden certifikát v textovém formátu PEM.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 107666 (0x1a492)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CZ, CN=I.CA - Test CA, O=Prvni certifikacni autorita a.s.
        Validity
            Not Before: Apr  9 12:39:38 2007 GMT
```

```
        Not After : Apr 23 12:39:38 2007 GMT
    Subject: C=CZ, CN=Milan Tomasek/Email=xtomas09@stud.fit.vutbr.cz
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:c9:93:2c:98:42:d9:63:14:2a:2a:01:8f:c1:4e:
                fb:47:80:1e:69:9f:d2:14:70:6f:bd:98:bc:02:2e:
                06:a1:d4:53:85:fc:f2:b9:30:b7:cb:a0:1d:02:16:
                dc:3f:76:8a:43:11:73:0b:47:a6:76:5b:04:ce:10:
                ee:2c:61:4c:6c:a7:2b:15:66:83:98:d6:a8:08:ac:
                c9:04:7e:14:aa:c8:8f:dd:d3:90:b2:05:dc:55:3e:
                5b:27:0a:41:3d:b9:e7:02:c3:ec:5c:40:ca:51:17:
                f2:52:04:00:ad:c4:ca:d2:d1:a8:46:10:a6:02:26:
                75:93:38:2f:d2:76:0c:a9:31
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
        AB:77:3A:F0:A7:F4:1C:A6:B0:75:85:FE:F6:02:51:0D:08:6B:0B:CC
        X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.6625.1.1.3
          User Notice:
            Explicit Text: Jen pro TESTOVACI ucely.
            (Only for TESTING purposes.)

        X509v3 CRL Distribution Points:
        URI:http://ca.ica.cz/test_ica.crl

        X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment,
        Data Encipherment
Signature Algorithm: sha1WithRSAEncryption
    32:5b:c5:5b:f1:ad:0b:85:be:25:18:f1:2d:12:f3:28:71:93:
    e5:e0:20:6f:c6:ef:cb:6c:96:75:f5:cd:bc:68:08:6d:e9:fa:
    ba:3b:66:c4:5d:5b:e9:71:41:33:df:6c:f2:87:73:4b:7c:df:
    dd:58:5c:f3:8f:a7:19:e3:51:ae:c5:d3:46:5c:70:11:2b:e4:
    bb:86:1c:f3:fb:11:f2:7b:a7:5b:67:3a:70:66:d6:1f:73:4b:
    ba:3e:ea:47:84:a8:cf:a1:4f:02:2f:18:a2:89:ee:fd:5a:7f:
```

```
        cc:32:e7:b8:a4:95:08:c2:c8:be:49:e2:c3:c2:31:e6:10:ff:
        c2:a7:fc:41:25:28:96:bd:c8:12:d5:32:14:47:77:d6:e4:cf:
        0e:b2:b1:67:0e:5c:3a:0d:61:3b:e9:e8:dd:66:57:d7:ae:68:
        e8:56:c3:f7:3f:3a:0c:46:24:af:0c:e7:22:0f:75:cc:ea:19:
        2c:60:4e:19:3d:ce:3f:54:b2:3a:25:84:46:0d:f6:70:90:cc:
        c9:c2:39:62:91:f1:18:66:0d:5b:ac:eb:d4:bc:db:1a:9e:8f:
        88:db:3b:b9:ac:90:3f:83:fd:88:e7:12:25:82:73:6f:9f:1d:
        95:67:9b:17:4e:80:b3:9b:22:6a:a5:20:7e:0b:79:92:66:6b:
        7d:9b:68:30
-----BEGIN CERTIFICATE-----
MIIDTTCCAjWgAwIBAgIDAaSSMA0GCSqGSIb3DQEBBQUAMFExCzAJBgNVBAYTAkNa
MRcwFQYDVQQDEw5JLkNBIC0gVGVzdCBDQTEpMCcGA1UEChMgUHJ2bmkgY2VydGlm
aWthY25pIGF1dG9yaXRhIGEucy4wHhcNMDcwNDA5MTIzOTM4WhcNMDcwNDIzMTIz
OTM4WjBDMQswCQYDVQQGEwJDWjEUMBIGA1UEAxMLUGVwYSBUZXN0ZXIxHjAcBgkq
hkiG9w0BCQEWD21hamxvbkBlbWFpbC5jejCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAyZMsmELZYxQqKgGPwU77R4AeaZ/SFHBvvZi8Ai4GodRThfzyuTC3y6Ad
AhbcP3aKQxFzC0emdlsEzhDuLGFMbKcrFWaDmNaoCKzJBH4UqsiP3dOQsgXcVT5b
JwpBPbnnAsPsXEDKURfyUgQArcTK0tGoRhCmAiZ1kzgv0nYMqTECAwEAAaOBvzCB
vDAdBgNVHQ4EFgQUq3c68Kf0HKawdYX+9gJRDQhrC8wwXgYDVR0gBFcwVTBTBgor
BgEEAbNhAQEDMEUwQwYIKwYBBQUHAgIwNxo1SmVuIHBybyBURVNUT1ZBQ0kgdWNl
bHkuIChPbmx5IGZvciBURVNUSU5HIHB1cnBvc2VzLikwLgYDVR0fBCcwJTAjoCGg
H4YdaHR0cDovL2NhLmljYS5jei90ZXN0X2ljYS5jcmwwCwYDVR0PBAQDAgTwMA0G
CSqGSIb3DQEBBQUAA4IBAQAyW8Vb8a0Lhb4lGPEtEvMocZPl4CBvxu/LbJZ19c28
aAht6fq6O2bEXVvpcUEz32zyh3NLfN/dWFzzj6cZ41GuxdNGXHARK+S7hhzz+xHy
e6dbZzpwZtYfc0u6PupHhKjPoU8CLxiiie79Wn/MMue4pJUIwsi+SeLDwjHmEP/C
p/xBJSiWvcgS1TIUR3fW5M8OsrFnDlw6DWE76ejdZlfXrmjoVsP3PzoMRiSvDOci
D3XM6hksYE4ZPc4/VLI6JYRGDfZwkMzJwjlikfEYZg1brOvUvNsano+I2zu5rJA/
g/2I5xIlgnNvnx2VZ5sXToCzmyJqpSB+C3mSZmt9m2gw
-----END CERTIFICATE-----
```

3.1.2 Soubory standardu X.509

V rámci standardu X.509 jsou definovány následující typy souborů, obsahující jednotlivé informace:

- .cer - Certifikáty nebo sekvence certifikátů kódované pomocí CER (Canonical Encoding Rules).
- .der - Certifikáty kódované metodou DER (Distinguished Encoding Rules). V případě

formátu DER jsou data certifikátu uložena přímo v binární podobě.

- .pem - Certifikáty kódované pomocí base64. Jde v podstatě o binární data formátu DER převedená do textové podoby.
- .p7s - Elektronicky podepsaná data (neobsahující samotná data, pouze podpis).
- .pfx - Umístění veřejných a privátních objektů (klíčů) v jediném souboru, chráněném heslem.

3.2 Procesy certifikace, autentizace, integrity a validace

Aby bylo používání osobních certifikátů bezpečné a věrohodné, je potřeba dodržet jistá pravidla, jak při vydávání kvalifikovaných certifikátů (proces certifikace), tak při ověřování jeho platnosti (proces validace) a náležitosti ke konkrétní osobě (proces autentizace). Také je potřeba ověřit integritu přijatých a odeslaných dat, zda nedošlo v průběhu přenosu ke změně obsahu zprávy.

3.2.1 Certifikace

Mluvíme-li o certifikaci myslíme tím vydávání certifikátů uživatelům. Certifikát je dokument, který jednoznačně říká, že veřejný klíč na něm uvedený náleží ke konkrétní osobě. Navíc také certifikát obsahuje informace o době platnosti klíče, o jeho používání a o certifikační autoritě, kterou byl vydaný. Každý Certifikát je rovněž podepsán elektronickým podpisem příslušné certifikační autority.

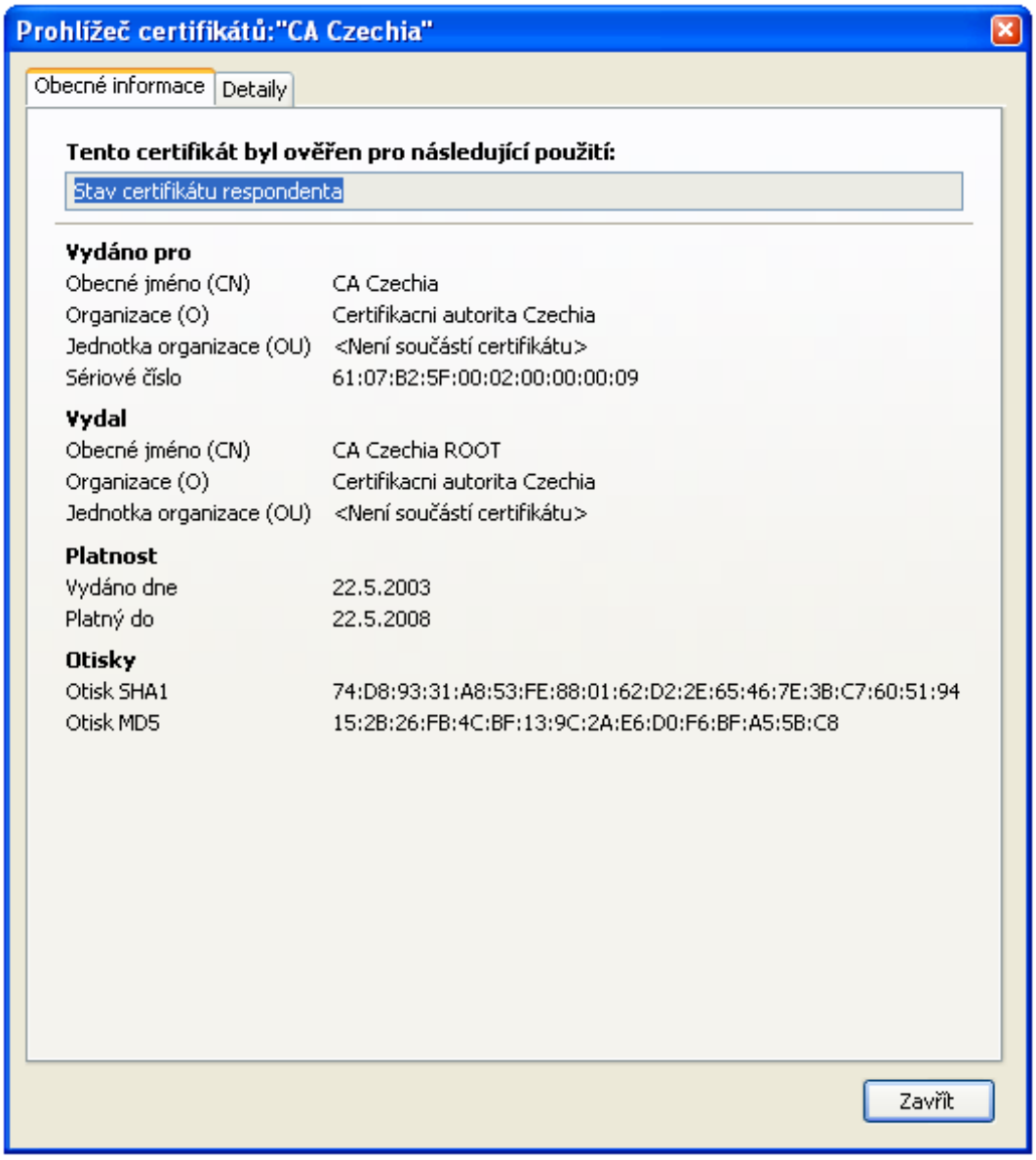
Podrobný popis procesu certifikace je popsán v bodě 3.4.

3.2.2 Autentizace

V případě doručení zprávy si příjemce po ověření elektronického podpisu také zjistí autentičnost veřejného klíče odesílatele ověřením podpisu certifikátu pomocí veřejného klíče certifikační autority (zda daný veřejný klíč opravdu náleží konkrétní osobě).

3.2.3 Integrita dat

Integrita dat zajišťuje, že nebyla odesílaná zpráva po zašifrování jakkoliv pozměněna, ať už záměrně (vlivem útoku třetí osoby) nebo neúmyslně (pokud došlo k chybě při přenosu dat). Aby byla integrita dat zajištěna, musí být vzorky získané rozšifrováním zašifrovaných dat (pomocí veřejného klíče) a zakódováním původní zprávy (pomocí hashovacího algoritmu) shodné.



Obrázek 3.1: Ukázka certifikátu certifikační autority Czechia

3.2.4 Validace

Proces validace se skládá z mnoha dílčích kroků a má za úkol rozhodnout zda je použitý certifikát, jímž byla zpráva podepsána, důvěryhodný a platný. Kontrola spočívá v ověření platnosti certifikátu, náležitosti ke konkrétní emailové adrese odesílatele, dále se kontroluje zda byl certifikát vydaný akreditovanou, popřípadě aspoň důvěryhodnou certifikační autoritou, účel pro který byl certifikát vydán, atd.

Aby mohla být zpráva prohlášena za regulérně podepsanou, je po ověření jejího odesílatele a CA nutné, aby se následně příjemce dotazoval na platnost certifikátu odesílatele.

Ověřování platnosti certifikátu je možné provádět dvěma způsoby:

- Ověřením u příslušné certifikační autority, zda se certifikát nachází v seznamech zneplatněných certifikátů CRL vydaných příslušnou certifikační autoritou.
- Druhá možnost je provedení on-line dotazu u poskytovatelů informací o stavu certifikátů, OCSP (On-line Certificate Status Provider), pomocí některého dotazovacího protokolu. Například OCSP (On-line Certificate Status Protocol, definovaný v RFC2560).

CRL (Certificate Revocation List)

Jde o seznam zneplatněných certifikátů, které již dále nemohou být akceptovány jako důvěryhodné při elektronické komunikaci. CRL se může vyskytovat ve dvojí podobě. Jednak je vydáván kompletní seznam, obsahující všechny zneplatněné certifikáty, ten je pravidelně doplňován tzv. ΔCRL (rozdílový seznam), ve kterém se objevují změny od vydání posledního kompletního CRL. Každý certifikát, figurující na seznamu CRL, se může vyskytovat v jednom ze dvou následujících stavů:

1. **Zrušení certifikátu**

   Ke zrušení certifikátu (certificate revoked) dochází tehdy, pokud byl kompromitován privátní klíč vlastníka certifikátu nebo existuje důvodné podezření jeho zneužití (což je pravděpodobně nejčastější případ). Druhým, neméně závažným důvodem pro zrušení platnosti je porušení požadavků na bezpečnost ze strany certifikační autority. Ke zneplatnění certifikátu může dojít také tehdy, je-li vystaven namísto něj certifikát nový (například z důvodu aktualizace informací v certifikátu).

2. **Pozastavení platnosti certifikátu**

   Narozdíl od úplného zrušení platnosti certifikátu, kdy se jedná o nevratný proces, jde v tomto případě pouze o dočasné přerušení možností jeho požívání (certificate hold). K tomuto kroku se přistupuje v případech, kdy majitel například ztratil svůj privátní klíč. Po opětovném nalezení je certifikát ze seznamu CRL opět odstraněn (pouze v případě, že nemohl být zneužit).

Povinností každého příjemce elektronicky podepsané zprávy je ověřit si, zda-li se certifikát odesílatele nenachází v seznamu CRL. V případě, že by byl certifikát (respektive jeho sériové číslo) uveden v CRL, mělo by se se zprávou nadále zacházet jako s nepodepsanou [8].

Problémy s CRL

Mezi hlavní problémy vznikající v souvislosti se zneplatněním certifikátů patří doba, která uběhla mezi obdržením požadavku na zneplatnění certifikátu a vydáním aktuální verze CRL. Po tuto dobu se příslušný certifikát stále chybně jeví jako platný. Vhodným řešením je častější vydávání delta Δ CRL.

Dalším problémem je samotná velikost CRL. Pro snížení nároků na přístup a zpracování CRL, mohou být seznamy vedeny jako více samostatných seznamů (CRL šifrovacích certifikátů, neplatných atributových certifikátů, identifikačních certifikátů). Certifikační autorita má možnost také uveřejnit dílčí CRL konkrétní organizace, označované jako Redirected CRLs.

3.3 Certifikační autorita

Jedná se o nezávislou důvěryhodnou organizaci (v zákoně 227/2000 Sb. o elektronickém podpisu se nazývá poskytovatel certifikačních služeb), která má legitimitu k vydávání kvalifikovaných certifikátů. Obecně certifikační autorita spadá do skupiny důvěryhodných subjektů poskytujících služby označovaných jako TSP (Trusted Service Provider).

Vydáním certifikátu certifikační autorita stvrzuje, že subjekt, kterému byl certifikát vydán, skutečně vlastní daný pár klíčů.

Kromě toho, že certifikační autorita má oprávnění k vydávání a správě certifikátů, plní další neméně důležitou činnost, kterou je udržování a zveřejňování tzv. seznamu zneplatněných certifikátů CRL.

Záleží na každém zájemci o certifikát, kterou certifikační autoritu zvolí. Roli hraje typ požadovaného certifikátu a samozřejmě také důvěryhodnost té či oné certifikační autority [5].

Mezi akreditované certifikační autority patří:

- První certifikační autorita, a.s. - oprávnění k vydávání kvalifikovaných certifikátů, vydávání kvalifikovaných systémových certifikátů a vydávání kvalifikovaných časových razítek.
- CA eIdentity a.s - oprávnění k vydávání kvalifikovaných certifikátů a vydávání kvalifikovaných systémových certifikátů.

- CA Česká pošta, s.p. - oprávnění k vydávání kvalifikovaných certifikátů a vydávání kvalifikovaných systémových certifikátů.

3.4 Vytvoření osobního certifikátu

Jak jsem se již zmínil, certifikáty přiděluje certifikační autorita. Při vytváření nového certifikátu si musí žadatel nejdříve vygenerovat dvojici klíčů (veřejného a privátního), což je možné na internetových stránkách zvolené certifikační autority. Po vygenerování obou klíčů je ještě potřeba, aby uživatel v žádosti o přidělení certifikátu vyplnil veškeré požadované identifikační údaje. Tato zpráva je následně podepsaná právě vygenerovaným privátním klíčem a odeslána příslušné certifikační autoritě. Certifikační autorita ma pak povinnost ověřit si pravdivost uvedených informací a to osobně překontrolováním všech údajů pomocí dokladu totožnosti žadatele. Pokud je vše v pořádku, vystaví certifikační autorita kvalifikovaný certifikát, který následně podepíše svým privátním klíčem. Nakonec je žadateli certifikát předán, buď na datovém nosiči nebo zaslán elektronickou poštou.

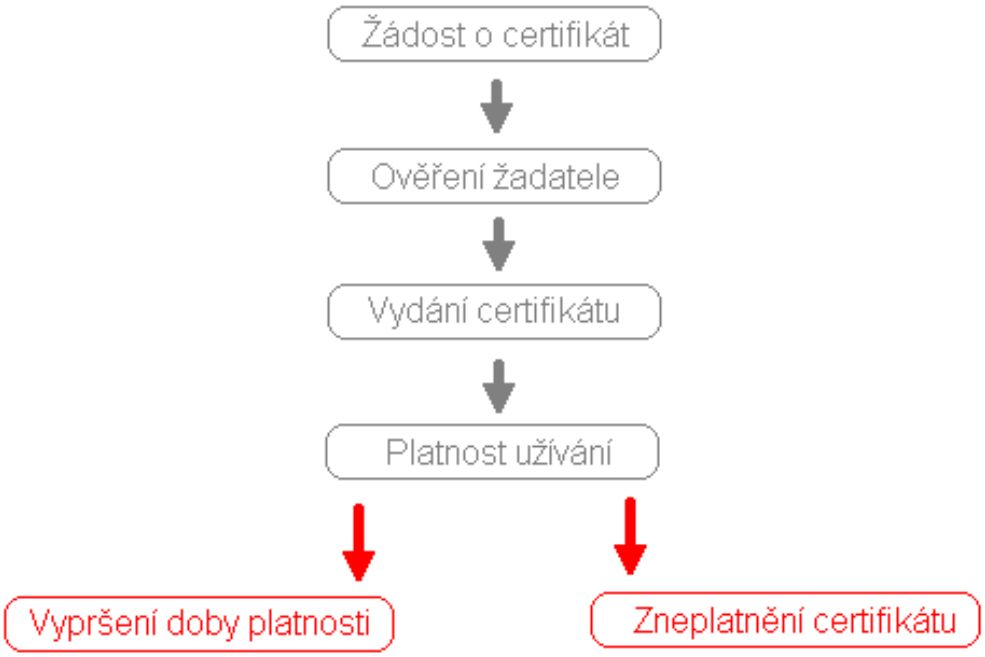
3.5 Životní cyklus certifikátu

Každý certifikát prochází třemi základními fázemi vývoje. V první fázi dochází ze strany uživatele k žádosti o vytvoření osobního certifikátu, je vygenerována dvojice klíčů (veřejný a privátní) a následně je ověřena platnost informací poskytnutých žadatelem. V závěru první fáze je certifikát vytvořen a předán uživateli.

Ve druhé fázi, která by se dala označit jako fáze platnosti certifikátu, je možné jej používat k účelům, pro které byl vystaven.

Poslední fází v životním cyklu certifikátu je jeho zrušení, kdy certifikát pozbývá platnosti. To je možné řešit dvěma způsoby. Certifikát může být zrušen buď z důvodu vypršení svojí doby platnosti nebo umístěním na seznam zneplatněných certifikátů.

Životní cyklus certifikátu je znázorněn na obrázku 3.2.



Obrázek 3.2: Životní cyklus certifikátu

Kapitola 4

Elektronické podatelny

V této kapitole se budu zabývat komerčně dostupnými elektronickými podatelnami, jež jsou využívány státními úřady. Ty mají dle nařízení vlády z roku 2001 povinnost poskytnout občanům možnost podávat datové zásilky v elektronické podobě. Dále se zaměřím na některé další subjekty poskytující svým partnerům tuto formu komunikace.

Elektronické podatelny (hlavně co se týče orgánů státní správy) by se měly řídit určitými standardy, které definují pravidla pro jejich provoz a funkce.

Schéma elektronické podatelny je znázorněno na obrázku 4.1.

4.1 Funkce elektronické podatelny

Jsou obdobou klasické podatelny a slouží jako prostředek ke komunikaci uživatelů a různých institucí elektronickou formou. Nespornou výhodou je možnost odesílat zprávy v kteroukoliv denní i noční hodinu.

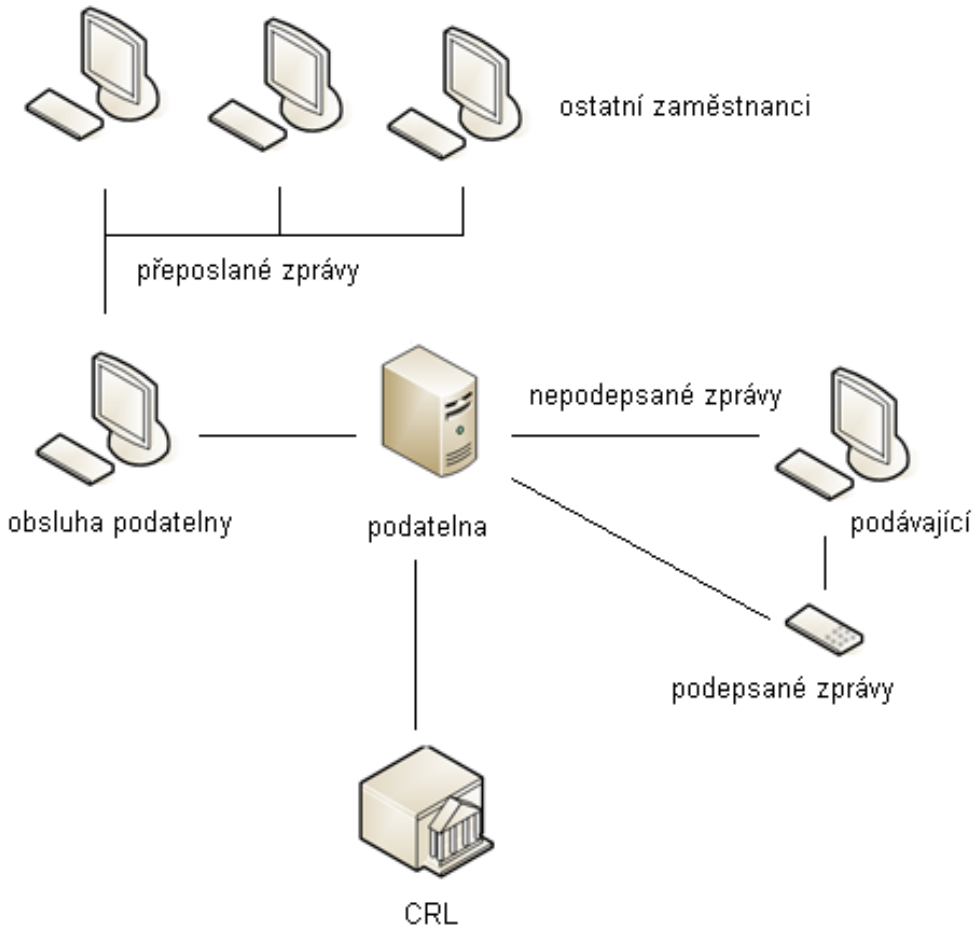
Komunikace probíhá pomocí datových zpráv opatřených elektronickým podpisem, vytvořeným pomocí kvalifikovaného certifikátu odesílatele. Kompetentní zaměstnanec provozovatele elektronické podatelny (instituce), který je rovněž vybaven kvalifikovaným certifikátem, přebírá příchozí zprávy, ověřuje platnost elektronického podpisu, rozesílá zprávy k vyřízení příslušným adresátům a podává odesílateli informaci o jejich přijetí.

Další možností je uskutečnit podání bez elektronického podpisu pouze přes rozhraní podatelny.

Funkce vyžadované od elektronické podatelny by se tedy daly shrnout do několika následujících bodů [4].

4.1.1 Provedení podání

Podání je zpravidla možné realizovat pomocí emailu, přes www rozhraní, osobně nebo posláním podporovaného datového nosiče na podatelnu. Příslušný pracovník podatelny je



Obrázek 4.1: Schéma elektronické podatelny

zodpovědný za převzetí zprávy a předání adresátovi, popřípadě ji sám vyřídí nebo vymaže, uzná-li za vhodné.

4.1.2 Potvrzení o přijetí podání

Po odeslání podání je odesílateli zasláno potvrzení o přijetí. Potvrzující zpráva by měla obsahovat jednak potvrzení o přijetí, dále pak unikátní identifikační číslo podání a termín nejpozdějšího vyřízení podání. Nedílnou součástí je i elektronický podpis pracovníka podatelny, popřípadě vyřizující osoby.

4.1.3 Kontrola elektronického podpisu a příloh (pokud existují)

Je-li podání podepsáno elektronickým podpisem, je nutné provést jeho kontrolu. Tato kontrola spočívá v ověření správnosti podpisu na základě certifikátu a dále v kontrole, zda jde o kvalifikovaný certifikát, čili certifikát vydaný akreditovanou certifikační autoritou. Pokud by byly zjištěny nedostatky, mělo by se se zprávou nakládat jako by byla nepodepsaná.

Jsou-li ke zprávě přiloženy soubory nepovoleného formátu (např. spustitelné aplikace), měly by být tyto přílohy odmítnuty.

4.1.4 Zpracování podané zprávy

Zaměstnanec podatelny přijímající příchozí podání má několik možností jak se zprávou naložit:

- Předat zprávu k řešení příslušnému adresátovi, který ji vyřídí.
- Odpovědět, pokud je povaha podání taková, že jej je možné vyřídit přímo zaměstnancem podatelny (např. žádosti o zaslání dokumentů, poskytnutí informace, stížnosti, podněty, oznámení).
- Vymazat, je-li zpráva vyhodnocena jako nežádoucí pošta SPAM

4.1.5 Kontrola stavu podané zprávy

Podávající by měl mít kdykoli možnost přes webové rozhraní podatelny zjistit stav svého podání na základě jednoznačného identifikátoru. Zpráva může být například ve stavu řešená, vyřízená nebo smazaná.

4.1.6 Vyřízení podané zprávy

Přijatá zpráva je zaměstnancem podatelny předána k vyřízení adresátovi. V okamžiku předání začíná běžet lhůta, v rámci které je očekávána odpověď od vyřizující strany. Kompetentní osoba vyřídí podání a podepíše svým elektronickým podpisem vytvořeným na základě kvalifikovaného certifikátu. Vyřízená zpráva (včetně případných příloh) je poté bez dalšího zásahu zaměstnance podatelny odeslána podávající osobě.

4.1.7 Archivace podání

Veškeré informace elektronické podatelny by mělo být možné archivovat pro případ pozdějšího dohledání přijatých podání nebo obnovy dat.

4.2 Porovnání vybraných elektronických podatelen

Z velkého množství dostupných systémů elektronických podatelen jsem vybral následující zástupce, kteří poskytují službu elektronické podatelny pro různé státní instituce jako jsou ministerstva, úřady, města, městské části, atd. Tyto orgány státní správy jsou dle zákona povinné občanům poskytovat možnost podání v elektronické podobě.

4.2.1 podatelna.info

- **Uskutečnění podání, potvrzení.**

  Podání lze uskutečnit emailem, osobně nebo pomocí datového nosiče.

  Po odeslání podání emailem nebo pomocí formuláře je odesílateli doručena zpráva o přijetí podání systémem.

  Uživateli je zaslána potvrzující zpráva, která obsahuje identifikační číslo podání (PID), datum dokdy bude podání nejpozději vyřízeno a je podepsána elektronickým podpisem úředníka, přijímajícího podání.

- **Elektronický podpis a přílohy**

  Pokud je podání elektronicky podepsáno, provede se kontrola, zda je podpis korektní a je-li certifikát vystavený některou z akreditovaných certifikačních autorit. Jestli ne, zachází se zprávou jako s nepodepsanou.

  Obsahuje-li zpráva připojenou přílohu a soubor v této příloze je jiného typu než je akceptovaný, je odmítnut a odesílatel je o tomto informován.

  Systém podatelna.info je vybaven antivirovým software Kaspersky Lab. Při zjištění přítomnosti viru je zpráva vyřazena.

- **Přijetí podání a vyřízení podání.**

  Každému podání je přiřazeno jednoznačné identifikační číslo (PID)

  Operátor podatelny rozhodne zda podání předá k vyřízení (stav řešená), sám na něj odpoví (stav vyřízená) nebo jej vymaže, například v případě SPAMu (stav smazaná).

  Operátor má k dispozici tzv. FAQ databázi nejčastějších otázek a k nim připravených odpovědí.

- **Kontrola stavu podání**

  Podávající má možnost zjistit stav svého podání na internetových stránkách úřadu, pomocí adresy ze které bylo podání posláno a identifikátoru PID.

- **Vyřízení podání**

Zákonná lhůta na vyřízení podání je v případě veřejných úřadů 30 dnů. Zpráva je podepsána elektronickým podpisem vyřizující osoby a odeslaná podávajícímu.

- **Archivace dat**

  Data elektronické podatelny jsou archivována po dobu 5 let. Jsou uložena v databázi PostGresSQL a zajištěna proti poškození prostřednictvím diskového pole RAID5.

- **Funkce administrátora podatelny**

  Administrátor podatelny má možnost provádět veškeré změny v podatelně. Pro jednoduchost uvedu jen několik málo pravomocí, kterými disponuje administrátor systému podatelna.info.

  Vytvoření a editace uživatelů podatelny, editace automatických odpovědí, vytvoření a editace uživatelských odpovědí, varovná hlášení, nastavení podporovaných příloh, změna stavu podání a další [10].

4.2.2 Mail602 ePodatelna

Jde o jednoduché řešení elektronické podatelny od společnosti Software 602. Nevýhodou Mail602 ePodatelny je absence funkce obecné spisovny a dokument flow. Není proto vhodná pro přijímání velkého množství elektronických podání.

- **Práce s elektronickým podpisem**

  Mail602 ePodatelna zajišťuje identifikaci elektronicky podepsaných zásilek, zobrazení certifikátů a umožňuje tak i ověření elektronického podpisu na webové stránce příslušné certifikační autority. Ověření zda nebyl elektronický podpis zneplatnění se provádí na stránkách I.CA.

- **Antivirová a antispamová ochrana**

  Součástí Mail602 ePodatelna je vestavěný antivirový systém BitDefender^{TM} pro centrální kontrolu elektronické pošty. Ochranu před nevyžádanými zásilkami (spamy) zajišťuje filtr, který analyzuje obsah všech přijatých zpráv.

- **Archivace podání**

  Automatická archivace veškeré přijaté i odeslané pošty je v centrálním archivu (obsah je šifrován a zároveň komprimován). Uživatel systému nemá žádnou možnost zásilku v archivu modifikovat ani odstranit.

- **Postoupení elektronických podání**

  Mail602 ePodatelna umožňuje postoupit elektronické podání odpovědné osobě.

- **Odeslání oznámení o doručení**

  Potvrzení o přijetí elektronického podání je řešeno pomocí automatické odpovědi, zaslané podávajícímu.

- **Faxování**

  Součástí řešení od Software 602 je i možnost odesílání a příjmu faxů [11].

4.2.3 Podatelna spol. ICZ

- **Rozhraní pro klienty**

  zajišťuje elektronický podpis dat odesílaných ve www formuláři a také elektronický podpis libovolného souboru určeného k odeslání na internetový server elektronické podatelny.

  Dále je podporováno vytváření a přijímání XML formulářů pomocí aplikace FormFiller, které jsou potom ověřovány na serveru.

- **Serverová sekce**

  zajišťuje kontrolu integrity dat a ověření elektronického podpisu. Podporováno je jak uložení elektronického podpisu v textovém formátu, tak společně s daty v XML nebo kryptograficky zašifrovaném formátu CMS [12].

4.2.4 TrustPort ePodatelna

Jedná se o elektronickou podatelnu od společnosti AEC, která existuje pod označením TrustPort ® ePodatelna. Podatelna podporuje elektronická podání pomocí předdefinovaných formulářů.

- **Uskutečnění a kontrola stavu podání.**

  Provést podání a kontrolovat stav jeho vyřízení je podávajícímu umožněn po přihlášení do systému podatelny (nutná předchozí registrace). Elektronickou podatelnu může využívat i nepřihlášený uživatel, avšak bez možnosti kontrolovat stav svých podání.

- **Registrace podávajícího.**

  Při registraci je vložen kvalifikovaný certifikát uživatele do systému ePodatelny. Díky tomu je kromě použití jména a hesla možné přihlásit se do systému také pomocí osobního certifikátu.

- **Elektronický podpis podání.**

  Podávající může podepsat podání buďto v přiloženém souboru nebo přímo v textu zprávy, popřípadě odeslat podání v podobě podepsané přílohy nepodepsané zprávy.

- **Kontrola elektronického podpisu a vyřízení podání.**

  V případě doručení nepodepsaného podání je odesílatel upozorněn na nutnost odeslat podání znovu. Podatelna tudíž nepodporuje podání, která nejsou opatřena elektronickým podpisem.

  Po přijetí podepsaného podání provedena kontrola elektronického podpisu. Při problému (porušení, neplatnost, atd.) s elektronickým podpisem je odesílatel o této skutečnosti vyrozuměn. Pokud je elektronický podpis v pořádku, dojde k jejímu vyřízení (v zákonné lhůtě 30 dnů).

- **Administrátorská sekce**

  Obdobně, jako je tomu ve většině systémů, existuje i v tomto případě správce podatelny, který je kompetentní provádět veškeré změny a nastavení [13].

4.2.5 Post Office Elektronická podatelna

V tomto případě je podatelna součástí většího programového balíku Post Office, sloužícího pro evidenci práce se zásilkami.

Elektronická podatelna slouží jako prostředek pro evidenci elektronických zásilek.

Funkce elektronické podatelny Post Office:

- Příjem šifrovaných emailových zpráv pomocí kryptografických algoritmů.
- Příjem REP (registrovaná elektronická pošta) zpráv. Jde o šifrovaný a elektronicky podepsaný přenos využívaný Českou poštou, kdy je také automaticky vytvořeno potvrzení o převzetí informací příjemcem.
- Automatické třídění zásilek přijatých od klientů.
- Ověření elektronického podpisu na základě platného osobního certifikátu vydaného akreditovanou certifikační autoritou.
- Automatické zasílání potvrzení přijetí elektronické zásilky (doručenky).
- Správa akceptovaných typů certifikátů a certifikačních autorit [14].

4.2.6 TOPSPIN EPodatelna

Jedná se o další z řešení elektronické podatelny pro orgány veřejné správy. Informace k tomuto produktu je možné vyčíst jedině z referencí odkazujících na příslušné úřady využívající tento systém [15].

4.2.7 Shrnutí

Vzhledem ke stále vzrůstajícímu podílu elektronické komunikace a právním normám přikazujícím provozovat elektronickou podatelnu státním institucím je na českém trhu velké množství společností, zabývajících se touto problematikou.

Všechny prozkoumané systémy, umožňující uskutečnit elektronické podání, poskytují až na drobné odlišnosti v zásadě stejné funkce, plynoucí z požadavků na elektronickou podatelnu. Některé aplikace navíc nabízejí zajímavá rozšíření v možnosti přijímat XML formuláře, faxy, či využít databázi nejčastěji kladených dotazů (FAQ).

Kapitola 5

Návrh elektronické podatelny pro VUT

5.1 Specifikace požadavků na elektronickou podatelnu VUT

Pro návrh elektronické podatelny je nejdříve potřeba si uvědomit požadavky a funkce, které by měl systém splňovat.

Celá podatelna bude rozdělena do dvou částí:

1. Klientská část
2. Zaměstnanecká část

Vzhledem k tomu, že budeme celý systém projektovat ve dvoučlenném týmu, zaměřím se ve své práci na klientskou část a můj kolega na sekci pro zaměstnance VUT.

Rozhraní pro klienty by mělo umožňovat dva druhy elektronického podání. Jednak by klienti měli mít možnost uskutečnit podání elektronicky podepsané na základě kvalifikovaného certifikátu a také podání bez elektronického podpisu, s využitím formuláře na internetových stránkách podatelny.

K oběma variantám podání by mělo být možné připojit přílohy (typy akceptovaných příloh budou ještě otázkou diskuse).

Pomocí www rozhraní by také měli mít registrovaní klienti možnost sledovat stav svého podání, zda je ve fázi přijato, vyřizováno, vyřízeno, či smazáno. To by bylo možné realizovat na základě přiděleného identifikátoru podání a uživatelského hesla.

Veškerá podání budou zasílána na jednu centrální adresu, odkud budou zaměstnancem podatelny distribuována jednotlivým adresátům, popřípadě přímo vyřízena zaměstnancem, bude-li tomu povaha podání odpovídat.

5.2 Návrh funkcí elektronické podatelny VUT

Po prostudování funkcí poskytovaných ostatními systémy elektronických podatelen a po analýze požadavků jsem sestavil následující přehled funkcí, které by měla vytvořená elektronická podatelna poskytovat.

- Provedení podání buďto za použití elektronického podpisu nebo bez podpisu.
- Potvrzení o přijetí elektronického podání na podatelnu.
- Kontrola stavu podepsaných podání ze strany odesílatele na základě přijatého identifikátoru podání a uživatelského hesla.
- Kontrola platnosti osobního certifikátu podávajícího a správnosti elektronického podpisu (pokud existuje).
- Přijetí a předání, popřípadě vyřízení podání zaměstnancem podatelny.
- Vyřízení podání adresovaným zaměstnancem VUT.
- Změna stavu podání ze strany obsluhy podatelny nebo zaměstnance VUT.
- Vymazání podání odhalených jako nežádoucí pošta (SPAM).
- Záloha přijatých podání.
- Obnova zálohovaných dat.

5.3 Implementace do portálu VUT

Elektronická podatelna vytvořená v rámci této práce by měla být implementovatelná do portálu VUT v Brně. Z tohoto důvodu budu volit grafické rozhraní aplikace tak, aby zapadalo do již zavedeného a fungujícího systému.

Dále bude potřeba vytvořit na poštovním serveru VUT emailovou schránku, sloužící pro příchozí podání a také založit nový účet v databázi Oracle, která bude sloužit coby úložiště informací získaných z příchozích zpráv.

5.4 ER diagram objektů podatelny

Na obrázku 5.1 je znázorněn návrh logické struktury elektronické podatelny.

V podatelně jsou evidována podání jak elektronicky podepsaná, tak bez elektronického podpisu s atributy ID (jednoznačný identifikátor), adresát podání, datum uskutečnění podání předmět podání, samotný text zprávy a pokud existuje tak také příloha (popřípadě seznam příloh) akceptovaná podatelnou. U podepsaných podání, která smí provádět pouze

uživatel s platným kvalifikovaným certifikátem, jsou oproti nepodepsaným zprávám položky obsahující informace o elektronickém podpisu. V případě nepodepsaných podání je naopak vyžadován atribut obsahující email odesílatele.

Zaměstnanec podatelny (chápáno jako osoba mající přístup k centrální schránce, na kterou jsou podání doručována) a ostatní zaměstnanci VUT jsou jednoznačně identifikovatelní na základě osobního ID (loginu), z dalších údajů jsou v systému uchovávány informace o jméně, příjmení, emailu, osobním certifikátu, fakultě, ústavu jednotlivých zaměstnanců a případně činnost nebo funkce, kterou v rámci VUT zastávají.

5.5 Use Case diagram uživatelů podatelny

Funkce jednotlivých uživatelů podatelny, ať už na straně klientské nebo na straně zaměstnanců jsou názorně zobrazeny pomocí tzv. Use Case diagramu (diagram případu užití) na obrázku 5.2.

Uživatelé elektronické podatelny by se dali rozdělit do tří skupin:

- **Klienti elektronické podatelny**, uskutečňující podání, kteří se dále dělí na autorizované a neautorizované uživatele. Autorizovaní uživatelé, vlastnící osobní certifikát, mají možnost provádět elektronicky podepsaná podání a následně kontrolovat jejich stav. Ostatní klienti mají možnost provádět pouze zjednodušenou formu podání, které nevyžaduje ověření elektronickým podpisem a má zpravidla podobu dotazu, návrhu, či připomínky.

- **Zaměstnanci VUT vyřizující podání** se dělí také do dvou skupin.

  První skupinou jsou osoby přijímající podání z centrální schránky podatelny a na základě jeho povahy jej buďto sami vyřídí, přepošlou příslušnému adresátovi nebo odstraní, vyhodnotí-li podání jako SPAM.

  Druhou skupinou jsou všichni ostatní zaměstnanci s možností vyřizovat příchozí podání.

  Všichni zaměstnanci mají také možnost nastavovat stav podání, v závislosti na stádiu jeho vyřizování (přijato, vyřizováno, vyřízeno, smazáno).

- **Administrátor podatelny** je osoba, která je oprávněna ke všem změnám v systému, jako je vkládání, editace a mazání všech údajů, zálohování dat, obnova informací ze zálohy a také odstranění jednotlivých bodů obnovy.

5.6 Návrh databáze

Na základě ER diagramu by se mohla výsledná databáze skládat ze tří tabulek. V první by byly uchovávány informace o přijatých podání, jejich stavu, atd. Ve druhé tabulce budou

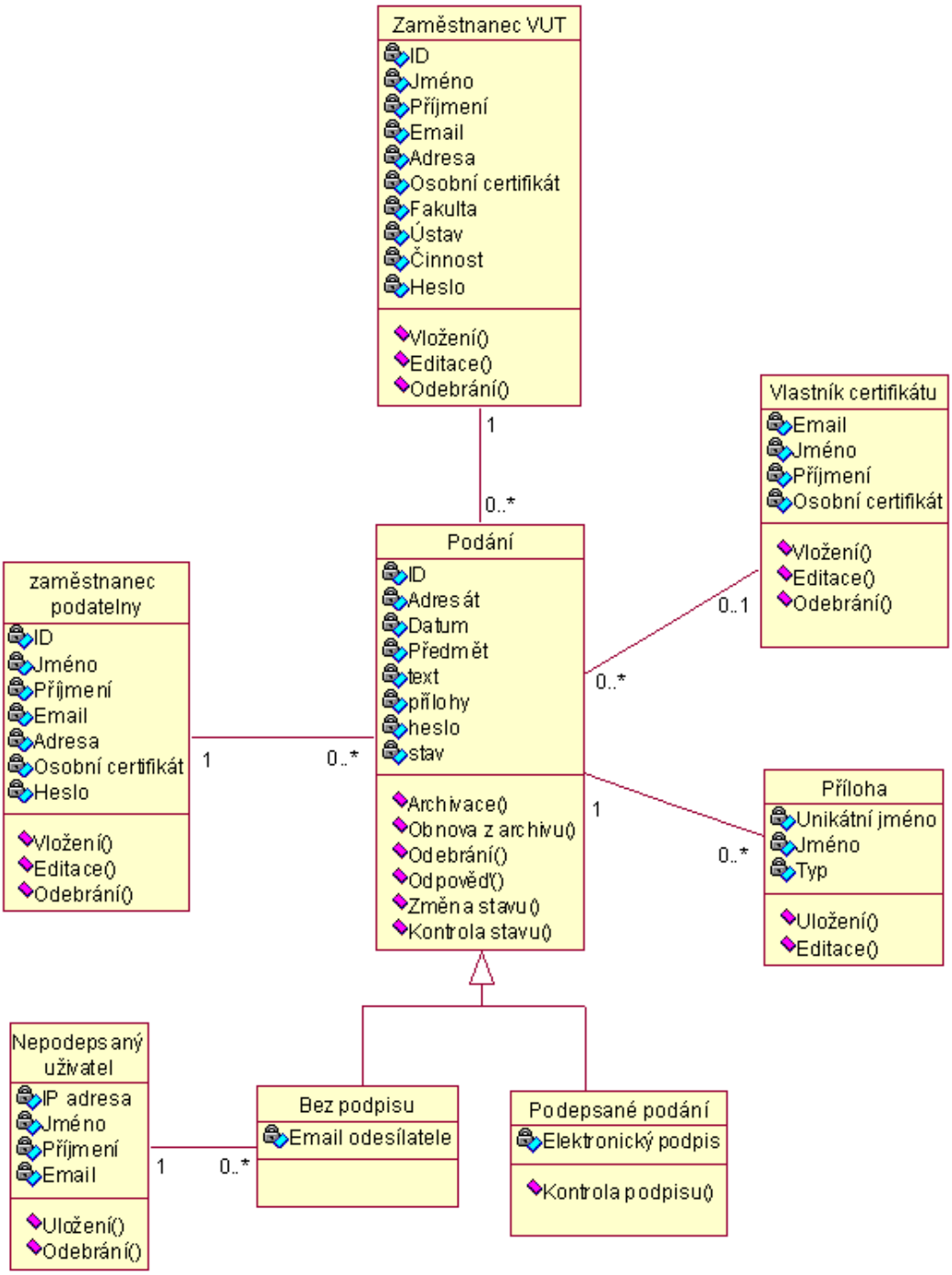
informace o případných přílohách přijatých zpráv, a v poslední tabulce se budou vyskytovat údaje o zaměstnancích VUT a dalších osob oprávněných k obsluze podatelny.

Vzhledem k faktu, že bude podatelna začleněna do již existujícího systém, není nutné se zabývat tvorbou poslední tabulky, jelikož jsou již potřebné informace v databázi uloženy pro potřeby ostatních aplikací.

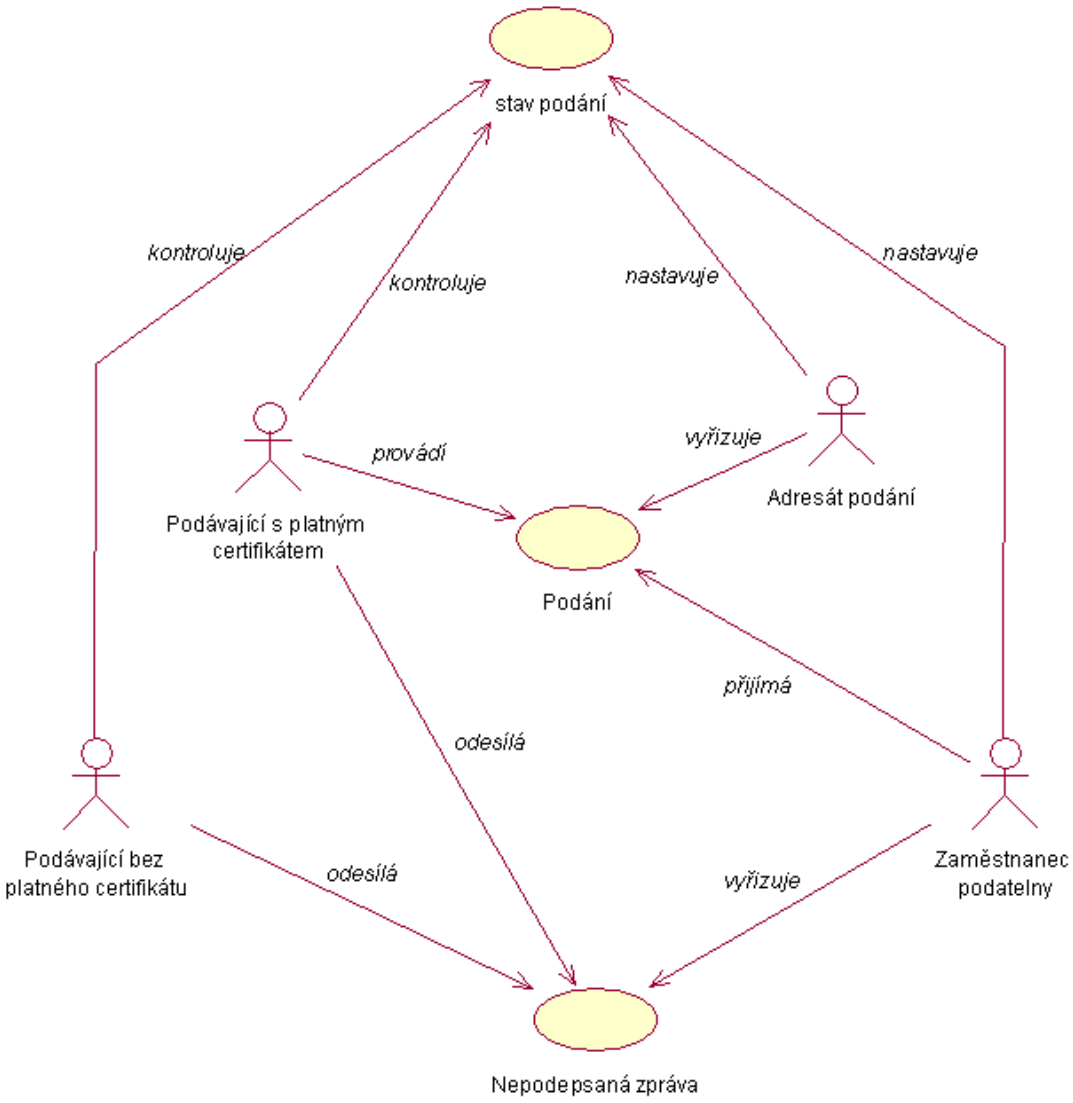
5.7 Způsob implementace do portálu VUT

Elektronická podatelna vytvořená v rámci této práce by měla být implementovatelná do portálu VUT. Z tohoto důvodu budu volit grafické rozhraní aplikace tak, aby zapadalo do již zavedeného a fungujícího systému.

Dále bude potřeba na serveru VUT vytvořit emailovou schránku, sloužící pro příchozí podání a také vytvořit novou databázi pro uchovávání informací získaných z příchozích zpráv a informací o uživatelích.



Obrázek 5.1: ER diagram objektů podatelny



Obrázek 5.2: Use Case diagram uživatelů podatelny

Kapitola 6

Realizace elektronické podatelny

V této kapitole rozeberu implementaci elektronické podatelny z pohledu vývoje a funkčních náležitostí, specifikovaných ve fázi návrhu a interakce s uživatelem.

6.1 Vývojové prostředí

Elektronická podatelna je vytvořena jako webová aplikace na portálu VUT. Celý program je podle zadání vytvořen ve skriptovacím jazyce PHP [18], implementovaném do HTML kódu. Práce s daty uloženými v databázi Oracle je řešena pomocí dotazovacího jazyka SQL. Dalšími technologiemi, které jsem při tvorbě elektronické podatelny využil jsou XML, CSS a javascript. K databázi (CISB_CISB.RO.VUTBR.CZ) jsem se připojoval pomocí programu PL/SQL Developer, spouštěného prostřednictvím vzdálené plochy na adrese lemur2.ro.vutbr.cz.

Parametry využívaného školního software:

- PHP version 4.3.2
- Oracle Database 10g Release 10.2.0.3.0
- OCI version 9.2 (Oracle Call Interface)
- PL/SQL Developer version 6.0.5.931

6.2 Grafické rozhraní

Grafické rozhraní elektronické podatelny se skládá ze dvou na sobě nesouvisejících částí.

1. Uživatelské rozhraní - Jedná se o tu část elektronické podatelny, se kterou přichází do styku uživatelé podatelny při uskutečnění podání, popřípadě při kontrole stavu svých již uskutečněných podání.

2. Interní rozhraní - Jde o část, se kterou pracují zaměstnanci podatelny při vyřizování, editování nebo přeposílání přijatých podání.

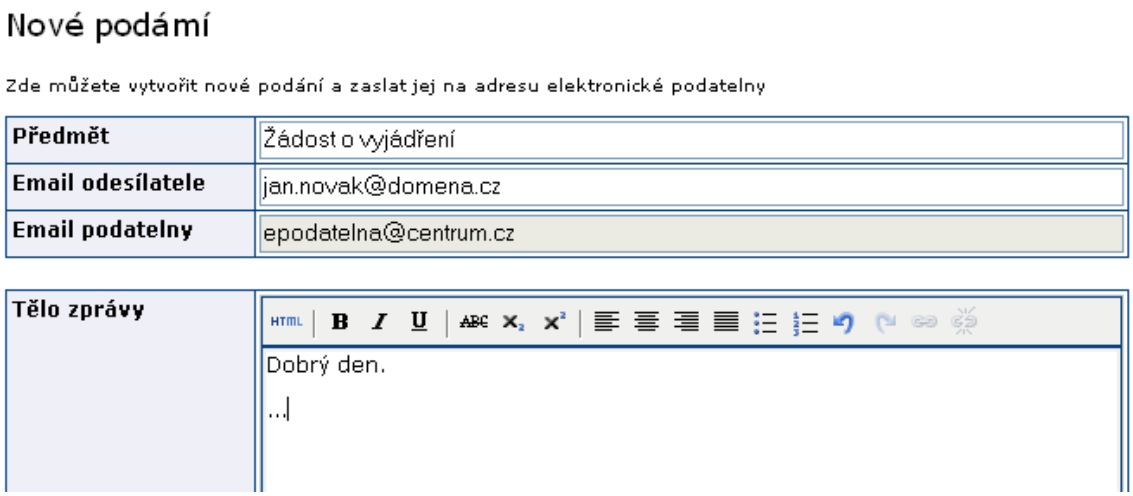
6.2.1 Uživatelské rozhraní

Uživatelské rozhraní sestává z formuláře pro odesílání nepodepsaných podání, sekce pro ověřování stavu podání (obr. 6.2) a odkazu na emailovou adresu podatelny, pokud si přeje uživatel uskutečnit podání s elektronickým podpisem pomocí svého emailového klienta (obr. 6.1).

Rozhodne-li se uživatel provést podání přímo přes uživatelské rozhraní podatelny (čili bez elektronického podpisu), je nutné vyplnit emailovou adresu, na kterou má být doručena případná odpověď. Pokud tak podávající neučiní nebo uvede chybnou adresu, nemůže bohužel očekávat žádnou odpověď ze strany obsluhy podatelny, popřípadě konkrétního adresáta zprávy.

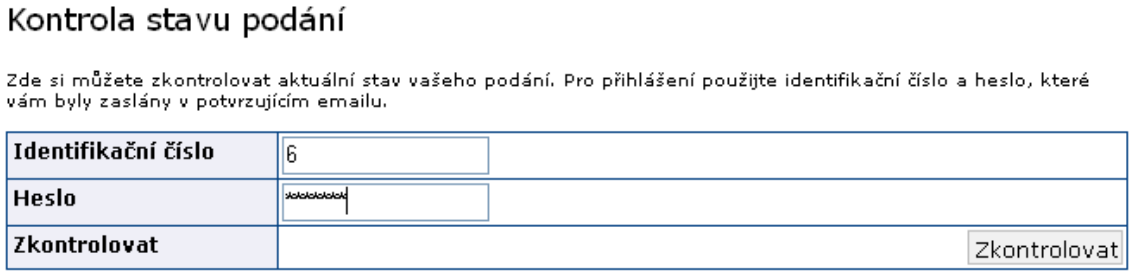
V textové oblasti je možné vytvořit požadovanou zprávu, ke které lze přiložit datový soubor. Pomocí rozšířených nástrojů pro sazbu textu může být výsledná zpráva lépe a přehledněji strukturována.[1] Maximální velikost takto vložené přílohy nesmí překročit 2 MB. Bližší informace o povoleném formátu příloh připojených k podání jsou popsány v sekci 6.5.3.

Rozhraní pro kontrolu stavu podání sestává ze dvou polí, do kterých je zadáváno identifikační číslo podání a heslo. Tyto informace jsou uživateli doručeny na jeho emailovou adresu ihned po přijetí podání podatelnou.



Obrázek 6.1: Rozhraní pro provedení podání ze stránek podatelny

[1] Nástroje pro sazbu textu, které jsem použil ve svém grafickém rozhraní, byly již dříve vytvořeny pro jinou aplikaci na portálu VUT.



Obrázek 6.2: Kontrola stavu podání

6.2.2 Interní rozhraní

V mojí části aplikace jsem vytvářel uživatelské rozhraní a jednotlivé moduly pro práci s příchozími zprávami a databází. Interní rozhraní v rámci své práce zpracoval můj kolega Martin Beran.

6.3 Struktura databáze

Databáze je tvořena tabulkou *mail*, obsahující informace o příchozích emailech a *attachment*, ve které jsou uloženy informace o případných přílohách, připojených k emailu.

Pokud je zpráva elektronicky podepsána, nachází se v tabulce *attachment* také informace o souboru s elektronickým podpisem, jelikož tento soubor je k emailu přikládán jako příloha ve speciálním, normou definovaném formátu.

6.3.1 Struktura tabulky *mail*

Tabulka *mail* obsahuje informace z hlavičky emailu, odkazy na soubor s uloženými daty, stav elektronického podání a ukládá se zde i heslo, které se automaticky generuje, pokud je přijatá zpráva elektronicky podepsána.

Sloupce tabulky:

1. Id - Sloupec obsahující jednoznačný identifikátor každého příchozího podání. Jeho hodnota se pro každou další ukládanou zprávu inkrementuje o 1.

2. Sent_from - Informace o emailové adrese osoby, která podání uskutečnila, popřípadě adrese elektronické podatelny, pokud se jedná o vyřízení podání.

3. Sent_to - Emailová adresa příjemce, která je rovna buďto emailové adrese elektronické podatelny nebo emailové adrese podávajícího, v případě odpovědi ze strany VUT.

4. CC - Případná kopie další osobě.
5. Subject - Předmět přijaté zprávy nebo odeslané zprávy.
6. Body - Odkaz na soubor ve kterém je uloženo tělo zprávy. Tento soubor se nachází v adresáři *../files/body/* a jeho název je vytvořen pomocí jednoznačného identifikátoru.
7. El_sign - Odkaz na soubor s elektronickým podpisem, který je uložen do adresáře *../files/sign/*. Unikátní název souboru je vytvořen hashovací funkcí MD5.
8. State - Stav přijatého podání, implicitně nastaven na hodnotu 'PRIJATO' (dalšími stavy jsou ''VYRIZOVANO', 'VYRIZENO' a 'SMAZANO').
9. Date - Datum a čas uskutečnění elektronického podání (např. Sat, 07 Apr 2007 22:23:50 +0200).
10. Pssw - Heslo automaticky generované při přijetí podání. Společně s hodnotou *id* slouží toto heslo pro pozdější kontrolu stavu podání ze strany odesílatele.
11. Id_ref - Hodnota, která v případě odpovědi na zprávu ze strany VUT slouží jako ukazatel na přijaté elektronické podání, uskutečněné uživatelem.
12. Id_uziv - Identifikátor uživatele, jemuž byla zpráva v rámci podatelny předána k vyřízení.
13. Cert_info - Informace o platnosti certifikátu a možnosti jeho použití.

6.3.2 Struktura tabulky *attachment*

V tabulce *attachment* jsou uloženy informace týkající se příloh emailu, jako jsou odkazy na přiložené soubory, jejich jména a také náležitost ke konkrétní zprávě.

Sloupce tabulky:

1. Uniq - Unikátní název souboru, vytvořený pomocí funkcí **uniqid(rand())** a původního jména souboru, pro případ přijetí více stejně pojmenovaných souborů.
2. Name - Skutečné jméno souboru, tak jak byl poslán společně se zprávou.
3. Sent_from - Informace o emailové adrese osoby, která přílohu odeslala.
4. Id_mail - Náležitost ke konkrétnímu emailu. Cizí klíč, odkazující se na hodnotu prvního sloupce (*id*) v tabulce *mail*.

6.3.3 Struktura tabulky *podat_prac_oc*

Ačkoliv nebylo s touto tabulkou v původním návrhu počítáno, vznikl při vývoji aplikace problém s určením správného adresáta v rámci celého VUT (vzhledem k velkému počtu uživatelů). Proto jsou podání předávána obsluhou podatelny nejdříve příslušným zaměstnancům jednotlivých ústavů a ti je pak přeposílají již cílovým adresátům. Informace o těchto zaměstnancích a pracovištích jsou obsaženy právě v tabulce *podat_prac_oc*.

Sloupce tabulky:

1. Id - Jednoznačná hodnota přijatého podání.
2. Id_prac - Identifikátor pracoviště, na které je podání přeposláno.
3. Id_osoba - Jednoznačný identifikátor zaměstnance ústavu, který podání předává konkrétnímu adresátovi.

6.4 Implementované funkce podatelny

V této části se budu zabývat bližším rozborem jednotlivých funkcí poskytovaných elektronickou podatelnou, které byly vytvořeny na základě předchozího návrhu (viz. 5.2).

6.4.1 Uskutečnění podání

Základní funkcí každé elektronické podatelny je možnost provádění podání elektronickou formou, která jsou shromažďovaná na jednom místě.[2]

Ve vytvořené aplikaci je tato možnost realizovatelná dvěma způsoby:

- **Pomocí uživatelského rozhraní**, přímo ze stránek elektronické podatelny. Při vytváření nového podání se do kolonek 'Předmět' a 'Email odesílatele' vyplní příslušné údaje a do 'Těla zprávy' je možné vepsat samotný text podání, jež lze dle potřeby strukturovat pomocí nástrojové lišty. K celému emailu je také možné připojit přílohu (viz. obr. 6.1).
- **Prostřednictvím uživatelova poštovního klienta**, pokud je například potřeba uskutečnit elektronicky podepsané podání. V takovém případě je nutné, aby měl odesílatel ve svém emailovém klientovi nainstalovaný platný certifikát, vydaný autorizovanou certifikační autoritou, a zprávu před odesláním na adresu podatelny pomocí tohoto certifikátu elektronicky podepsal. Ve všech ostatních případech je zpráva považována za nepodepsanou.

[2] V době odevzdání této práce ještě nebyla aktivní poštovní schránka elektronické podatelny VUT. Pro vývoj byla proto používána testovací emailová adresa epodatelna@centrum.cz.

6.4.2 Potvrzení o přijetí podání

Po doručení zprávy na adresu podatelny je pro každé podání automatiky vygenerováno sedmimístné heslo (složené z písmen a číslic), které je vzápětí společně s unikátním identifikátorem podání zasláno na emailovou adresu podávajícího.

6.4.3 Kontrola stavu podání

Na základě přijatého potvrzujícího emailu, který byl odeslán podatelnou si, každý uživatel může pomocí přiděleného identifikačního čísla a hesla kdykoliv zkontrolovat stav svého podání na stránkách elektronické podatelny.

Na obrázku 6.3 je znázorněn výpis stavu konkrétního podání, které je evidované pod identifikačním číslem 6. Dále jsou na výpisu zobrazeny informace o datu a času podání, emailu odesílatele a nakonec stavu, který může kromě aktuálního označení 'PRIJATO' nabývat ještě hodnot 'VYRIZOVANO', 'VYRIZENO' a 'SMAZANO'.

ID emailu	Odeslano z emailu	Datum a čas odeslání	Stav emailu
6	majlon@email.cz	Mon, 14 May 2007 15:33:27 +0200	PRIJATO

Obrázek 6.3: Výpis stavu přijatého podání

6.4.4 Kontrola platnosti certifikátu

Tato funkce je prováděna automaticky pokud je rozpoznáno podání obsahující přílohu s elektronickým podpisem. Výsledkem této kontroly jsou:

- Informace, zda byla zpráva korektně podepsána.
- Informace o platnosti certifikátu, kterým byla zpráva podepsána.
- Informace, zda certifikát náleží konkrétní emailové adrese, ze které byla zpráva přijata.
- Ověření, zda byl certifikát vydaný akreditovanou certifikační autoritou.
- Zjištění, k jakým účelům byl certifikát vydaný a v kterých případech může být legitimně použitý.

Obsluha podatelny má potom na základě získaných informací možnost rozhodnout, zda je certifikát opravdu důvěryhodný, nebo jestli se má se zprávou dále nakládat jako s nepodepsanou.

Finální a důležitou fází ověřování pravosti elektronického podpisu je zjištění, zda se příslušný certifikát nenachází na seznamu zneplatněných certifikátu CRL. Tato kontrola se provádí přímo na stránkách příslušné certifikační autority, která certifikát vydala.

6.4.5 Vyřízení podání

Obsluha podatelny má možnost přímo odpovědět na přijatá podání odesílateli, provést jejich smazání pokud jsou vyhodnocena jako nevyžádaná pošta, popřípadě podání přeposlat odpovědné osobě v rámci VUT. Tyto úkony také signalizuje změnou stavu podání.

6.4.6 Změna stavu podání

Zaměstnanci podatelny mohou nastavovat stav ve kterém se podání vyskytuje. Možné hodnoty stavu podání jsou:

- 'PRIJATO' - Jedná se o implicitní hodnotu, která je podání nastavena automaticky po jeho přijetí a zpracování podatelnou.
- 'VYRIZOVANO' - Hodnota kterou nastaví obsluha podatelny poté, kdy si nové podání přečte a začne jej vyřizovat.
- 'VYRIZENO' - Stav který nastává po vyřízení podání a odeslání zprávy zpět podávajícímu.
- 'SMAZANO' - Pokud je podání vyhodnoceno jako nevyžádaná pošta.

6.4.7 Smazání podání

Pokud obsluha podatelny vyhodnotí přijaté podání jako jakoukoliv formu nevyžádané pošty (SPAM) nebo bude-li obsah podání v rozporu z dobrými mravy, či zákony České republiky nebo pokud nebude podání obsahovat zpáteční emailovou adresu, může být obsluhou odstraněno z databáze.

6.4.8 Záloha přijatých podání

Obsluha podatelny má možnost kdykoliv provést zálohu informací uložených v databázi a veškerých souborů, které byly ke zprávám připojeny. Vytvořené zálohy je také možné dle uvážení odstraňovat.

Kompletní popis celého procesu zálohy dat podatelny se nachází v oddílu 6.5.7.

6.4.9 Obnova zálohovaných dat

Z vytvořených záložních souborů je poté kdykoliv možné provést obnovu dat. Způsob, jakým probíhá obnova dat ze zálohy, je podrobně popsána v odstavci 6.5.8.

6.4.10 Smazání zálohy dat

Jednotlivé bod obnovy databáze a dat je možné kdykoliv zcela odstranit ze systému, pokud je již záloha neaktuální.

6.5 Popis jednotlivých komponent aplikace

V této části je vysvětlena funkce jednotlivých komponent aplikace na implementační úrovni. V následujících bodech jsou přesně popsané jednotlivé funkční celky podatelny, struktura databáze, struktura dat, popisy funkcí, tříd, atd.

6.5.1 Parser příchozích emailů

Základním prvkem celé aplikace je parser nově příchozích elektronických podání. Emaily jsou nejdříve zpracovávány pomocí *IMAP funkcí*, standardně obsažených v jazyce PHP. Jedná se o následující funkce:

- **imap_open()**, zajišťující navázání spojení s příslušným POP3/IMAP serverem.
- **imap_fetchheader()**, která načítá do proměnné hlavičku zprávy.
- **imap_body()**, ukládající samotné tělo příchozího emailu. Toto tělo obsahuje jak text zprávy, tak případné přiložené soubory nebo soubor s elektronickým podpisem.

Pro samotnou analýzu takto získaných dat jsem použil již vytvořenou třídu *mimedecode* [19], vracející pole, které obsahuje jednotlivé informace o odesílateli, kódování, typu zprávy, atd. Veškeré potřebné hodnoty jsou následně uloženy do pole *mail_arr*, obsahující položky 'from', 'to', 'cc', 'subject', 'date', 'body' (definované pro data získaná z hlavičky zprávy) a poslední položkou 'attachments' typu pole, do kterého jsou ukládány informace o případných přílohách.

Ve fázi získávání hodnot z těla emailu mohou nastat tři případy:

1. Zpráva obsahuje pouze tělo v textovém tvaru, bez dalších částí.
2. Zpráva je složená z více částí (tzv. multi-part message) a neobsahuje přílohy (typicky v případě, kdy je tělo posláno zároveň v textové podobě a HTML kódu).
3. Zpráva je složená z více částí a obsahuje přiložené soubory.

Po vytvoření datové struktury pro konkrétní zprávu jsou zavolány funkce **SaveMail()** a **SaveAttachments()**, které zajistí uložení příslušných informací jak do databáze, tak do souborů. Procedura ukládání získaných dat je podrobně popsána v následujících bodech.

6.5.2 Ukládání hlavičky a těla emailu

Pro každé nově příchozí podání jsou volány funkce třídy **MailProcessor**, které mají za úkol uložení všech informací do databáze a také uložení příloh s těly emailů do souborů.

Ukládání údajů do databáze

Vkládání dat do databáze zajišťují funkce **SaveMail()** a **SaveAttachments()** třídy **MailProcessor** v souboru *mailprocessor.php*.

SaveMail()

Jde o funkci, která se zavolá pokaždé, když je přijata nová zpráva. Pomocí této funkce jsou také zapisována data obsažená v těle emailu do samostatného souboru (viz. 6.5.2). Před vkládáním nového řádku do databáze se nejdříve zjistí hodnota identifikátoru posledního podání uloženého v databázi, která se inkrementuje o 1 a výsledná hodnota tvoří identifikátor právě zpracovávané zprávy.

Do tabulky *mail* jsou poté uloženy:

- Hodnoty získané z hlavičky emailu, kterými jsou email odesílatele, email kopie, předmět emailu, datum odeslání zprávy (tyto hodnoty jsou uloženy jako položky v poli *mail_arr*).
- Odkaz na tělo emailu, které z důvodu své potenciální velikosti není ukládáno přímo v databázi, ale je pro něj vytvořen samostatný soubor v adresáři *../files/body*
- Vygenerované heslo pro ověření stavu přijaté zprávy, pomocí funkce **RandomKey()**, uložené v souboru *random.php*.

SaveAttachments()

Tato funkce se provádí, pokud se pří zpracovávání emailu narazí na přílohu. Kromě vkládání dat do databáze se stará také o ukládání příloh emailů (viz. 6.5.2).

Po zavolání SaveAttachment() se pomocí funkce uniqid(rand()) a kódování MD5 nejdříve vytvoří unikátní název souboru, pro případ, že by byly poslány přílohy se stejným názvem.

Následně se zjišťuje, zda je příloha souborem obsahujícím elektronický podpis. V takovém případě je nastaven příznak *signed* na hodnotu *true*, jinak je jeho hodnota *false*.

Před samotným uložením dat do databáze ze ještě zjistí, jestli jde o přílohu povoleného formátu (zakázány jsou soubory typu *bat*, *chm*, *cmd*, *com*, *cpl*, *dll*, *exe*, *hlp*, *hta*, *js*, *pif*, *reg*, *scr*, *shs*, *vbe*, *vbs*, *vxd*, *wsf*) a nastaví se příznak *forbidden_attach* na *true* pokud jde o nepovolené soubory a na *false* jde-li o soubory povolené.

Nejsou-li přílohy vyhodnoceny jako zakázané, je do tabulky *attachment* uloženo:

- Unikátní jméno společně s původním jménem souboru, tak jak byl připojen ke zprávě. Unikátní jméno slouží také jako odkaz do adresáře *../files/attachment/* kde jsou ukládány přílohy, popřípadě do adresáře *../files/sign/* obsahujícího soubory s elektronickými podpisy.

- Skutečné jméno souboru, tak jak bylo odesláno uživatelem.
- Email odesílatele souboru.
- Identifikátor emailu, ke kterému soubor náleží.

Pokud se jedná o soubor standardu X.509, obsahující elektronicky podepsaný hash dat, je také aktualizován příslušný záznam v tabulce *mail* a do sloupce *el_sign* je přidán odkaz na soubor s tímto podpisem.

Ukládání dat do souborů

Pro ukládání dat do souborů slouží stejné funkce jako pro vkládání informací do databáze. Soubory s daty jsou vytvářeny pomocí funkcí sloužících pro práci se soubory standardně obsažených v PHP. Konkrétně jde o funkce **fopen()**, **fwrite()**, **fclose()**.

Těla emailu

Celé tělo emailu je uloženo v poli, jako položka *body* (*mail_arr['body']*). Soubory s tělem emailu se nacházejí v adresáři *../files/body/* a jejich název je odvozen od identifikátoru konkrétního emailu, ke kterému tělo náleží. O vytvoření příslušného souboru a o zapsání všech dat se stará funkce **SaveMail()**.

Přílohy

Informace o ukládání souborů s přílohami jsou popsány v odstavci 6.5.3.

6.5.3 Ukládání příloh

Pokud je zjištěno, že zpráva obsahuje přiložené soubory, vyhodnotí se nejprve jejich typ a poté dojde (pokud se nejedná o nepovolené přílohy) k uložení souborů do příslušných adresářů. Přílohy mohou být trojího typu:

- Běžné datové soubory, které jsou ukládány do adresáře *../files/attachment/*. Název těchto souborů je změněn na unikátní hodnotu, aby nedocházelo ke konfliktu v případě přijetí více souborů stejného názvu.
- Soubory s elektronickým podpisem jsou ukládány do svého samostatného adresáře *../files/sign/* a jejich název je tvořen pomocí stejného postupu, jako u běžných datových souborů.
- Nepovolené soubory (*bat*, *chm*, *cmd*, *com*, *cpl*, *dll*, *exe*, *hlp*, *hta*, *js*, *pif*, *reg*, *scr*, *shs*, *vbe*, *vbs*, *vxd*, *wsf*), které jsou v případě komunikace prostřednictvím emailových zpráv nežádoucí a proto jsou zakázány a na server se vůbec neukládají.

6.5.4 Kontrola platnosti a ověření certifikátu

Pro kontrolu platnosti certifikátu jsem využil předem definovaných funkcí, obsažených v PHP modulu OpenSSL [17].

OpenSSL je projekt zaměřující se na vývoj nástrojů pro komerční využití protokolu SSL (Secure Sockets Layer). Jde o vrstvu tvořící mezistupeň mezi transportní a aplikační vrstvou, pomocí níž je realizováno zabezpečení komunikace mezi komunikujícími stranami (šifrováním a autentizací).

Získání certifikátu z elektronického podpisu

Pomocí OpenSSL funkce **OpenSSL_pkcs7_verify()** je z každé příchozí zprávy, která je elektronicky podepsána vyexportován osobní certifikát podávajícího a uložen ve formátu PEM (viz. 3.1.2).

Pokud proběhla analýza přijaté zprávy v pořádku a certifikát byl získán, znamená to, že je podání právoplatně podepsané. V případě, že dojde při vykonávání *OpenSSL* funkce k chybě, je elektronický podpis v nepořádku a tudíž neplatný.

Funkcí **OpenSSL_x509_parse()** je tento certifikát následně rozparsován a na základě získaných informací jsou poté vyhodnocovány konkrétní požadavky na validitu osobního certifikátu.

Jednotlivé testy platnosti certifikátu jsou obsaženy ve funkci **validate()**, nacházející se v souboru *validate.php*.

Kontrola platnosti certifikátu podle data vystavení

Čas odeslání podání, získaný při zpracování přijaté zprávy je převeden na řetězec ve formátu 'YYYYMMDDHHmmss', kde posloupnost 'YYYY' odpovídá roku, 'MM' měsíci, 'DD' dni v měsíci, 'HH' hodině, 'mm' minutě a 'ss' sekundě.

Z hodnot získaných pomocí parsovací OpenSSL funkce je vybrána položka *ValidTo* nesoucí informaci o konci platnosti certifikátu, která je ve stejném formátu, jako vytvořený řetězec. Pokud je po porovnání obou hodnot zjištěno, že je den a čas odeslání zprávy pozdější, než je konec platnosti certifikátu, je tento certifikát prohlášen za neplatný.

Kontrola vydávající certifikační autority

V České republice existují tři akreditované certifikační autority, které jsou legitimní k vydávání kvalifikovaných certifikátů (viz. 3.3). V této fázi kontroly dochází k ověření, zda byl certifikát vydaný jednou z těchto CA. Informace o vydávající CA je získána z hodnoty *issuer* vrácené po analýze certifikátu.

Pokud certifikát není vydaný jednou z akreditovaných CA, nemusí to nutně znamenat jeho neplatnost, ale snižuje se tím do jisté míry jeho důvěryhodnost.

Kontrola náležitosti certifikátu k emailu odesílatele

Každý certifikát není vydávaný pouze pro konkrétní osobu, ale jeho platnost je vztažena také ke konkrétní emailové adrese uživatele.

Pokud se je zjištěno, že emailová adresa rozpoznaná jako adresa odesílatele při analýze příchozí zprávy a emailová adresa vlastníka certifikátu nejsou totožné je elektronický podpis neplatný.

Ověření účelu, pro které byl certifikát vydán

Různé typy certifikátů mohou mít různý účel použití. Například zkušební certifikát, sloužící pro testovací účely není, možné považovat za důvěryhodný (nebyla ověřena totožnost vlastníka certifikátu). Informace o možnosti použití je získávána pomocí OpenSSL funkce **OpenSSL_x509_checkpurpose()**, s následujícími atributy, pro jednotlivé případy:

- X509_PURPOSE_SSL_CLIENT - Certifikát může být při zabezpečené komunikaci použit ze strany klienta.
- X509_PURPOSE_SSL_SERVER - Certifikát může být při zabezpečené komunikaci použit ze strany serveru.
- X509_PURPOSE_SMIME_SIGN - Informace o tom, že může být certifikát použit pro podepisování emailů ve formátu S/MIME.
- X509_PURPOSE_SMIME_ENCRYPT - Informace o tom, že může být certifikát použit pro dekódování emailů ve formátu S/MIME.
- X509_PURPOSE_CRL_SIGN - Certifikáty určené pro podepisování seznamu zneplatněných certifikátů (CRL).
- X509_PURPOSE_ANY - Certifikát je možné použít pro všechny účely.

Pro úplnost uvádím všechny možné účely užití, avšak z mého pohledu jsou zajímavé hodnoty v případě X509_PURPOSE_SSL_CLIENT a X509_PURPOSE_SMIME_SIGN.

Pokud certifikáty nedisponují požadovaným oprávněním pro jejich použití, je elektronický podpis vytvořený takovýmto certifikátem opět považován za neplatný.

6.5.5 Generátor přístupového klíče

Obsahuje-li přijatá zpráva elektronický podpis, je pomocí funkce **RandomKey()** nacházející se v souboru *random.php* vygenerováno přístupové heslo, které je uloženo jako jedna z položek podání v databázi.

Heslo je sedmimístné, tvořené písmeny nebo číslicemi. Podávajícímu je po jeho vygenerování toto heslo zasláno, společně s jednoznačným identifikátorem podání, aby bylo možné kontrolovat stav podání ze strany uživatele.

6.5.6 Odeslání potvrzení o přijetí

Pokud byla korektně zadána emailová adresa odesílatele, je okamžitě po zpracování zprávy, uložení dat do databáze a příslušných datových souborů do adresářů, automaticky odesláno potvrzení o přijetí na email, ze kterého bylo podání doručeno.

Funkce zajišťující odeslání tohoto potvrzení je funkce **mail()**, která je standardně obsažena v jazyce PHP. Tato funkce je součástí funkce **SendReceived()**, implementované v souboru *send_received.php*. **SendReceived()** zajišťuje odesílání potvrzujícího emailu podávající osobě. Kromě informace o přijetí zprávy podatelnou je tímto emailem zaslán také jednoznačný identifikátor a vygenerované heslo, na základě kterých je možné kontrolovat stav podání. Nakonec potvrzujícího emailu je ještě přiloženo tělo uživatelova podání.

6.5.7 Zálohování databáze a dat

Zálohování databáze je řešeno pomocí funkce **Export()**, definované ve třídě **ExportImport**, která se nachází v souboru *db_export_import.php*.

Data jsou exportována do souborů, formátu XML, které jsou ukládány v podadresářích adresáře *backup*.

Systematika vytváření záložních souborů

Pro snadnější orientaci je při zálohování pro každou tabulku vytvářen samostatný soubor, obsahující všechna její data. Název každého XML souboru zálohy je vytvořen na základě jména konkrétní tabulky. Přílohy a těla zpráv se zálohují zkopírováním celé adresářové struktury ve složce *files*. Tato kopie je vytvořena pomocí funkce **structureCopy()** implementované v souboru *copy_file.php*.

Pro každou verzi zálohy je vytvořen ve složce *backup* adresář, jehož název je odvozen z data a času provedení zálohy, ve formátu rok, měsíc, den, hodina, minuta, sekunda (tato hodnota je v jazyce PHP získána pomocí funkce **date("YmdHis")**).

Název souboru obsahujícího zálohu tabulky s informacemi o přílohách pak může vypadat například takto:

backup/20070326091814/attachment.xml

Přílohy, soubory s elektronickým podpisem a těla emailů jsou poté ukládány do složky *files*, která má stejnou adresářovou strukturu, jako původní složka do které jsou ukládána data při zpracování zprávy, například:

backup/20070326091814/files

Struktura dat v záložních souborech XML

Data jsou v záložních souborech strukturována hierarchicky a jsou ohraničena tagy, jejichž názvy korespondují s názvy sloupců tabulek. Každý řádek tabulky je pak opět uzavřen v

párových značkách.

Záložní soubor tabulky *attachment*

Jednotlivé záznamy jsou elementy objektu *tabattachment*, kdy každému souboru odpovídá záznam ohraničený tagy *attachment*. Formát souboru vypadá následovně:

<tabattachment>
<attachment>
<UNIQ> *unikátní název souboru* </UNIQ>
<NAME> *skutečné jméno souboru* </NAME>
<SENT_FROM> *emailová adresa odesílatele* </SENT_FROM>
<ID_MAIL> *identifikátor emailu, ke kterému příloha náleží* </ID_MAIL>
</attachment>
<attachment>
...
</attachment>
...
...
...
</tabattachment>

Záložní soubor tabulky *mail*

Analogicky jsou vytvářeny záložní soubory pro tabulku *mail*, obsahující základní informace o příchozích zprávách.

Informace jsou strukturovány obdobným způsobem, v tomto případě však jako položky v objektu *tabmail* a jednotlivé elementy tohoto objektu jsou uzavřeny klíčovým slovem *mail*.

Formát záložního souboru tabulky *mail*:

<tabmail>
<mail>
<ID> *unikátní identifikátor emailu* </ID>
<SENT_FROM> *emailová adresa odesílatele emailu* </SENT_FROM>
<CC> *adresát, pro kterého je určena kopie zprávy* </CC>
<SUBJECT> *předmět příchozí zprávy* </SUBJECT>
<BODY> *unikátní identifikátor emailu* </BODY>
<EL_SIGN> *odkaz na elektronický podpis* </EL_SIGN>
<STATE> *stav ve kterém se podání nachází* </STATE>
<DATE> *datum uskutečnění podání* </DATE>
<PSSW> *přidělené heslo, sloužící odesílateli pro ověření stavu podání* </PSSW>

<ID_REF> *referenční hodnota na podání u odeslaných odpovědí* </ID_REF>
<ID_UZIV> *identifikátor uživatele, kterému byla přeposlána zpráva* </ID_UZIV>
<CERT_INFO> *informace o validitě certifikátu* </CERT_INFO>
</mail>
<mail>
...
</mail>
...
...
...
</tabmail>

6.5.8 Obnova databáze ze zálohy

Nejdříve je potřeba si z nabízených záložních verzí vybrat tu, která má posloužit pro obnovu všech dat podatelny.

Před samotným zahájením procesu obnovy jsou z databáze nejdříve smazány všechny záznamy a také jsou kompletně odstraněny soubory v adresáři *files* a jeho podadresářích, pomocí funkce **structureDel()** nacházející se v souboru *delete_file.php*.

Obnova databáze ze souborů XML se provádí pomocí funkce **Import()**, která je rovněž jako funkce pro export dat součástí třídy **ExportImport**, nacházející se v souboru *db_export_import.php*.

Tato funkce načítá jednotlivé XML soubory vybrané verze zálohy a následným rozparsováním extrahuje potřebná data s využitím funkcí **startElement()**, **endElement()** a **characterData()** a PHP funkcí pro XML parsing.

Funkce startElement()

Tato funkce při procházení jednotlivých tagů rozpoznává hodnotu indikující začátek nového elementu (záznamu). Jakmile se tak stane, dochází k inicializaci datového pole, které bude postupně naplňováno daty.

Funkce characterData()

Pokud bylo inicializováno datové pole, dochází v této fázi k jeho naplnění, kdy každá položka pole odpovídá jedné hodnotě příslušného záznamu (příslušnému sloupci v databázi).

Funkce endElement()

Jakmile se při analýze narazí na hodnotu označující konec příslušného záznamu, dojde k uložení všech hodnot z datového pole do databáze.

Funkce pro XML parsing obsažené v php

- **xml_parser_create()** je funkce, pomocí níž se nejdříve vytvoří nový XML parser.
- **xml_parser_set_option()** následně nastaví možnosti XML parseru.
- **xml_set_element_handler()** provede vyhodnocení začátku a konce konkrétního elementu.
- **xml_set_character_data_handler()** způsobí po zavolání naplnění všech dat do výstupního pole.
- **xml_parser_free()** se volá úplně v závěru a ukončuje aktuální parser, vytvořený pomocí **xml_parser_create()**.

Obnova datových souboru (těla emailů, přílohy, soubory s elektronickým podpisem) je prováděna stejně jako při zálohování souborů pomocí funkce **structureCopy()**.

6.5.9 Odstranění zálohy

Pomocí funkce **removeDir()**, v souboru *delete_backup.php* je možné libovolnou verzi zálohy kdykoliv vymazat ze systému.

Kapitola 7

Závěr

V rámci mé diplomové práce jsem se zabýval problematikou elektronického podepisování a osobních certifikátů. V souvislosti s osobními certifikáty jsem se seznámil s procesem jejich vydávání a rušení certifikačními autoritami.

V kapitole zabývající se elektronickými podatelnami jsem prostudoval funkce požadované od podatelny a následně jsem porovnával aplikace umožňující elektronické podání, které jsou dostupné na českém trhu. Na základě získaných poznatků jsem vytvořil návrh elektronické podatelny pro VUT v Brně.

Při samotné tvorbě systému elektronické podatelny jsem implementoval jednotlivé požadavky podatelny vycházející z předchozího návrhu s důrazem na vizuální i funkční provázanost s již fungujícím portálem.

Jako možné pokračování této práce vidím vytvoření elektronické spisové služby, která by byla využívána pro správu a archivaci dokumentů a informací v rámci VUT v Brně.

Literatura

[1] WWW stránky. Ministerstvo informatiky České republiky.
http://www.micr.cz

[2] WWW stránky. Národní bezpečnostní úřad.
http://nbu.cz

[3] Peterka, J.: Elektronický podpis. In: e-archiv Jiřího Peterky, 2001
Dokument dostupný na URL http://www.earchiv.cz/i_digsig.php3
(leden 2007).

[4] Peterka, J.: Elektronické podatelny. In: e-archiv Jiřího Peterky, 2001
Dokument dostupný na URL http://www.earchiv.cz/b01/b0500010.php3
(leden 2007).

[5] Vícha, K.: E-podpis aneb testujeme digitální certifikáty. In: interval.cz, 21.3.2003
Dokument dostupný na URL
http://interval.cz/clanky/e-podpis-aneb-testujeme-digitalni-certifikaty
(leden 2007).

[6] Doležal, D.: Co to je digitální certifikát. In: interval.cz, 21.1.2003
Dokument dostupný na URL
http://interval.cz/clanky/co-to-je-digitalni-certifikat (leden 2007).

[7] Staudek, J., Hanáček, P.: Certifikační infrastruktury veřejných klíčů, PKI. Vyd. 1.
Bratislava: Slov. informatická společnost, 2001, s. 47, Sborník konferenceDATAKON
2001.

[8] Kropáčová, A.: Bezpečnost elektronických dat a elektronické komunikace. Zpravodaj
ÚVT MU. ISSN 1212-0901, 2006, roč. XVI, č. 4, s.15-20.

[9] Vondruška, P., Bosáková,D.: Vysvětlení základních pojmů zákona o elektronickém
podpisu. Crypto-World, Informační sešit GCUCMP, 2002, roč. 4, č. 3, s. 2-17.

[10] Internetová prezentace produktu podatelna.info.
http://www.epodatelna.cz

[11] Internetová prezentace produktu Mail602 ePodatelna
http://www.602.cz

[12] Internetová prezentace elektronické podatelny spol. ICZ.
http://www.i.cz/verejnasprava

[13] Internetová prezentace produktu TrustPort spol. AEC.
http://www.epodatelny.cz

[14] Internetová prezentace produktu Post Office.
http://postoffice.spost.cz

[15] Internetové stránky společnosti Topspin Solutions.
http://www.topspin.cz/tis

[16] Internteová enciklopedie Wikipedia.
http://www.wikipedia.org

[17] WWW stránky. Projekt OpenSSL.
http://www.openssl.org

[18] WWW stránky. Online PHP manuál.
http://www.php.net

[19] WWW stránky. PHP Classes Repository.
http://www.phpclasses.org

Seznam příloh

Dodatek A

Seznam použitých zkratek

ASK - asymetrická kryptografie
PKI (Public Key Infrastructure) - infrastruktura veřejných klíčů
RSA (Rivest, Shamir, Adleman) - asymetrický kryptovací algoritmus
DSA (Digital Signature Algorithm) - asymetrický kryptovací algoritmus, využívaný pro elektronický podpis
DSS (Digital Signature Standard) - standardy týkající se elektronického podpisu
ALGO (Algorithms and Parameters for Secure Electronic Signatures) - seznam požadavků na kryptovací algoritmy
MD5 (Message-Digest algorithm 5) - hashovací funkce
NBÚ - Národní bezpečnostní úřad
SHA-1/SHA-2 (Secure Hash Algorithm)- hashovací funkce
X.509 - standard kvalifikovaných certifikátů
PEM (Privacy Enhanced Mail)- formát pro práci s certifikáty v textovém tvaru zakódovaný pomocí base64
DER (Distinguished Encoding Rules) - pravidla pro kódování certifikátů
CER (Canonical Encoding Rules) - pravidla pro kódování certifikátů
CA (Certificate Authority) - certifikační autorita
I.CA - První certifikační autorita a.s.
CRL (Certificate Revocation List) - seznam zneplatněných certifikátů
Δ CRL (Delta Certificate Revocation List) - rozdílový seznam zneplatněných certifikátů
OCSP (On-line Certificate Status Provider) - poskytovatel informací o stavu certifikátů
TSP (Trusted Service Provider) - důvěryhodný poskytovatel
SPAM - nežádoucí elektronická pošta
FAQ (Frequently Asked Questions) - seznam často kladených dotazů
REP - registrovaná elektronická pošta
ER (Entity Relationship) - diagram entitních vztahů
PHP (PHP: Hypertext Preprocessor) - skriptovací jazyk

OCI (Oracle Call Interface) - dotazovací rozhraní Oracle
SQL (Structured Query Language) - neprocedurální strukturovaný dotazovací jazyk
HTML (HyperText Markup Language) - značkovací jazyk
CSS (Cascade Style Sheet) - kaskádové styly
XML (eXtensible Markup Language) - rozšiřitelný značkovací jazyk
POP3 (Post Office Protocol version 3) - protokol pro přijímání emailů
IMAP (Internet Message Access Protocol) - protokol pro přístup k elektronické poště

Dodatek B

Uživatelská příručka

Nové podání

Podání je možné uskutečnit dvěma způsoby:

1. S využitím poštovního klienta, na elektronickou adresu podatelny.
2. Pomocí formuláře nacházejícího se na stránkách elektronické podatelny.

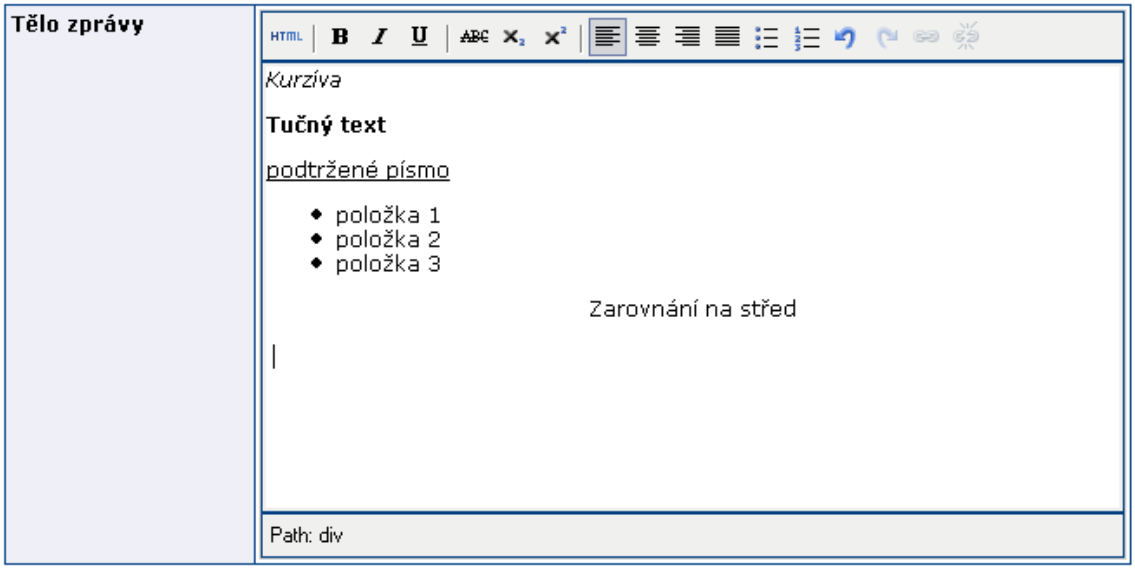
Formulář pro odesílání

Ve formuláři je nutné vyplnit emailovou adresu na kterou má být doručena případná odpověď a předmět zprávy (obr. B.1).

Předmět	Žádost o vyjádření
Email odesílatele	jan.novak@domena.cz
Email podatelny	epodatelna@centrum.cz

Obrázek B.1: Hlavička podání

V textové oblasti je poté možné vytvořit požadované podání ke kterému lze přiložit datový soubor (podle pravidel uvedených níže). Pomocí rozšířených nástrojů pro sazbu textu může být také výsledná zpráva přehledněji strukturována (obr. B.2).



Obrázek B.2: Tělo zprávy s nástrojovou lištou a ukázkou formátování textu

Podání pomocí poštovního klienta

Pro tento případ je na stránkách podatelny uveden odkaz v podobě emailové adresy, na kterou jsou podání doručována.

Povolené přílohy

Při odesílání podání pomocí formuláře na stránkách elektronické podatelny je maximální velikost přílohy 2 MB. Při provedení podání pomocí poštovního klienta je příloha limitována velikostí 20 MB.
Zakázáno je odesílat se zprávou následující přílohy:

bat, *chm*, *cmd*, *com*, *cpl*, *dll*, *exe*, *hlp*, *hta*, *js*, *pif*, *reg*, *scr*, *shs*, *vbe*, *vbs*, *vxd*, *wsf*

Kontrola stavu podání

Stav podání je možné kontrolovat na základě identifikačního čísla a hesla, uvedených v potvrzujícím dopisu. Formulář pro kontrolu stavu podání se nachází ve spodní části úvodní stránky podatelny.
Podání se může vyskytovat v následujících stavech:

- ‘PRIJATO’ - Podání bylo přijato podatelnou
- ‘VYRIZOVANO’ - Podání bylo zpracováno a je ve stádiu vyřizování

- ‘VYRIZENO’ - Podání bylo vyřízeno a odpověď byla zaslána na emailovou adresu podávajícího.
- ‘SMAZANO’ - Podání bylo vyhodnoceno jako nepovolené.

Zákon o elektronickém podpisu

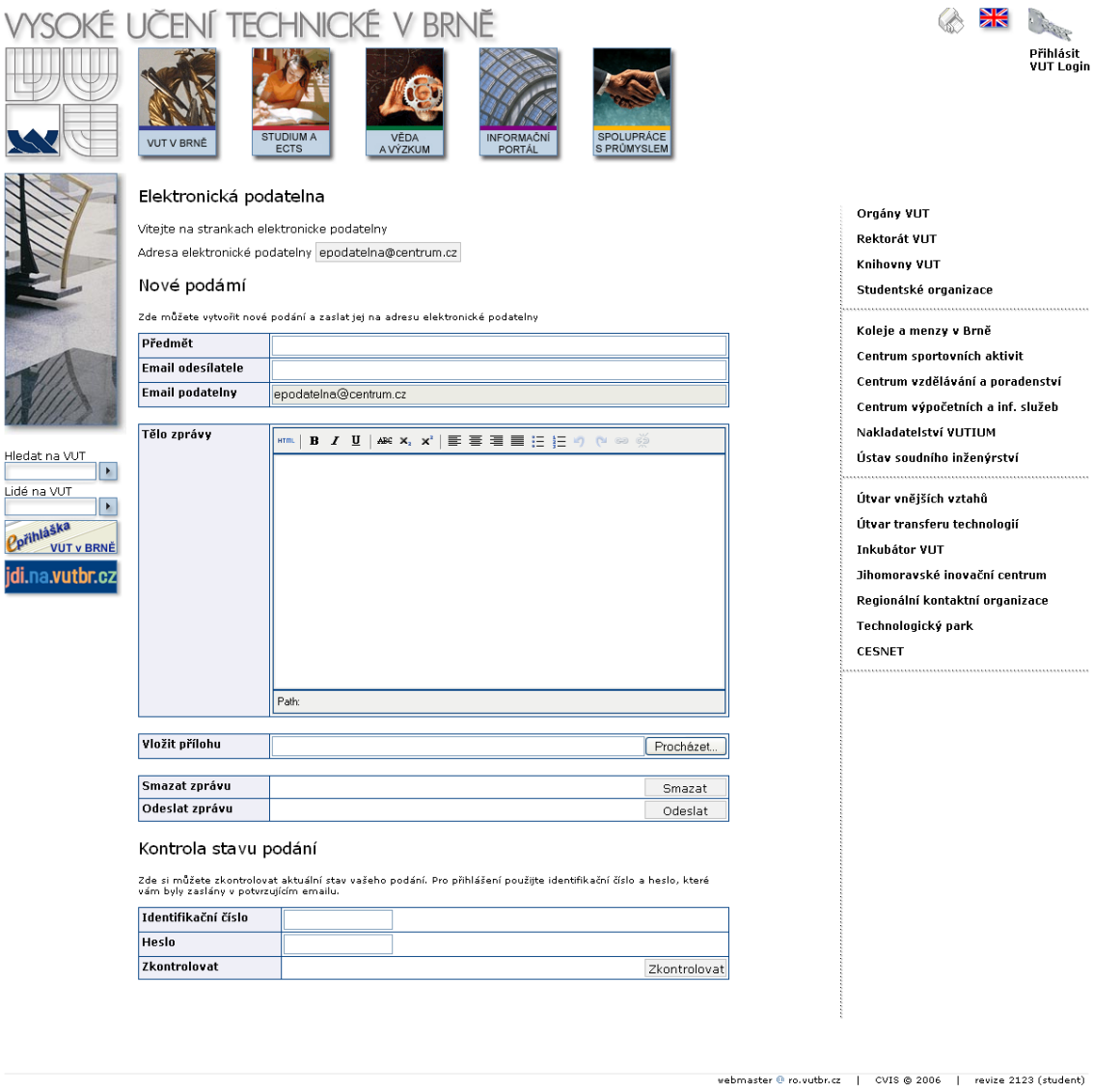
Pravidla používání elektronického podpisu stanoví zákon č. 227/2000 Sb., o elektronickém podpisu.

Obsluha podatelny

Obsluha podatelny má možnost vytvářet záložní kopie všech informací pomocí tlačítka ‘Export’ (viz. obr. B.3). Z těchto záložních kopií je poté kdykoliv možné databázi zpětně obnovit. Pro obnovu dat je nejdříve nutné vybrat verzi obnovy a poté stisknout tlačítko ‘Import’. Je důležité dbát zvýšené opatrnosti při provádění obnovy dat, jelikož všechny původní záznamy jsou z databáze odstraněny. Jednotlivé verze verze zálohy je možné kdykoliv odstranit tlačítkem ‘Smazat’.[1]

Obrázek B.3: Rozhraní pro práci se zálohami dat

[1] Další funkce dostupné pro obsluhu podatelny jsou popsány v uživatelské příručce, která je součástí diplomové práce: Beran, M.: Elektronická podatelna VUT 2. Brno, 2007. Diplomová práce na FIT VUT v Brně. Vedoucí diplomové práce Ing. Jaromír Marušinec, Ph.D.



Obrázek B.4: Uživatelské rozhraní podatelny, v rámci portálu VUT

Dodatek C

Přiložené CD

Obsahem přiloženého CD je:

- Písemná zpráva ve formátu PDF.
- Zdrojový tvar písemné zprávy ve formátu TEX, včetně všech potřebných souborů (šablona, obrázky), ve složce *zpráva*.
- Zdrojové kódy aplikace.
- Diagramy (Use case, ERD) ve formátu MDL.
- Kopie licenční smlouvy ve formátu PDF.