# Certifikáty a certifikační autority

Diplomová práce

Autor: Bc. Stanislav Čeleda

Vedoucí práce: PhDr. Milan Novák Ph.D.

Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra informatiky

Rok 2011

## Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Praze dne 1. prosince 2011.

## Poděkování

Rád bych tímto poděkoval vedoucímu práce panu PhDr. Milanu Novákovi Ph.D. za možnosti konzultace, trpělivost a jeho cenné rady při tvorbě mé diplomové práce.

## Anotace

Tato práce se zabývá možnostmi využití digitálních certifikátů a analýzou certifikačních autorit nebo jejich alternativ a jejich využití pro vytvoření zabezpečené komunikace v informačních systémech. V praktických ukázkách je předvedena realizace certifikační autority pod různými operačními systémy a generování různých druhů digitálních certifikátů. Na základě získaných poznatků je provedeno doporučení pro volbu vhodné certifikační autority.



Klíčová slova: digitální certifikát, certifikační autorita



## Abstract

This work deals with the possibilities of using digital certificates and certification authorities or analysis of alternatives and their use to create secure communication in information systems. In practical examples is demonstrated by the CA implementation on different platforms and generate various types of digital certificates. Based on the findings is made recommendations for choosing the appropriate certification authority.



Keywords: digital certificate, certification authority

# Obsah

# 1 Úvod

Infrastruktura veřejných klíčů je systémem digitálních certifikátů a certifikačních autorit, které slouží k ověřování identity (autentizaci) účastníků elektronické komunikace. Celá technologie je postavena na asymetrické kryptografii s veřejným a soukromým klíčem.

Neustálý rozvoj digitální komunikace, nahrazování klasických papírových dokumentů elektronickými a stále vyšší počet osob využívající moderní komunikační technologie, vyžaduje rozšíření moderních autentizačních metod. V současné době je možné za pomoci kvalifikovaného digitálního certifikátu komunikovat s orgány státní správy, podávat žádosti, vyřizovat daňová přiznání, obchodovat apod. Komerční certifikáty se využívají zejména pro šifrování, autentizaci a přístupy na neanonymní webové servery pomocí protokolu SSL/TLS.

Snahou této práce je přiblížit možnosti využití autentizačních metod a především digitálních certifikátů a jejich využití v informačních systémech, vytipovat vhodná řešení a doporučit vhodnou certifikační autoritu na základě požadavků uživatele. V případě, že služby certifikační autority neodpovídají potřebám uživatelů, představuje práce možné alternativy a realizuje ukázková řešení vybraných softwarových nástrojů pro správu vlastní certifikační autority na různých operačních systémech.

Právě školství a především pedagogické a technicky zaměřené fakulty vysokých škol by měly řídit rozvoj a podporovat proces přípravy učitelů a studentů. Na přípravě budoucích učitelů informatiky tak bude záviset, zda jejich žáci získají kvalitní informace a naučí se využívat možnosti, které jim moderní autentizační technologie nabízejí. Na samotných učitelích pak bude záležet, zda zařadí toto téma (a jakým způsobem) do školních vzdělávacích plánů. Z těchto důvodů by běžné využívání autentizačních metod, založených na digitálních certifikátech ve školství, přispělo k všeobecnému rozvoji a tím k dosažení cíle, kterým je bezpečná elektronická komunikace.

# 2 Předmět výzkumu

Práce je rozdělena do několika částí:

Teoretická část práce se nejprve zabývá analýzou používaných základních metod autentizace z hlediska možnosti zneužití a náročnosti překonání, dále z hlediska technické náročnosti a spolehlivosti a z hlediska nákladů. Kombinací více autentizačních metod pro zvýšení bezpečnosti se zabývá kapitola vícefaktorová autentizace.

Pro analýzu digitální certifikátů je potřeba vycházet ze znalosti obsahu certifikátu, významu jednotlivých položek, které řídí jeho vlastnosti a možnosti využití. Zvláštní pozornost v analýze je věnována kryptografickým algoritmům, protože především na jejich kvalitě závisí spolehlivost celého procesu. Je vysvětlen postup tvorby digitálního podpisu a jeho princip, který musí splňovat základní požadavky na autenticitu, integritu a nepopiratelnost.

Cílem hlavní části práce je analýza digitálních certifikátů a certifikačních autorit. Nejdříve je detailně popsána činnost certifikační autority, podmínky pro vydání certifikátu, procesu revokace certifikátu v případě kompromitace soukromého klíče nebo jiného závažného důvodu. V neposlední řadě jsou důkladně analyzovány české certifikační autority, které získaly akreditaci Ministerstva vnitra České republiky pro vydávání kvalifikovaných certifikátů. Komparace je provedena z hlediska bezpečnosti, nabízených služeb a produktů, rychlostí reakce na požadavky (např. na revokaci certifikátu) a cen. Výsledkem komparace je hodnotící tabulka, která stanoví pořadí kvality jednotlivých certifikačních autorit. Na základě těchto analýz bude doporučena vhodná certifikační autorita pro uživatele hlavně v oblasti školství ale i jiných oborů.

V praktické části práce jsou předvedeny možnosti autentizace prostřednictvím digitálního certifikátu na funkčním webovém serveru. Pro případ volby alternativy ke službám certifikační autority, je odzkoušeno několik dostupných softwarových nástrojů, které slouží ke správě certifikační autority. Za pomoci těchto nástrojů byla vždy vytvořena sada základních certifikátů: certifikát certifikační autority, serverový a klientský certifikát. Jsou popsány zkušenosti s těmi nástroji, doporučení čeho se vyvarovat a na co se zaměřit. Za pomoci redakčního systému, je odzkoušeno zabezpečené přihlášení do systému volně dostupnými moduly.

Z hlediska struktury práce a uvedené problematiky byly vytyčeny následující cíle práce:

- analýza autentizačních metod,
- analýza digitálních certifikátů, jejich druhy, vlastnosti, použité technologie, možnosti využití,
- průzkum certifikačních autorit, analýza kvality zabezpečení, služeb a činností,
- vypracování hodnocení certifikačních autorit a doporučení vhodného řešení na základě požadavků uživatelů,
- odzkoušení na praktických ukázkách, vytvoření certifikační autority, generování různých druhů certifikátů, vytvoření zabezpečeného spojení na webovém serveru.

## 2.1 Metoda práce

V teoretické části jsou shrnuty potřebné znalosti pro analýzu samotných certifikátů a následně certifikačních autorit.

Výzkum certifikačních autorit vychází především z:

- teoretických znalostí, získaných v teoretické části práce,
- podrobného studia certifikačních politik jednotlivých autorit,
- prohlídky jejich webových prezentací,
- instalace a odzkoušení software pro správu digitálních certifikátů,
- komunikace s operátory uživatelské podpory prostřednictvím emailu nebo telefonicky.

Na certifikačních autoritách je provedena analýza z hlediska technické způsobilosti, bezpečnosti, nabízených služeb a produktů, dostupnosti uživatelské podpory, cenové náročnosti, dostupnosti pracovišť registračních autorit apod. Po shromáždění potřebných dat byla provedena jejich komparace a přehledné zobrazení výsledků v tabulce.

V praktické části bude odzkoušeno vytvoření certifikační autority a vygenerování digitálních certifikátů pro server i pro klienta pomocí běžně dostupných softwarových nástrojů. Vygenerované certifikáty budou použity pro vytvoření zabezpečeného spojení na webovém serveru.

# 3 Obecné metody autentizace

Nejprve se zastavme u samotného termínu „autentizace“. V odborné literatuře se můžeme běžně setkávat s dalšími termíny jako „autentifikace“ nebo „autentikace“. Původ slova je v latinském „authenticus“, ze kterého je převzala většina jazyků. V češtině se ujalo několik výše uvedených termínu, které však představují pouze synonyma stejného slova a mají naprosto stejný význam. V této práci se bude užívat nejvíce používaný termín „autentizace“, ke kterému se přiklání i Ústav pro jazyk český.

Proces autentizace představuje prokázání pravosti entity, např. osoby nebo programu (kódu), zprávy apod. Úspěšná autentizace potvrzuje identitu ověřované entity a zajišťuje ochranu před falzifikací identity.

Autentizace využívá velice mnoho metod různé úrovně spolehlivosti a stupně zabezpečení. V další části bude provedena analýza nejpoužívanějších autentizačních metod a jejich využití ve vícefaktorové autentizaci.

## 3.1 Autentizace za pomocí hesla.

Autentizace za pomocí hesla je pravděpodobně nejstarší metoda. Má velice mnoho slabých míst, především hrozí snadné vyzrazení hesla. Uživatelé často používají jména, telefonní čísla, adresy bydliště apod. Tato hesla může i nezkušený útočník snadno uhodnout. Ani volba běžných slov není příliš bezpečná. Za použití slovníku běžných slov, který obsahuje 30 000 slov, není problém heslo odhalit. Tento nedostatek je možné částečně eliminovat donucením uživatele použít heslo o určitém počtu znaku složených z velkých a malých písmen a čísel.

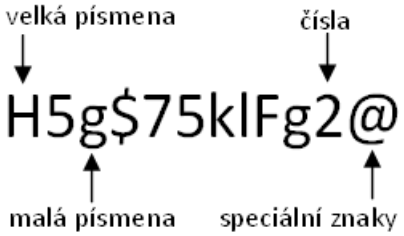
Velkou nevýhodou této metody je možnost zaznamenání stisknutých kláves rezidentním programem, který může na stanici běžet bez uživatelova vědomí. Těchto programů je na internetu velké množství a běžný uživatel i bez znalosti programování dokáže snadno heslo získat. Z tohoto důvodu byly vyvinuty další spolehlivější metody autentizace.

### 3.1.1 Požadavky na bezpečné heslo

Za bezpečné heslo můžeme považovat takové heslo, které splňuje následující podmínky:

- obsahuje velká a malá písmena, speciální a numerické znaky,
- je dostatečně dlouhé,
- nemá vztah k uživateli hesla, např. jméno, datum narození apod.,

- nemá vztah k prostředí, kde se heslo používá, např. adresa,
- neobsahuje opakující se znaky, např.: 1111,
- nevyužívá abecední posloupnosti, nebo rozložení kláves,
- slovo není obsažené v běžném slovníku.




Obrázek 3.1.1-1: Znázornění spolehlivého hesla.

Proces vytváření bezpečného hesla a dodržování určitých podmínek by měl kontrolovat samotný systém správy hesel. Nemůžeme se spolehnout na disciplínu uživatelů. Systém sám by měl kontrolovat, zda zadávané heslo obsahuje velká a malá písmena, čísla, speciální znaky a neobsahuje slova uvedená ve slovníku. Dále by měl systém kontrolovat, jakou má heslo délku, zda již nebylo uživatelem jednou použito nebo zda není jen drobnou obměnou některého v minulosti použitého hesla. Pokud je uživateli nastaveno výchozí heslo, určené pouze pro první přihlášení, měl by systém vyzvat uživatele ke změně hesla hned po prvním přihlášení do systému. Systém by také neměl prozrazovat, který ze zadávaných údajů je špatný, zda jméno nebo heslo.

Doba platnosti hesla by měla být závislá na úrovni spolehlivosti hesla, tzn. na použité délce a použitých znacích. Tyto parametry určují dobu potřebnou k prolomení hesla. Tato doba by měla být přímo úměrná délce platnosti hesla a nepřímo úměrná kvalitě hesla.

### 3.1.2 Požadavky na systém

Podle uvedených požadavků na heslo, můžeme stanovit, jaké parametry musí splňovat systém správy hesel.[1]

- Historie hesel: kolik hesel si systém pamatuje a nedovolí dříve použité heslo znovu použít.

[1] Clever and smart. *Politika účtů a hesel* [online]. [cit. 2011-09-21]. Dostupné z WWW: <http://www.cleverandsmart.cz/autentizace-politika-uctu-a-hesel>.

- Počet neplatných pokusů přihlášení: pokud uživatel (nebo útočník) provede určitý počet neplatných přihlášení, dojde k uzamknutí účtu. Typicky se používají 3 – 5 neplatných pokusů.
- Doba uzamčení: pokud dojde k uzamčení účtu, je možné definovat dobu, po kterou není možné se znovu pokusit zadat heslo. U kritických účtů je vhodné uzamknout účty trvale, odblokovaní musí provést administrátor systému.
- Minimální doba platnosti hesla: doporučené nastavení je 0, heslo je možné měnit kdykoliv. Uživatel může heslo změnit i v případě, že má podezření, že jeho heslo bylo vyzrazeno.
- Maximální doba platnosti: maximální doba platnosti hesla vychází z délky a spolehlivosti hesla. Měla by být nižší než doba, za kterou je útočník schopen heslo prolomit hrubou silou.
- Počet neúspěšných pokusů o přihlášení: systém by měl zobrazovat informace o posledních neúspěšných pokusech o přihlášení od posledního úspěšného přihlášení.
- Zobrazení posledního místa a času posledního přihlášení.

## 3.2 Autentizace za pomoci technické pomůcky

Jednou z nejdůležitějších metod autentizace je metoda, kdy se uživatel prokazuje vlastnictvím předmětu.

### 3.2.1 Metoda za použití hardwarového klíče.

Hardwarový klíč je zařízení, které se připojuje k počítači nejčastěji pomocí USB portu, dříve také paralelním portem. Tato metoda se nejčastěji využívá k ověření platnosti softwarové licence a k zabránění nelegálnímu používání aplikací. Samozřejmě je také možné tuto metodu využít i při přihlašování uživatele k systému, např. internetového bankovnictví.

Hardwarový klíč je možné rozdělit ještě do dvou dalších typů:

- hardwarový klíč obsahuje data, která systém při spuštění nebo za běhu kontroluje a při načtení nesprávných dat na toto skutečnost reaguje.
- hardwarový klíč překládá data z aplikace do strojového jazyka a umožňuje zpracování informace.

V dnešní době se nejvíce využívají tzv. tokeny. Může se jednat o čipovou kartu nebo USB token.

### 3.2.2 Čipové karty:

Data na čipové kartě jsou oddělena od počítače a útočník se k nim nedostane tak snadno, jako v případě, kdy jsou uložena přímo na pevném disku.

Základní funkce čipové karty:

- záznamová: na čipovou kartu je možné zapsat data a z karty je číst,
- identifikační: čipovou kartu je možné použít k identifikaci jejího držitele,
- kryptografická: umožňuje bezpečně provádět kryptografické operace, zejména šifrování, autentizaci a elektronický podpis,
- programová: na čipovou kartu lze umístit aplikace pro vytváření rozšířených funkcí. [2]

Na kartě je integrována paměť typu ROM, do které je při výrobě nahrán operační systém. Dále čip obsahuje operační paměť typu RAM o velikosti řádově jednotek kilobajtů. Tuto paměť využívá operační systém k provádění datových operací. Posledním typem paměti integrované v čipu je pracovní paměť EEPROM, která je využita k ukládání kryptografických dat např. klíčů. Její velikost se liší podle typu karty, běžně dosahuje velikosti až desítek kilobajtů. Karty komunikují se čtecím zařízením v poloduplexním režimu.

Čipové karty podle normy FIPS 140–1 level 2 současně umožňují i generování nových klíčů (privátního a veřejného), které mají být následně určeny pro tvorbu elektronického podpisu, případně jeho ověřování. Vlastností, kterou zatím nikdo nezpochybnil, je to, že pokud je na takové čipové kartě vytvořen privátní klíč, tak tento klíč po celou dobu své existence neopustí kartu. Operace, při kterých je třeba privátní klíč použít, jsou prováděny na čipové kartě.[3]

### 3.2.3 Autentizační kalkulátor

Jedná se o elektronickou pomůcku, která slouží k autentizaci protistrany. Komunikující protistrany jsou vybaveny autentizačním kalkulátorem. Kalkulátor je hardwarové zařízení obsahující sdílené tajemství. Součástí kalkulátoru je algoritmus pro vytváření otisků, např. MD5 nebo SHA-1.

---

[2] Svoboda, J. *Seminář PKI* [online]. [cit. 2011-09-21]. Dostupné z WWW: <http://www.cesnet.cz/akce/20031204/karty.pdf>.

[3] Nápravník, J. *Jsou čipové karty bezpečné?* [online]. [cit. 2011-09-20]. Dostupné z WWW: <http://www.lupa.cz/clanky/jsou-cipove-karty-bezpecne/>.

Kalkulátor určený pouze pro autentizaci zahrnuje zdroj přesného času. Kalkulátor generuje heslo na jednorázové použití. Toto heslo je vytvořeno jako kontrolní součet času a sdíleného tajemství. Kalkulátor protistrany jednorázové heslo ověří na základě stejného principu.

Nevýhodou použití kalkulátoru je nutnost synchronizace sdíleného tajemství a zdroje času. Zdroj přesného času běží s přesností na minuty (resp. poloviny minut). Drobné odchylky zdroje času lze řešit následujícím způsobem. Kalkulátor vypočítá několik hodnot vpřed i vzad. Je-li nalezena shoda, je umožněn přístup a zaznamenán časový posun.[4]

### 3.2.4 USB tokeny

USB tokeny jsou konstrukčně velice podobné čipovým kartám. Obsahují kryptografický mikroprocesor, vnitřní paměti, komunikační rozhraní. USB tokeny umožňují generování privátního klíče přímo v tokenu. Pro asymetrické šifrování je to velmi výhodné, protože se privátní klíč nemusí posílat přes bezpečnostně slabé kanály, minimalizuje se tak možnost zneužití zabezpečených dat. Moderní tokeny podporují generovaní privátního klíče pro asymetrickou šifru RSA o délce až 2048 bitů.[5]

### 3.2.5 Bezpečnost hardwarových pomůcek

Aby mohl nějaký hardwarový token bezpečně poskytnout autentizaci uživatele a autorizaci jeho operací, je nutné, aby především on sám byl navržen s ohledem na požadovanou míru bezpečnosti. Ačkoliv se může zdát, že zařízení dostupná v současné době na trhu mají v tomto smyslu obdobné vlastnosti, ani zdaleka tomu tak není.

Útoky na hardwarová zařízení lze rozdělit na fyzický nebo softwarový útok. U softwarového útoku se často využívá nalezené softwarové chyby, která umožní přístup k datům i bez znalosti hesla.

U fyzických útoků se využívají neinvazivní metody, které jsou nejméně náročné. Spočívají často zejména ve změně provozních podmínek zařízení tak, aby se chovalo jiným způsobem, než je obvyklé. Nejznámějším případem jsou změny teploty, ať už podchlazení, nebo přehřátí.

---

[4] Popelka, A. *Metody autentizace sběrové centrály a koncových zařízení* [online]. [cit. 2011-09-20]. Dostupné z WWW: <http://www.ais-brno.cz/vyvoj/zprava_09.pdf?lang=cz>.

[5] Lorenc, V., Matyáš, V. *Autentizační HW a možná vylepšení.* Zpravodaj ÚVT MU, 2007. ISSN 1212-0901.

U invazivní metody se zařízení nejprve rozebere až na samotný čip, odstraní se krycí vrstvy a útočník se následně pomocí speciálního hardwaru, mikroskopů a mikrosond napojí na sběrnici, případně vyčítá data přímo z paměti. Tyto metody patří mezi nejnáročnější na vybavení, už kvůli nutné míře potřebných znalostí i miniaturním rozměrům současných čipů. Proto jsou nejčastěji používány zejména pro čipové karty.

Středně obtížné, přesto však velice účinné, jsou poměrně moderní semiinvazivní postupy. V nich je čip rozebrán jen částečně, obvykle pouze zbaven vrchní vrstvy nebo plastového krycího pouzdra a dále je na něj působeno některým druhem záření, obvykle elektromagnetickým či silným světelným zdrojem. Tento druh útoků je finančně dostupný a potřebné znalosti jsou nižší, než u invazivních útoků.

Semiinvazivní útoky jsou často používány pro útoky na USB zařízení. Jejich velikost je dostatečná na to, aby nebylo nutné používat mikroskopy, a často si při jejich výrobě sami výrobci pomáhají různými testovacími obvody, které pak nedostatečně odstraňují. To vede ke zjednodušení situace při získávání klíčů a jiných citlivých dat uložených na takovýchto zařízeních.[6]

Jádrem čipových karet je čip zastříknutý do plastového obalu. V čipu je integrován kryptografický mikroprocesor, paměťově prostředky a vstupně-výstupní kanály. Mikroprocesor bývá většinou osmibitový. Karty jsou vybaveny třemi typy pamětí.

Požadavky na úroveň zabezpečení specifikuje bezpečnostní norma vydaná Národním institutem standardů a technologií Spojených států (NIST – National Institute of Standarts and Technology). Tato norma stanovuje bezpečnostní požadavky, které musí být splněny, aby čip mohl nést toto označení. Norma nese označení FIPS 140 (Federál Information Processing Standards).

V roce 2001 byla NIST schválena druhá verze této normy FIPS 140-2., která nahrazovala předchozí verzi FIPS PUB 140-1 z roku 1994.

Bezpečnostní požadavky, které tato norma určuje, jsou rozděleny do 11 oblastí a hodnoceny podle čtyř úrovní bezpečnosti s postupně narůstajícími nároky. Následující tabulka popisuje obsah těchto oblasti:

---

[6] Lorenc, V., Matyáš, V. *Autentizační HW a možná vylepšení.* Zpravodaj ÚVT MU, 2007. ISSN 1212-0901.

| FIPS 140-1 | FIPS 140-2 |
|---|---|
| 4.1 Cryptographic Modules | 4.1 Cryptographic Module Specification* |
| 4.2 Cryptographic Module Interfaces | 4.2 Cryptographic Module Ports and |
| 4.3 Roles and Services | 4.3 Roles, Services, and Authentication* |
| 4.4 Finite State Machine | 4.4 Finite State Model |
| 4.5 Physical Security | 4.5 Physical Security* |
| 4.6 Software Security | 4.6 Operational Environment* |
| 4.7 Operating System Security | 4.7 Cryptographic Key Management |
| 4.8 Cryptographic Key Management | 4.8 EMI/EMC |
| 4.9 Cryptographic Algorithms | 4.9 Self-Tests* |
| 4.10 EMI/EMC | 4.10 Design Assurance* |
| 4.11 Self-Tests | 4.11 Mitigation of Other Attacks* |

Tabulka 3.2.5-1: Oblasti normy FIPS.[7]

Odstavce označené * byly zcela přepracovány. Změny vychází ve značné většině z nevyhnutelnosti odpovídat na existenci nových technologií nebo nových bezpečnostních nároků. V odstavci 4.6 dochází k důležité změně v odkazu na hodnocení bezpečnosti informačních systémů. Odstavec 4.11 je nový a jeho obsah spočívá v tom, že metodika zde umožňuje reagovat na řadu kryptografických útoků, které se objevily až v poslední době. Tyto útoky spočívají v analýze spotřeby proudu, časové analýze, analýze vynucených chyb apod.

Norma FIPS 140–2 definuje čtyři stupně (levels) bezpečnostních požadavků:

- Level 1 definuje základní bezpečnostní požadavky, jako je např. použití schválených kryptografických algoritmů apod.
- Level 2 klade nároky na evidenci průniku, autentizace je závislá na rolích.
- Level 3 klade nároky na evidenci průniku a odezvu (destrukce citlivých dat apod.), autentizace je založená na identitách.
- Level 4 definuje nejsilnější bezpečnostní opatření. Protože se předpokládá použití v nezabezpečených prostorech, požaduje silnou fyzickou ochranu a dodržování vnějších pracovních podmínek.

[7] National Institute of Standarts and Technology. *FIPS Publications* [online]. [cit. 2011-09-09]. Dostupné z WWW: <http://csrc.nist.gov/publications/PubsFIPS.html>.

## 3.3 Biometrická autentizace

Biometrie se zabývá zkoumáním živých organismů, především jejich měřitelných fyziologických, anatomických nebo behaviorální vlastnosti. Využití tohoto oboru může spočívat právě ve spolehlivé a rychlé autentizaci osob.

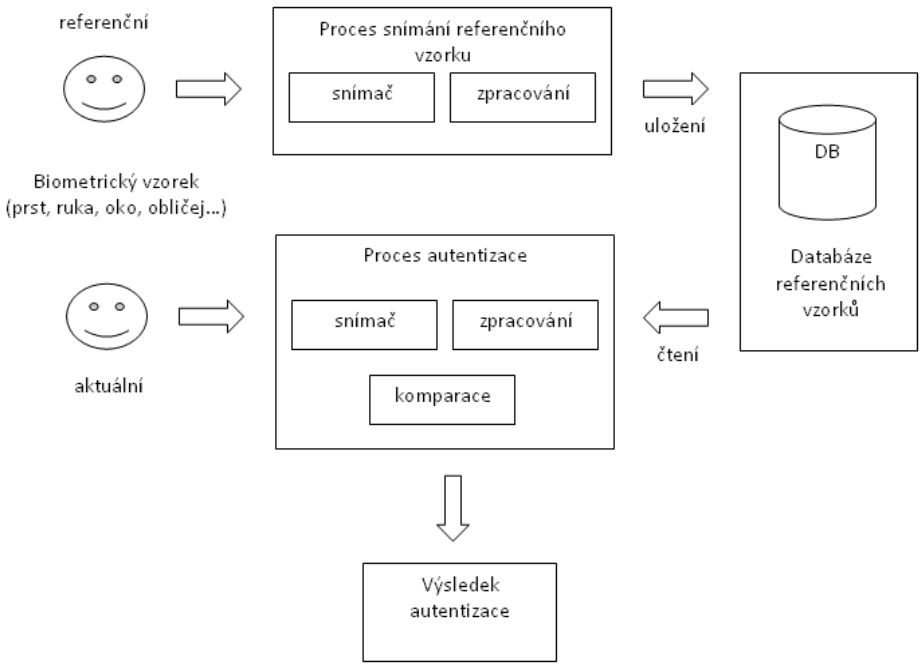
Biometrie je metoda autentizace založená na rozpoznávání unikátních biologických charakteristik živé osoby. Metoda vychází z podmínky, že některé biologické charakteristiky jsou pro každého člověka jedinečné a neměnitelné.

### 3.3.1 Proces biometrické autentizace

Proces autentizace má podobný princip v případě, že se jedná o autentizaci pomocí otisků prstů, rozpoznání oční duhovky nebo další metody.

V procesu inicializace je nutné provést sejmutí, získaní referenčního vzorku a odfiltrování nežádoucích jevů, které by mohly požadovaný výsledek před uložením do databáze referenčních vzorků, zkreslit.

V rámci autentizace se provede opět sejmutí aktuálního vzorku a porovnání s referenčními vzorky, které jsou uloženy v databázi.




Obrázek 3.3.1-1: Proces biometrické autentizace.

### 3.3.2 Otisky prstů

Otisky prstů mají za sebou dlouhou historii s počátky v kriminalistice. Metoda vychází z předpokladu, že každý jedinec má unikátní otisk. Na bříškách prstů

můžeme nalézt tzv. papilární linie, které se formují v různých tvarech. Algoritmus porovnávání otisků prstů má několik fází, ve kterých se tyto tvary porovnávají.

Snímačů prstů je více druhů, které se liší svojí kvalitou a cenou. Nejstarší typy jsou optické, které pracují na principu odrazu světla od papilárních linií. Jsou levné, ale disponují pouze nízkou spolehlivostí.

Vyšší spolehlivost vykazují kapacitní snímače, kde snímaný prst tvoří jednu desku kondenzátoru. Druhou desku tvoří snímací plocha. Protože rýhy nepřiléhají k snímací ploše stejně jako linie, mají nižší kapacitu. Rozdíly v kapacitách vytváří požadovaný obraz otisku prstu. Tento typ snímače je dražší ale podstatně přesnější.

V kvalitních snímačích je integrována tzv. detekce „živosti“, která zabezpečuje, aby prst nebylo možné nahradit jeho replikou. Detekce spočívá v měření teploty, případně pulsu a tlaku. Tato detekce ale může být negativně ovlivněna zdravotními dispozicemi autorizované osoby.

Obrázek 3.3.2-1: Čtečka otisků prstů Čtečka e-DATA TLR401.[8]

### 3.3.3 Oko

**Snímání duhovky**

Velmi spolehlivá metoda autentizace je založena na snímání oční duhovky. Stejně jako otisk prstu je i vzor oční duhovky jedinečný pro každého člověka. Pravděpodobnost nalezení shodného vzorku oční duhovky dvou různých osob je mnohonásobně nižší než u otisku prstu. Duhovky se liší i dvojčat, dokonce se liší obě duhovky jedné osoby. Oční duhovku není možné chirurgicky změnit a zůstává po celý život stejná.

[8] INTO CZ s.r.o. *Čtečka e-DATA LTR401* [online]. [cit. 2011-09-20]. Dostupné z WWW: <http://www.timelink.cz/products/ctecka-e-data-tlr401-cteni-i-zapis-otisku-prstu>.

Zařízením pro skenování oční duhovky je kamera s CCD prvkem. Analogová data z CCD snímače se digitalizují a posléze analyzují speciálním software, který provede zmapování duhovky v závislosti např. na rozšíření oční zorničky. Výsledky analýzy se uloží do databáze.

Protože tato metoda nabízí vyšší spolehlivost je vhodná pro nejkritičtější aplikace autentizace osob, např. v armádních systémech.

**Snímání sítnice**

Pro velmi vysoké bezpečnostní nároky je možné také využít metodu snímání sítnice. Žíly oka jsou u každého jedince odlišné a struktura a žilní schéma zůstává po celý život neměnné. Sítnice je velmi dobře chráněna proti vnějším vlivům prostředí, a proto je velmi vhodná pro biometrické metody autentizace.

Tato metoda není běžné využívána ke komerčním účelům, využívá se pro nejnáročnější aplikace s vysokými nároky na bezpečnost, např. vládní a armádní systémy apod. Z tohoto důvodu není na trhu dostupné žádné zařízení schopné tuto metodu využít.


Obrázek 3.3.3-1: Biometrický snímač oční duhovky LG IrisAccess 4000[9]

### 3.3.4 Geometrie ruky

Rozpoznání je založeno na tvrzení, že lidská ruka je jedinečná. K rozlišení jedinců mezi sebou se používají typické charakteristiky ruky:

- délka prstů,
- šířka prstů,
- výška prstů,

[9] LG Electronics Iris Technology Division. *IrisAccess 4000* [online]. [cit. 2011-09-20] Dostupné z WWW: <http://www.lgiris.com/ps/products/irisaccess4000.htm>.

- zakřivení a lokální anomálie.

Zařízení snímá pouze siluetu ruky, ostatní podrobnosti, jako papilární linie nejsou využívány. Pro nasnímání se používají ortografické snímače, tzn. pohled shora a zboku. Systém lze využít spolehlivě od 8 let věku uživatele. Před tímto věkem nemusí být metoda spolehlivá, z důvodu rychlého vývoje jedince a výrazným změnám geometrie ruky. [10]

V průběhu registrace je nutné provést vícenásobné nasnímání uživatelovy ruky, zpravidla se provádí tři snímání. Ze snímků se průměrem vytvoří šablona. V procesu autentizace zadá uživatel svoji identitu a přiloží svoji ruku na snímač. Výsledkem je buď přijetí, nebo odmítnutí uživatele.

V současné době se pracuje na vývoji metody pracující s 3D povrchem ruky. Hlavním zlepšením je tedy použití celé geometrie ruky oproti pouhé siluetě v případě 2D varianty, čímž se výrazně zvýší míra spolehlivost metody, a bude tudíž možné nasadit výsledné zařízení pro větší počet uživatelů.

Obrázek 3.3.4-1: Čtečka geometrie ruky HandKey II.[11]

Tato metoda má bohužel negativní zdravotní dopad, spočívajících v přenosu nakažlivých chorob, což může významným způsobem podporovat šíření nemocí, zvláště v době epidemií chřipky a podobných nakažlivých nemocí. Další nevýhodou je nespolehlivost způsobená např. kožními chorobami, revmatickými žilami, či obyčejnými prsteny.

Metodu je možné využít v systému, kde je registrováno řádově stovky uživatelů. Při větším počtu již může docházet k chybným vyhodnocením a nesprávným

[10] Vysoké učení technické v Brně, Fakulta informačních technologií. STRaDe [online]. [cit. 2011-09-20]. Dostupné z WWW: <http://strade.fit.vutbr.cz>.

[11] Digitus s.r.o. *Handkey II* [online]. [cit. 2011-09-20] Dostupné z WWW: <http://www.digitus.cz/produkt_handkey2.php>.

autorizacím. Využívá se v systémech s vyšším nárokem na bezpečnost, např. jaderné elektrárny.

### 3.3.5 Další biometrické metody

V současné době probíhá výzkum dalších na biometrii založených metod. Tyto metody jsou ve stádiu vývoje nebo testování a zatím nejsou komerčně využívány. Jedná se především o metody založené na snímání obličeje, snímaní žil nebo metoda založena na analýze DNA.

## 3.4 Vícefaktorová autentizace

Pod pojmem vícefaktorová autentizace rozumíme kombinaci dvou nebo třech faktorů (metod) autentizace. Kombinace více metod autentizace samozřejmě přináší větší míru spolehlivosti a úroveň zabezpečení. Je důležité vhodně zkombinovat jednotlivé metody, tak aby se vzájemně doplňovaly.

Jednotlivé metody můžeme zkombinovat celkem do sedmi různých skupin, které jsou uvedeny v tabulce.

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| Autentizace za pomocí hesla | • | | | • | | • | • |
| Autentizace za pomoci technické pomůcky | | • | | • | • | | • |
| Biometrická autentizace | | | • | | • | • | • |

Tabulka 3.3.5-1: Tabulka skupin vícefaktorové autentizace.

V první skupině A je autentizace pouze za pomocí uživatelského jména a hesla. Tato metoda je nejméně bezpečná, protože je možné heslo zachytit pomocí rezidentních programů, odpozorovat, apod. Výhodou je jednoduchost a levné nasazení této metody a za předpokladu, že uživatel použije dostatečně silné heslo, i dostačující úroveň zabezpečení pro méně významné aplikace, jako např. volně dostupné e-mailové schránky, diskusní fóra, apod.

Do skupiny B patří čipové karty nebo tokeny, bez zabezpečení heslem. Této nevýhody lze zneužít při ztrátě nebo krádeži. Těchto zařízení se běžně využívá při zabezpečení budov v systémech EZS (elektrický zabezpečovací systém), kde nahrazují klasické klíče.

Příkladem ze skupiny C může být snímač otisků prstů, který se hojně využívá i v levnějších počítačových sestavách nebo noteboocích. I tato metoda není bez spojení s další autentizační metodou příliš spolehlivá a účinná.

Další skupiny již představují různé kombinace dvou nebo všech třech metod. Ve skupině D se jedná o kombinaci hesla a technické pomůcky, tzn. především čipové karty nebo tokeny s možností zadání hesla nebo PIN. Do této skupiny spadají v dnešní době asi nejvíce využívané zařízení, jako jsou úložiště šifrovacích klíčů. Do skupiny F patří např. snímač geometrie ruky, který je kombinovaný se zadáním hesla. Skupina G představuje nejsilnější vicefaktorovou autentizaci, kde se využívají všechny tři autentizační metody.

### 3.4.1 Výběr vhodné autentizační metody

Pro výběr vhodné metody je nutné znát základní parametry, které určují cenu, spolehlivost, prostředí a dostupnost dané metody.[12]

- Počet uživatelů - jedním z parametrů, který určuje cenu a dostupnost metody je počet uživatelů, kteří budou daný systém využívat.
- Frekvence využívání – jak často bude uživatel procházet procesem autentizace.
- Prostředí autentizace – v jakém prostředí bude autentizace probíhat, může se např. jednat o veřejné místo, kancelář, domov, apod.
- Kdo se bude autentizovat – jedná se určení schopností uživatelů, kteří budou danou metodu využívat.
- Úroveň zabezpečení – čas a nároky na prolomení dané autentizace.
- Náklady – pořízení zařízení, software a hardware, zprovoznění a náklady na provoz určují celkovou cenu a dostupnost pro koncového zákazníka.
- Začlenění do stávajícího systému – pokud bude systém nasazován do již existujícího systému, bude vhodné využít již použité technologie a vhodně je doplnit.
- Budoucnost – volba vhodné metody z hlediska vývoje autentizačních metod a předpokládané doby využívání autentizačního systému.

Zodpovězení těchto otázek má klíčový vliv na výběr vhodné metody. Každá metoda není vhodná nebo cenově dostupná pro každého uživatele.

[12] Clever and smart. *Jak vybrat vhodnou autentizační metodu* [online]. [cit. 2011-10-16]. Dostupné z WWW:<http://www.cleverandsmart.cz/autentizace-jak-vybrat-vhodnou-autentizacni-metodu/>.

# 4 Digitální certifikáty

Digitální certifikáty slouží pro identifikaci jednotlivých subjektů, které spolu na určitých úrovních digitálně komunikují. Může se jednat o jednoduchou komunikaci za použití e-mailů, kde se použije digitální podpis k ověření identity odesílatele a zároveň potvrzení, že odeslaná zpráva nebyla upravena třetí stranou. Další funkcí je vytváření zabezpečeného spojení v komunikaci serverů a klientů.

## 4.1 Obsah certifikátu

Data v certifikátu jsou popsána jazykem ASN.1. Výhody ASN.1 spočívají v nezávislosti na počítačové platformě a dobré čitelnosti pro člověka. K převodu do binární podoby se používá kódování DER nebo BER a následovně ještě Base64. Soubor s digitálním certifikátem je po otevření zobrazen v čitelné podobě, což umožňuje zkontrolovat údaje o jeho předpokládaném majiteli. Podstatné ovšem je, že všechny tyto formáty a kódy jsou popsány pomocí mezinárodních norem a s takto uloženými certifikáty by měla umět pracovat většina programů, které podporují elektronický podpis, a to i napříč jednotlivými počítačovými platformami. Certifikáty by také měly podporovat běžné operační systémy, při pokusu o otevření souboru s certifikátem, by jej systém měl rozeznat a zobrazit dostupné informace v čitelné podobě. [13]

### 4.1.1 Norma X.509

Norma X.509 specifikuje formát dat pro ukládání a přenos certifikátů, parametry certifikátů a formát dat seznamů odvolaných certifikátů. Norma určuje v jakém formátu je možné certifikáty ukládat, omezení na jednotlivé položky certifikátu apod. Formát vznikl v roce 1988 a vývojem byl postupně doplňován.

Pro tuto normu se používají přípony:

- .DER – zakódovaný certifikát,
- .PEM – certifikát zakódovaný pomocí base64, může obsahovat soukromé klíče,
- .P7B, .P7C – obsahuje certifikáty nebo seznamy odvolaných certifikkátů,

[13] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 173-175.

- .PFX, .P12 – obsahuje certifikáty, veřejné i soukromé klíče chráněny heslem.

V dalších podkapitolách jsou popsány nejdůležitější položky digitálních certifikátů. Příklady uvedené v popisu položek, jsou exportovány ze skutečného certifikátu a zobrazeny za pomocí editoru jazyka ASN.1.

### 4.1.2 Version

Vyjadřuje verzi certifikátu, která je snížena o hodnotu 1, (tj. 0 pro 1, 2 pro 3), pokud se jedná o verzi 1, muže být toto pole vynecháno. Nyní se požívá verze 3.

### 4.1.3 Serial Number

Položka *serialNumber* obsahuje číslo vyjadřující pořadí vydaného certifikátů certifikační autoritou. Musí být kladné celé číslo, jedinečné pro každý certifikát vydaný danou certifikační autoritou. Tato kombinace (pořadové číslo a jméno certifikační autority) jednoznačně identifikuje každý certifikát. Číslo může nabývat značně velkých hodnot, ale nesmí přesahovat 20 bajtů.

Příklad:

```
INTEGER : 10639983
```

### 4.1.4 Subject

Položka *subject* obsahuje jedinečné jméno objektu, kterému je certifikát vydán, identifikuje tedy konkrétního držitele vydaného certifikátu. Pokud má držitel certifikátu vydáno více certifikátu u stejné certifikační autority, je nutné z důvodu zachování podmínky jedinečnosti, rozlišit objekty atributem *serialNumber* nebo *dnQualifier*. Tato položka se plní na základě žádosti o certifikát.

Příklad:

```
SEQUENCE :
SET :
SEQUENCE :
OBJECT IDENTIFIER : countryName [2.5.4.6]
PRINTABLE STRING : 'CZ'
SET :
SEQUENCE :
OBJECT IDENTIFIER : commonName [2.5.4.3]
UTF8 STRING : 'Stanislav Čeleda'
SET :
SEQUENCE :
OBJECT IDENTIFIER : organizationName [2.5.4.10]
UTF8 STRING : 'ČEZ, a.s.'
SET :
SEQUENCE :
OBJECT IDENTIFIER : emailAddress [1.2.840.113549.1.9.1]
IA5 STRING :'stanislav.celeda@cez.cz'
```

### 4.1.5 Issuer

Obsahem této položky je jedinečné jméno certifikační autority. Toto jméno by mělo být v ideálním případě jedinečným v rámci všech certifikačních autorit. Z tohoto důvodu by jméno mělo být vhodně voleno, aby jej nebylo třeba měnit. Změnou jména dojde k vytvoření zcela nové nezávislé autority.

**Distinguished name**

Položky subject a issuer používají stejný datový formát označovaný jako jedinečné jméno (distinguished name).[14]

| Atribut | Zkr. | Význam |
|---|---|---|
| Country | C | Stát podle ISO 3166, tj. podle stejné normy jaká se používá pro top level domény DNS (CZ=Česká republika, SK=Slovensko) |
| State or Province | SP | Nižší organizační jednotka státu. např. spolková země. |
| Locality | L | Místo (např. město) |
| Common Name | CN | Název objektu, pod kterým je místně znám. Např. u osob to může být jméno a příjmení. U serverů pak jejich DNS jméno. |
| Organization | O | Název firmy |
| Organization Unit | OU | Název části firmy |
| Email Address | E | Internetová adresa elektronické pošty. |

Tabulka 4.1.5-1: Atributy jedinečných jmen.

### 4.1.6 Signature Algorithm

Tato položka obsahuje identifikátor kryptografických algoritmů a jejich parametry použité pro podpis certifikátu. Tato položka se skládá ze dvou částí – *algorithm* a *parametrs.*

```
SEQUENCE :
OBJECT IDENTIFIER : rsaEncryption [1.2.840.113549.1.1.1]
NULL : ''
```

### 4.1.7 Validity

V této položce je specifikován časový interval platnosti certifikátu, ve které certifikační autorita ručí za informace v něm uvedené. Je tvořena položkami

[14] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 62.

*notBefore* – datum a čas od kterého je certifikát platný a *notAfter* – datum a čas konce platnosti certifikátu. Platnost je včetně mezních hodnot a je udávána v UTC.

### 4.1.8 Key-Usage

Určuje způsob využití certifikovaného veřejného klíče. Lze jím omezit způsob použití. Obsahuje bitový řetězec, kde každý bit odpovídá konkrétnímu způsobu použití certifikátu. Pokud je příslušný bit nastaven na *TRUE*, je možné certifikát k danému použití využívat.

- digitalSignature – je určen k digitálnímu podpisu, neopravňuje podepisovat certifikáty a CRL,
- nonRepudiation – je určen pro verifikaci digitálně podepsaných dat, neopravňuje podepisovat certifikáty a CRL,
- keyEncipherment – je určen k šifrování klíčů,
- dataEncipherment – je určen k šifrování jiných uživatelských dat,
- keyAgreement – je určen pro algoritmy založené na výměně klíčů,
- keyCertSign – je určen k podepisování certifikátů,
- cRLSign – je určen pro podepisování seznamu odvolaných certifikátů,
- encipherOnly – je určen pouze k šifrování,
- decipherOnly – je určen pouze k dešifrování.

Příklad:

```
SEQUENCE :
OBJECT IDENTIFIER : keyUsage [2.5.29.15]
BOOLEAN : 'TRUE'
OCTET STRING :
BIT STRING UnusedBits:4 : 'F0'
```

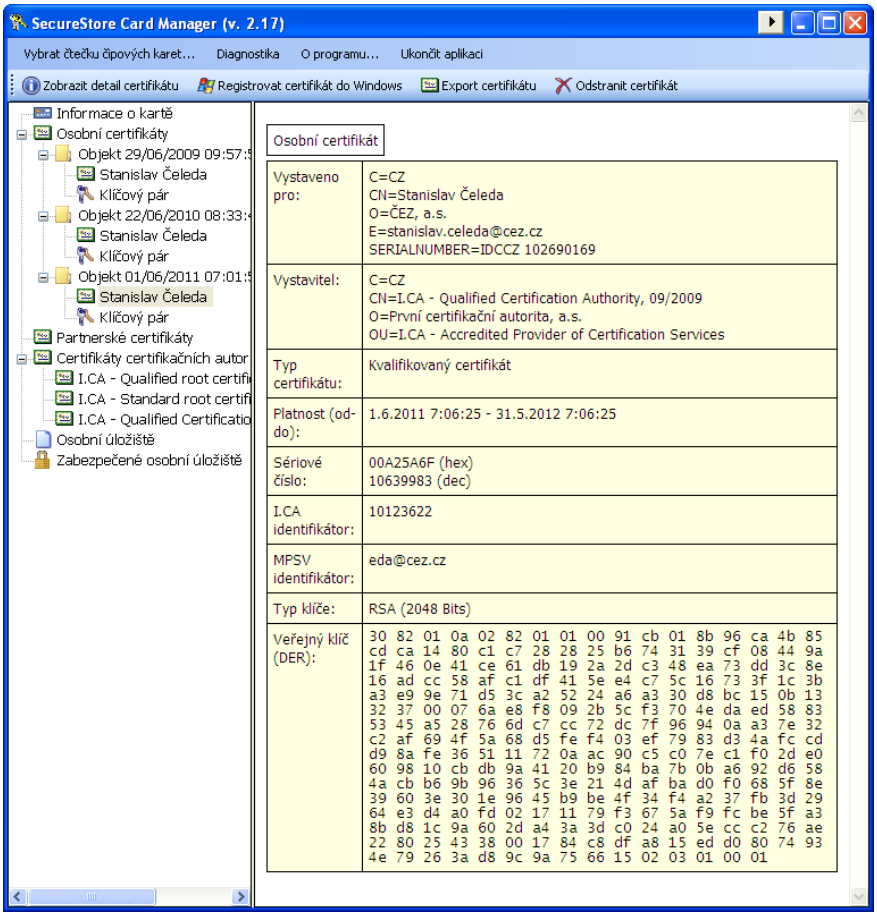
### 4.1.9 Public Key

Položka obsahuje veřejný klíč, který je s tímto certifikátem svázán. Obsahuje identifikátor algoritmu a samotný veřejný klíč. Jeho bitová délka je závislá na druhu použitého šifrování.

Příklad:

```
SEQUENCE :
OBJECT IDENTIFIER : rsaEncryption [1.2.840.113549.1.1.11]
NULL : ''
BIT STRING UnusedBits:0 :
384AA2E5CE2636E90C49DA4E3310F47D4140297446027A654E2C4A59A
B1BE30CFBA75EA271ADD005266658854EF82CC5901ABE8FA410B8304A
E1F172046025A7972F28B01255326C1ACFE4C94BEEB87B4DE5C0BA101
BC1D6D5ED4617E9E628E86382CF2E8162B10C682CE5F49AE1922984C6
```

```
6AFAE84B08605F1AEF4CF5C11FAADB31F4A6F676139A435E651B234C7
11BC878DC7244853EBB9E4AB259E73DECF8395F468E6F45496DE3946B
805C4E493EC08F0A14E468B025487E145BA7C42AA5A5638C6F8E604FA
8A0F9F66E30C1A1391BB62AB14EA2B56B2381D7D4F96A51B0CB89B153
18540B4D9EB5A7645C2C5311D624E9B8F10B396C2E92D7C7D70F8129
```




Obrázek 4.1.9-1: Výpis obsahu certifikátu správcem čipových karet.

## 4.2 Šifrovací algoritmy

### 4.2.1 Symetrické algoritmy

Symetrický algoritmus, někdy také označovaný jako konvenční, využívá k šifrování i dešifrování jediný stejný klíč. Tím se liší od algoritmů s veřejným klíčem, které mají dvojici klíčů – tajný a veřejný. Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost. Symetrické algoritmy pro šifrování jsou mnohonásobně (řády statisíců) rychlejší než asymetrické. Velkou nevýhodou je však

nutnost sdílení tajného klíče, tzn. že uživatelé se musí předem domluvit na tajném klíči a bezpečným způsobem si ho předat. [15]

**DES**

Tato šifra byla vyvinuta již v 70. letech minulého století. Nyní již není považována za spolehlivou, protože používá klíč pouze o délce 64 bitů, z nichž je 8 bitů kontrolních. Algoritmus má další slabá místa, která snižují její bezpečnost. V současné době je tuto šifru možné prolomit už za méně než 24 hodin. Určitým vylepším tohoto algoritmu je tzv. TripleDES, který aplikuje šifru DES třikrát, je však pomalejší než novější algoritmus AES.

**DSA**

Jedním z prvních algoritmů založených na symetrické šifře je DSA (Digital Signature Algorithm). Byl navržen americkým institutem NIST v srpnu 1991. Algoritmus je založen na obtížnosti řešení problému diskrétního logaritmu.

**AES**

Dalším algoritmem blokové symetrické šifry je AES (Advanced Encryption Standard). Šifra využívá 128, 192 nebo 256 bitu dlouhý klíč. Metoda šifruje data postupně v blocích s pevnou délkou 128 bitů. Vyznačuje se vysokou rychlostí šifrování. Zatím není znám žádný případ prolomení této metody.

### 4.2.2 Asymetrické algoritmy

V asymetrických metodách se pro šifrování a dešifrování používají odlišné klíče, to je hlavním rozdílem oproti symetrickým algoritmům.

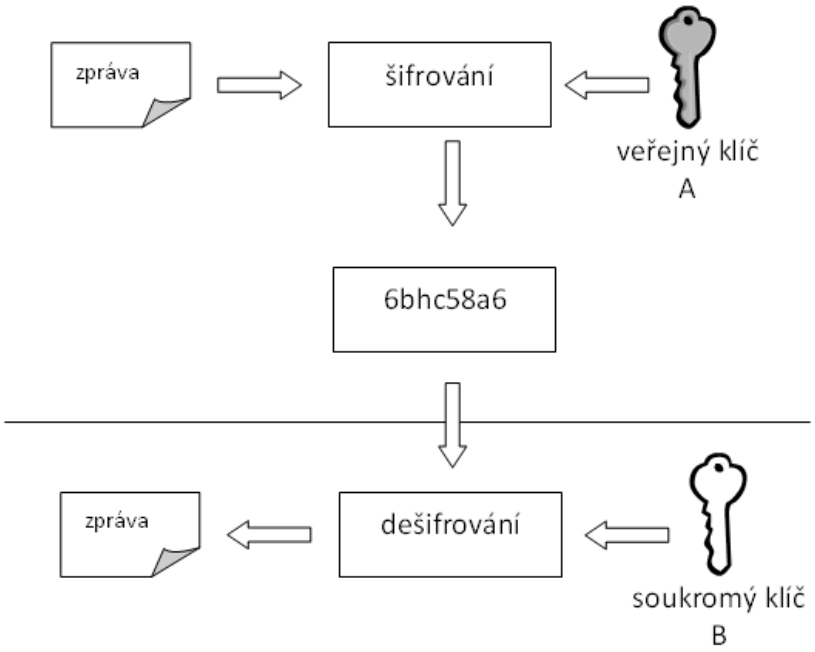
Šifrovací klíč pro asymetrickou kryptografii je složen z dvou částí: první část se používá pro šifrování zpráv. Příjemce zprávy tuto část nemusí znát. Druhá část je určena pro dešifrování a odesilatel šifrovaných zpráv ji nemusí znát. Z toho je patrné, že ten, kdo šifruje, nemusí s dešifrujícím příjemcem zprávy sdílet žádné tajemství. Tím je odstraněna potřeba výměny klíčů, což je hlavní výhodou asymetrické kryptografie.

Nejběžnější verzí asymetrické kryptografie je využívání tzv. veřejného a soukromého klíče: šifrovací klíč je veřejný, majitel klíče ho uveřejní, a kdokoli jím

[15] Dostálek, L., Vohnoutová, M., Knotek, M. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 24.

může šifrovat jemu určené zprávy. Dešifrovací klíč je soukromý, majitel jej drží v tajnosti a pomocí něj může tyto zprávy dešifrovat.

Je zřejmé, že šifrovací klíč A a dešifrovací klíč B spolu musí být matematicky svázány, avšak nezbytnou podmínkou pro užitečnost šifry je praktická nemožnost ze znalosti šifrovacího klíče spočítat dešifrovací.[16]




Obrázek 4.2.2-1: Princip asymetrického šifrování.

V principu se mohou šifrovací a dešifrovací funkce lišit, zpravidla jsou však matematicky přinejmenším velmi podobné.

**RSA**

RSA (iniciály autorů Rivest, Shamir, Adleman) je šifra s veřejným klíčem, jedná se o první algoritmus, který je vhodný jak pro podepisování, tak šifrování. Používá se i dnes, přičemž při dostatečné délce klíče je považován za bezpečný.

Bezpečnost tohoto algoritmu je založena na předpokladu, že rozložit velké číslo na součin prvočísel je velmi obtížná úloha. Z čísla n = pq je tedy v rozumném čase prakticky nemožné zjistit činitele p a q, neboť není znám žádný algoritmus

[16] Wikipedie, otevřena encyklopedie. *Asymetrická kryptografie* [online]. [cit. 2011-10-26]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Asymetrická_kryptografie>.

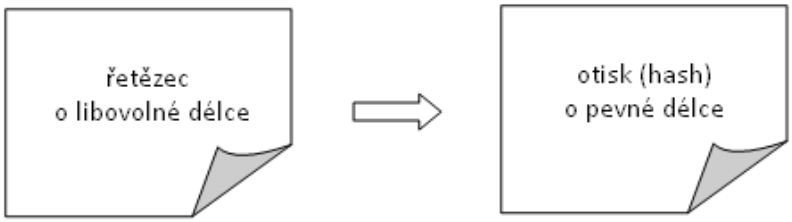
faktorizace, který by pracoval v polynomiálním čase vůči velikosti binárního zápisu čísla n. Naproti tomu násobení dvou velkých čísel je elementární úloha. [17]

Bezpečnost je závislá na výpočetních možnostech a velikosti klíče. Do roku 2002 byla délka klíče 1024 bitů považována za minimum. Po varování RSA, že klíče o délce 1024 bitů mohou být prolomitelné, se přešlo na délku klíče 2048 bitů. Tyto klíče budou dostatečné do roku 2030, poté bude nutné používat klíče o délce minimálně 3072 bitů.

## 4.3 Hašovací funkce

Hash – otisk – je jednocestná funkce, pomocí které je možné vytvořit z libovolně dlouhého řetězce (textu, zprávy…) řetězec konstantní délky. Výsledný řetězec musí maximálně charakterizovat původní řetězec, tzn., že již malá změna (jeden znak, např. číslo 0 v platebním příkazu), způsobí velkou změnu v otisku. Protože se hash počítá z libovolně dlouhého řetězce, je možné ke konkrétnímu otisku nalézt teoreticky nekonečné množství původních řetězců. [18]

Jednocestnou funkcí se rozumí algoritmus, který není výpočetně náročný ale je však velmi výpočetně náročné k výsledku nalézt původní text. Funkce jsou konstruovány na výpočetních operacích o nízké úrovni, např. bitové posuny a operace. Proto jsou velmi rychlé a na výpočet nenáročné. Tyto funkce nemůžeme označit jako šifrovací, už z toho důvodu, že není možné z otisku vytvořit původní text.




Obrázek 4.2.2-1: Vytvoření otisku.

Hašovací algoritmus můžeme označit za bezpečný, pokud je obtížné nebo nemožné

- najít původní řetězec, který odpovídá svému otisku,

[17] Algoritmy.net. *Algoritmus RSA.* [online]. [cit. 2011-10-26]. Dostupné z WWW: <http://www.algoritmy.net/article/4033/RSA>.

[18] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 21-23.

- najít dva stejné řetězce, které mají stejný otisk. Tento stav se nazývá kolize.

Na následujícím příkladu je vidět velká změnu otisku již při změně jednoho znaku v původním řetězci. První řetězec obsahuje slovo: „hodinky“.

Jeho otisk za použití algoritmu SHA-1 vypadá takto:

`73d6761d0a5f272d7b07fcf5890d9f869100855b.`

Již změna jednoho znaku způsobí velkou změnu v otisku. Záměnou jednoho písmene dostaneme „holinky“. Výsledný otisk se změnil takto:

`1367243746df82f9d650718f9e007127441b780b.`

### 4.3.1 MD5

Označením MD5 - Message-Digest algorithm je pojmenován hašovací algoritmus, který byl navržen už v roce 1991. V roce 1996 v něm byla nalezena chyba, která sice nebyla zásadní, ale vedla k postupnému přechodu k algoritmu SHA. Přesto se však ještě používá k ukládání hesel. Tento algoritmus vytváří otisk dlouhý 128 bitů.

### 4.3.2 SHA-0, SHA-1

Hashovací algoritmus SHA - Secure Hash Algorithm byl navržen Národní bezpečnostní agenturou v USA. SHA spojuje skupinu pěti algoritmů, které odlišuje délka výstupního klíče v bitech. Algoritmus SHA se také používá v různých protokolech a aplikacích, jako SSL, SSH a pro kontrolu integrity souborů a komunikace. Varianty SHA-0 a SHA-1 se liší pouze jednou bitovou rotací provedené pomocí jednocestné funkce. Oprava měla zvýšit bezpečnost algoritmu. Oba algoritmy vytváří 160 bitový obraz ze původního řetězce o délce $2^{64}$-1 bitů.

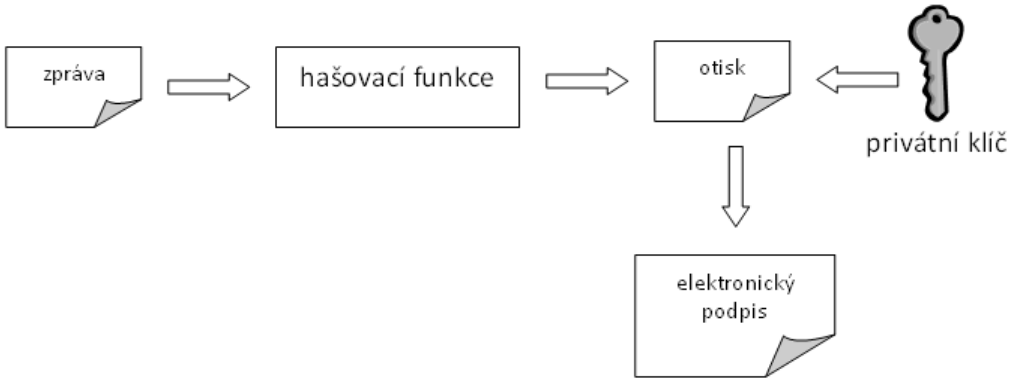
### 4.3.3 SHA-2

Další čtyři hashovací funkce SHA nesou jméno podle délky otisku v bitech: SHA-224, SHA-256, SHA-384 a SHA-512. Všechny tyto algoritmy jsou společně označovány jako SHA-2. Tato verze byla zveřejněna už v roce 2001, ale jejímu širokému používání bránila nedostačená podpora ze strany systému Windows XP. Verze SHA-384 a SHA-512 umožňují zpracovat řetězec o maximální délce $2^{128} – 1$.

### 4.3.4 Princip elektronického podpisu

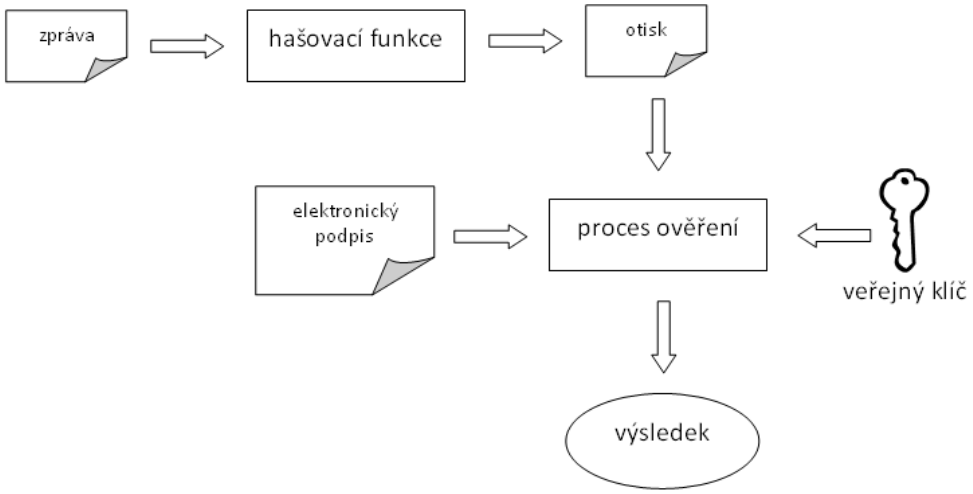
Elektronický podpis se využívá k distribuci zprávy, kdy přímce požaduje identifikaci odesílatele. Podepsání zprávy nemění vlastní zprávu, pouze vytvoří řetězec znaků elektronického podpisu, který je připojen k odesílané zprávě. Nejprve

se z vlastní zprávy vytvoří otisk, který je následně podepsán s využitím privátního klíče odesílatele. Tento proces je ve skutečnosti zašifrování hodnoty otisku privátním klíčem.




Obrázek 4.3.4-1: Princip elektronického podpisu.

Pro vlastní kontrolu je potřeba mít k dispozici vlastní zprávu a elektronický podpis. Nejprve se opět vytvoří otisk ze zaslané zprávy. Veřejným klíčem odesílatele se rozšifruje hodnota otisku, který byla vytvořena při podepisování. Pokud se obě hodnoty shodují, je to důkazem toho, že zpráva, kterou odesílatel odeslal, nebyla změněna. [19]




Obrázek 4.3.4-2: Princip ověření elektronického principu.

[19] Hernady, R. *Zavedení hash algoritmů SHA-2 v prostředí OS Microsoft Windows* [online]. [cit. 2011-10-28]. Dostupné z WWW: <http://www.lupa.cz/clanky/zavedeni-hash-algoritmu-sha-2-v-prostredi-ms-win/>.

## 4.4 Komunikační protokoly

Každá elektronická komunikace musí probíhat podle jasně definovaného komunikačního protokolu. Protokoly specifikují mnoho základních parametrů:

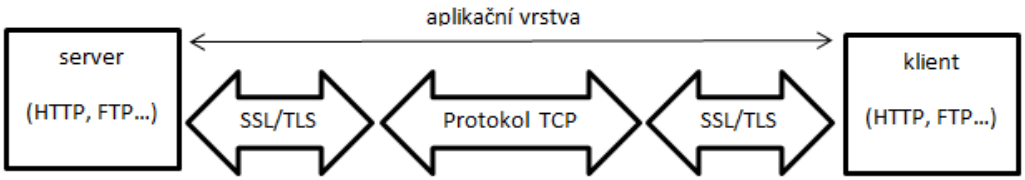
- hardwarové vlastnosti fyzického spojení,
- procesy navazování a ukončování spojení,
- detekce a opravy chyb v komunikaci,
- použité šifrování.

Mezi hlavní a nejčastěji používané komunikační protokoly používané na internetu patří skupina protokolu TCP/IP a dále aplikační protokoly, např. HTTP, FTP, POP3, IMAP, SMTP. Většina těchto protokolů existuje i ve verzi, která umožňuje zabezpečené šifrované spojení. [20]

### 4.4.1 HTTPS

Protokol, který umožňuje spojení mezi webovým serverem a webovým prohlížečem je Hypertext transfer protokol (HTTP), zabezpečená verze HTTPS přenáší data pomocí SSL nebo TLS. Písmeno „S“ značí Secure. Standardním portem na straně serveru je 443.

Protokol HTTPS využívá asymetrické šifrování. Obě strany si před zahájením komunikace vygenerují pár klíčů, vymění si své veřejné klíče a ověří je pomocí otisku veřejného klíče který je digitálně podepsaný důvěryhodnou certifikační autoritou.




Obrázek 4.4.1-1: Znázornění aplikační vrstvy.

### 4.4.2 SSL / TLS

Protokoly SSL (Secure Sockets Layer) a TLS (Transport Layer Security) jsou mezivrstvou vloženou mezi transportní protokol (např. TCP) a aplikační (např. HTTP). Protokol TLS je vyšší verzí protokolu SSL. Oba protokoly však nejsou

[20] Dostálek, L., Kabelová, A. Velký *průvodce protokoly TCP/IP a systémem DNS*, 5. aktualizované vydání. Praha: Computer press, 2008. 488 s. EAN 9788025122365.

kompatibilní! Hlavní rozdíl spočívá v rozdíleném postupu doplňování datových bloků při symetrickém šifrováni.

Hlavním úkolem těchto protokolů je:

- zabezpečit komunikaci šifrováním,
- autentizovat server oproti klientovi,
- autentizovat klienta oproti serveru.

Klient i server mají jistotu, že komunikace probíhá mezi těmi subjekty, se kterými skutečně chtěli komunikovat.

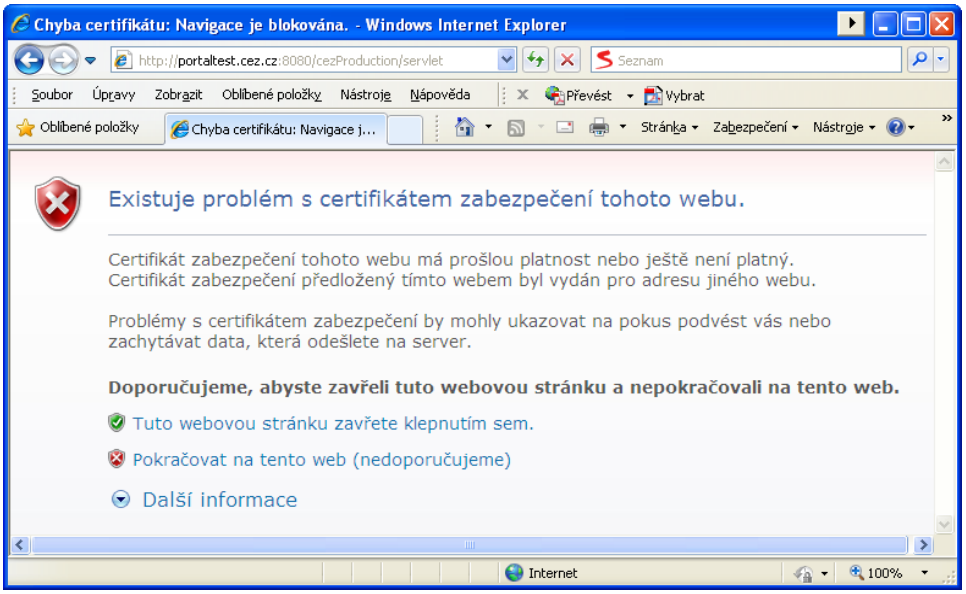
Navazování spojení probíhá v těchto krocích:[21]

- klient pošle serveru výzvu k navázání spojení pomocí protokolu SSL a zvolí vhodný šifrovací algoritmus, který budou používat,
- server odešle klientovi svůj serverový certifikát, který ověří jeho platnost,
- klient vygeneruje tzv. předběžné sdílené tajemství (premaster secret), který zašifruje veřejným klíčem serveru a odešle ho serveru. V případě, že je požadována i autentizace klienta, je odeslán i jeho certifikát,
- klient i server použijí předběžné sdílené tajemství k vytvoření tzv. hlavního sdíleného tajemství (master secret), kterým pak šifrují vzájemnou komunikaci.

Z pohledu uživatele jsou samozřejmě tyto kroky transparentní. Na uživateli je pouze zvolení svého platného certifikátu, v případě, že server požaduje autentizaci klienta.

Další interakcí, která je po uživateli požadována, se týká posouzení důvěryhodnosti serveru, respektive jeho certifikátu. Zde může dojít k problému, že webový prohlížeč nemá ve svém úložišti kořenový certifikát autority, která vydala certifikát serveru. Webové prohlížeče, v tomto případě, ne zcela korektně, prohlásí neznámou certifikační autoritu za nedůvěryhodnou a rozhodnutí o zařazení certifikační autority mezi důvěryhodné ponechají na straně uživatele.

[21] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 381-386.



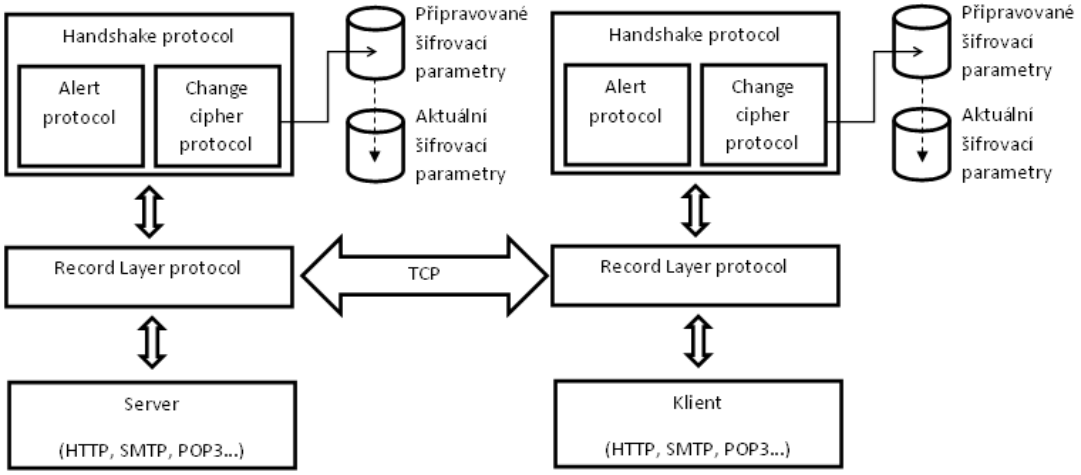

Obrázek 4.4.2-1: Informace o problému s certifikátem.

Protokoly se ve skutečnosti skládají ze dvou dílčích protokolů:

Record Layer Protocol (RLP) – přebírá data od aplikačních protokolů, šifruje je a počítá z nich kryptografický kontrolní součet. Druhý účastník komunikace stejným protokolem dešifruje data, ověří kontrolní součet a předá data aplikačnímu protokolu.

Handshake protocol (HP) – zajišťuje navázání šifrovaného a autentizovaného spojení mezi komunikujícími stranami. Tímto protokolem se obě strany dohodnou na použitých šifrovacích algoritmech a šifrovacích klíčích. Součástí toho protokolu jsou ještě dva pomocné protokoly:

- Change cipher specification protocol – informuje o nastavení nových šifrovacích parametrů,
- Alert protocol – slouží k podávání informací o varováních a chybách.




Obrázek 4.4.2-2: Architektura protokolů SLL / TLS.

Nejdůležitějším protokolem je Handshake protocol kterým se komunikující strany dohodnou na použitém šifrovacím algoritmu a klíči. Klient nejprve pošle serveru zprávu ClientHello, obsahující základní informace o použité verzi, dostupných možnostech šifrování a náhodně generovaná data. Server na tuto zprávu klientovi odpoví zasláním zprávy ServerHello, která obsahuje obdobné informace doplněné o certifikát. Poté mu předá aktivitu zprávou ServerHelloDone. Po ověření totožnosti serveru klient může volitelně prokázat svou identitu zasláním vlastního certifikátu, ale vždy musí reagovat zprávou ClientKeyExchange, která zahrnuje náhodná data šifrovaná veřejným klíčem serveru. Po provedení právě popsaných kroků nic nebrání započetí šifrované komunikace. Pokud již bylo spojení mezi klientem a serverem v minulosti vytvořeno, nemusí již probíhat celý proces znovu, ale lze provést obnovení spojení pomocí identifikátoru existující relace.[22]

## 4.5 Druhy certifikátů

### 4.5.1 Komerční certifikát

Jedná se o nejrozšířenější druh certifikátu. Jsou to takové certifikáty, které nejsou spjaty se zákonem o elektronickém podpisu. Vystavuje jej certifikační autorita, která ověří žadatele dle svých vlastních směrnic. Tento druh certifikátů nemusí dodržovat náležitosti zákona o elektronickém podpisu a je jen na dané certifikační autoritě jaké si stanoví podmínky. Komerční certifikáty mají velmi široké uplatnění. Tím, že není ze strany zákona na tento druh certifikátu kladen žádný

[22] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 391-401.

požadavek, je dána volnost v jejich využití. Komerční certifikáty lze využít k těmto nejčastějším účelům:

- autentizace – přihlášení uživatelů pomocí certifikátu,
- zajištění šifrované komunikace – např. šifrované SSL spojení,
- ověření elektronických podpisů.

Komunikující strany však musí důvěřovat danému certifikátu dané certifikační autority. Tento certifikát je totiž vydáván bez jakýchkoliv legislativních záruk.

Komerční certifikáty mohou být vystavovány jak osobám, tak i technologickým celkům jako jsou servery, aplikace a další zařízení.

### 4.5.2 Kvalifikovaný certifikát

Kvalifikovaný certifikát může vydávat pouze akreditovaná kvalifikovaná certifikační autorita, jejíž bezpečnost a důvěryhodnost je kontrolována a standardizována příslušnými úřady a řídící se zákonem o elektronickém podpisu podle §12 zákona č. 227/2000 Sb. Jedná se o standardní digitální certifikát, který je však uvedeným zákonem uznáván v rámci komunikace se státními institucemi České republiky. Z tohoto hlediska musí být akceptován stejně jako občanský průkaz avšak možnosti jeho využití v současné době jsou omezeny pouze na tyto případy:

- komunikace elektronickou cestou se státní správou pomocí emailu,
- pro bezpečné ověřování elektronických podpisů,
- zajištění neodmítnutelnosti odpovědnosti.

To znamená, že tyto certifikáty jsou určeny výhradně pro elektronické podepisování (nikoliv například pro šifrování). Lépe řečeno kvalifikovaný elektronický podpis zajišťuje integritu a autenticitu dat pro oficiální komunikaci se subjekty státní správy, pojišťoven apod.

Podle zákona č. 227/2000Sb, §12 musí kvalifikovaný certifikát splnit následující náležitosti: [23]

§ 12 Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,

[23] Ministerstvo vnitra. *Portál Veřejné správy České republiky* [online]. [cit. 2011-10-08]. Dostupné z WWW: <http://portal.gov.cz>.

b) 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,

c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,

d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,

e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,

f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává,

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

h) počátek a konec platnosti kvalifikovaného certifikátu,

i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,

j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám.

(3) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

Ministerstvo vnitra uděluje akreditaci na základě splnění těchto podmínek:[24]

- splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona č. 227/2000 Sb., (zákon o elektronickém podpisu);
- splnění podmínek, požadavků a postupů stanovených vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o

[24] Ministerstvo vnitra. *Přehled udělených akreditací* [online]. [cit. 2011-10-08]. Dostupné z WWW: <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>.

požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb);

- ověření kvalifikovaných systémových certifikátů Ministerstvem vnitra podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu.

Seznam subjektů, kterým byla udělena akreditace ministerstva vnitra je dostupná na WWW: http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx.

### 4.5.3 Serverové certifikáty

Serverový certifikát je umístěn na webovém (poštovním a jiném) serveru a klient má možnost jej autentizovat. Certifikát tím zaručuje, že server je skutečně provozován organizací, která má právo jméno uvedené v certifikátu provozovat. Klient má jistotu, že komunikuje se správným serverem. Webový server si také může vyžádat certifikát klienta a provést jeho autentizaci. Tuto vzájemnou autentizace umožňuje protokol SSL. Popis tohoto protokolu je součástí této práce.

Tyto certifikáty jsou vydávány jak fyzickým, tak i právnickým osobám na základě řádné elektronické žádosti o certifikát, zpravidla vytvořené přímo příslušným serverem, kterou žadatel předloží společně s požadovanými doklady totožnosti na vybraných registračních autoritách.

### 4.5.4 Kvalifikované systémové certifikáty

Kvalifikované systémové certifikáty jsou kvalifikovanými systémovými certifikáty vydanými akreditovaným poskytovatelem certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu. Kvalifikované systémové certifikáty tvoří samostatnou kategorii certifikátů odlišnou od kvalifikovaných certifikátů (bez přívlastku systémový). Tyto certifikáty jsou určeny k bezpečnému vytváření a ověřování elektronických značek. Označujícím subjektem (tvůrcem elektronické značky) může být nejen fyzická osoba, ale i právnická osoba nebo orgán státní správy či samosprávy. Elektronickou značku je možno vytvářet automatizovaně (např. v elektronických podatelnách pro potvrzování doručení podání).[25]

Kvalifikovaný systémový certifikát slouží zejména pro automatizované systémy, které využívají technologii založenou na principech elektronického podpisu bez

[25] I.CA a.s. *Kvalifikovaný systémový certifikát* [online]. [cit. 2011-10-09]. Dostupné z WWW: <http://www.ica.cz/Kvalifikovany-systemovy-certifikat.aspx>.

součinnosti konkrétní fyzické osoby (např. elektronická fakturace, hromadné zasílání e-mailů, doručenek e-podatelny apod.).

Použití kvalifikovaného systémového certifikátu je v souladu s platnou legislativou vázáno na specializované hardwarové zařízení.

Kvalifikované systémové certifikáty, lze používat pro:

- vytváření elektronické značky,
- ověřování elektronických značek,
- bezpečné ověřování elektronických značek,
- zajištění nepopiratelnosti (vazba mezi dokumentem a subjektem vytvářející elektronickou značku).

## 4.6 Kvalita certifikátů

Stejně jako je tomu u jednotlivých autentizačních metod, je i kvalita certifikátu určena několika důležitými faktory.

- Důvěryhodnost certifikační autority, respektování zákona o elektronickém podpisu podle §12 zákona č. 227/2000 Sb., reference apod.
- Kvalita kryptografických algoritmů využitých k vytvoření digitálního certifikátu. S ohledem na rostoucí výpočetní výkon a klesající odolností použitých algoritmů, je nutné využívat stále silnější kryptografické metody a omezovat dobu platnosti digitálního certifikátu.
- Chování uživatele, který certifikát využívá. Neproškolený nebo nedbalý uživatel může celý proces znehodnotit např. vložením falešného kořenového certifikátu. Obsluha by měla být dostatečně proškolena.

## 4.7 Vytvoření certifikátu

Vytvoření certifikátu předchází vytvoření žádosti o certifikát. Žádost o certifikát by měla obsahovat:[26]

[26] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 79-86

- Identifikační údaje žadatele o certifikát - tyto údaje budou uvedeny ve výsledném certifikátu v „předmětu“ případně v položce „rozšíření certifikátu“.
- Veřejný klíč a identifikace asymetrického algoritmu, ke kterému je veřejný klíč určen.
- Důkaz o vlastnictví soukromého klíče.
- Doplňující údaje, které si žadatel přeje do certifikátu doplnit, např. použití klíče.
- Pokud se jedná o placenou službu, obsahuje také žádost potřebné fakturační údaje.
- Hesla pro komunikace s certifikační autoritou, např. heslo pro odvolání certifikátu.

Důkaz o vlastnictví soukromého klíče je prokázán skutečností, že žádost je elektronicky podepsána tímto soukromým klíčem, který odpovídá veřejnému klíči obsaženému v žádosti. Formát a způsob předání žádosti je definováno certifikační politikou certifikační autority.

Nejběžnějším formátem žádosti o certifikát je žádost podle normy PKCS#10. Tento formát je podobný kořenovému certifikátu, ale obsahuje pouze potřebné položky pro vytvoření žádosti. Žádost musí obsahovat tyto údaje:

| Verze |
|---|
| Předmět |
| Veřejný klíč |
| Atributy |
| Elektronický podpis soukromým |

Tabulka 4.5.4-1: Položky žádosti o certifikát.

Položka Atributy obsahuje rozšíření, která žadatel chce mít ve výsledném certifikátu. Tento formát nelze použít pro žádost o certifikát, jehož veřejný klíč neumožňuje ověření digitálního podpisu. Také nelze využít pro případ, kdy párová data jsou generována až certifikační autoritou.

Příznivějším formátem pro podávání žádosti je formát CRMF (Certificate Request Message Format), který řeší problémy formátu PKCS#10. Navíc je doplněn o další informace, např. fakturační údaje.

Speciální formát SPK je vytvořen společností Netscape a je určen pro vytváření žádostí prostřednictvím webových stránek. Pomocí HTML tagu <KEYGEN> webový

prohlížeč zajistí vygenerování páru klíčů, vytvoření digitálního podpisu veřejného klíče soukromým klíčem a vložení kódovaného veřejného klíče a jeho podpisu do obsahu HTML stránky. Tento formát však není běžně podporován ze strany certifikačních autorit.

Protokol CMC využívá certifikační autorita v prostředí operačního systému Windows Server 2008. Dovoluje vytvořit žádost, která obsahuje více podpisů, např. podpis pomocí klíče žadatele a podpis pomocí klíče registrační autority.

Takto vytvořená žádost je předána certifikační autoritě, která ověří zadaná data a sestaví obsah certifikátu. Certifikát je předán žadateli většinou ve formátech DER, PEM nebo TXT.

Vydaný certifikát je po převzetí umístěn do seznamu vydaných certifikátů a jsou zveřejněny tyto údaje:

- sériové číslo certifikátu,
- doba platnosti,
- držitel (položka Subject),
- certifikát ve formátu DER, PEM a TXT.

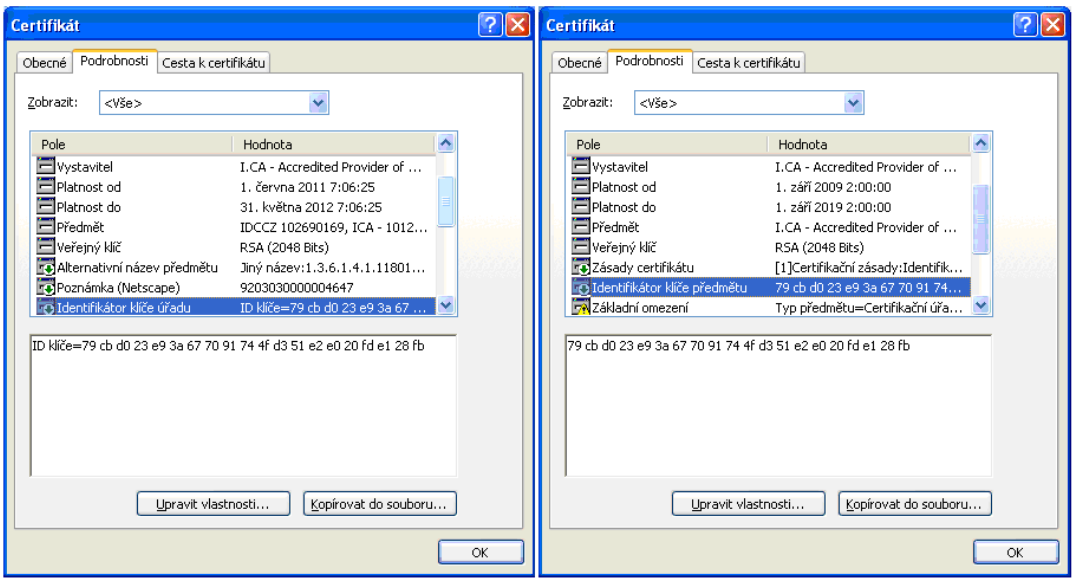
## 4.8 Ověření a platnost certifikátů

Certifikát je nutné ověřit a zjistit, zda veřejný klíč uvedený v certifikátu je platný a patří uvedenému majiteli, a zda tento klíč je může být využit k danému účelu. Za tímto účelem se vytvoří certifikační cesta až k důvěryhodné kotvě, kterou bývá kořenový certifikát. Z tohoto certifikátu se použije jméno vydavatele a veřejný klíč, včetně použitého algoritmu. Při ověřování postupujeme od kořenového certifikátu po certifikační cestě a ověřujeme:

- vydavatele certifikátu,
- platnost certifikátu v daném čase,
- certifikát není odvolán, není uveden na seznamu odvolaných certifikátů,
- účel použití, ke kterému byl certifikát vydán.

V tomto procesu probíhá „párování“ konkrétních certifikátů v certifikační cestě. První položkou, kterou je nutné spárovat je subjekt u nadřízeného certifikátu a vydavatel u podřízeného certifikátu. Nejvýznamnějším identifikátorem je soukromý klíč. Tento klíč samozřejmě není v žádném z obou certifikátů obsažen, ale najít zde můžeme alespoň jeho jednoznačný identifikátor, který je určitým způsobem odvozen z otisku soukromého klíče. Tento identifikátor bývá obsažen u

„podřízeného“ certifikátu v položce Identifikátor klíče úřadu a u „nadřízeného“ certifikátu v položce Identifikátor klíče předmětu.




Obrázek 4.5.4-1: Nadřízený certifikát, v tomto případě kořenový certifikát certifikační autority a podřízený certifikát.

Pokud neselhalo ověřování žádného certifikátu v certifikační cestě až k ověřovanému certifikátu, můžeme jej prohlásit za platný.

Sestavení a ověření certifikační cesty je poměrně složitá procedura a je samozřejmě úkolem pro speciální software. Toto ověřování probíhá automaticky bez přímého zásahu uživatele.

## 4.9 Odvolání certifikátu

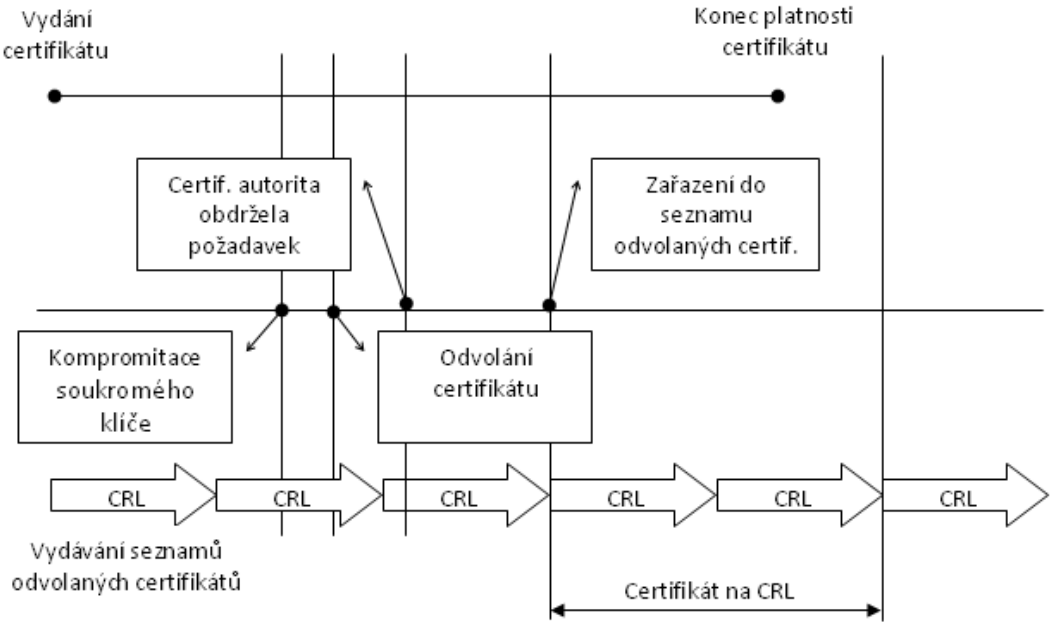
Certifikát může pozbýt planosti několika způsoby. Obvyklým způsobem je vypršení platnosti certifikátu, tzn., uplyne čas *notAfter* uvedený v certifikátu. Před tímto časem však může být certifikát odvolán nebo může být pozastavena jeho platnost. Pokud je certifikát odvolán, je zařazen do seznamu odvolaných certifikátů (CRL - certificate revocation list) a to po celou dobu původně uváděné platnosti. Seznamů odvolaných certifikátů může být více druhů, liší se množinou uváděných certifikátů. [27]

[27] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 87-89

- úplný seznam – obsahuje seznam všech odvolaných certifikátu, jejichž původní platnost dosud nevypršela,
- rozdílový seznam – obsahuje pouze certifikáty, které byly odvolány od posledního vydaného úplného seznamu,
- částečný seznam – obsahuje seznam podle zvoleného dalšího kritéria.

Podání žádosti o odvolání certifikátu může být provedena několika způsoby. Nejjednodušší formou je přímá osobní účast majitele odvolávaného certifikátu. Další formou je podání žádosti o odvolání a podepsání soukromým klíčem odvolávaného certifikátu. Těžko najdeme důvod, proč by útočník použil právě zcizený certifikát k jeho odvolání. Poslední možností je, pokud ji certifikační autorita dovoluje, odvolání pomocí jednorázového hesla, které bylo stanoveno při vytváření certifikátu.

Samotná doba provedení revokace je závislá od doby, za kterou se kompromitovaný certifikát dostane na seznam odvolaných certifikátů od podání žádosti o odvolání. Tento čas je určen certifikační autoritou a její periodou vydávání seznamu odvolaných certifikátů.




Obrázek 4.5.4-1: Proces odvolání certifikátu.

Ve skutečnosti však nedochází často ke kompromitaci soukromého klíče, častějším důvodem pro odvolání certifikátu je např. ukončení pracovního poměru zaměstnance, který certifikát vlastnil.

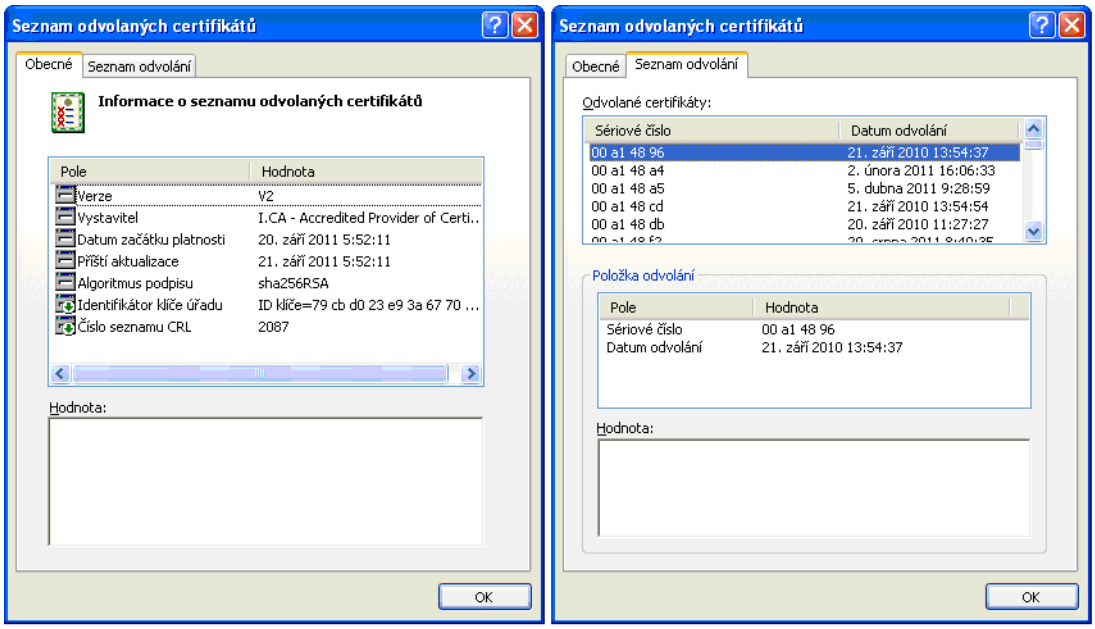
Odvolání platného certifikátu může také provést samotná certifikační autorita, např. v případě, že se objeví žádost o vydání certifikátu s již vydaným veřejným klíčem, nebo v případě, že údaje uvedené v certifikátu již nejsou platné.

### 4.9.1 Seznam odvolaných certifikátů

Seznam odvolaných certifikátů si můžeme představit jako vývěsku certifikační autority, kde pravidelně zveřejňuje odvolané certifikáty. Tento seznam většinou vydávají samotné certifikační autority, případně tímto úkolem mohou pověřit jinou certifikační autoritu. Odvolané certifikáty jsou v seznamu specifikovány svým pořadovým číslem. Forma CRL je dána normou X.509 a obsahuje tyto položky:[28]

- Verze: podle specifikace musí být použita a musí mít hodnotu 1.
- Algoritmus podpisu: vyjadřuje, jakým algoritmus byl použit pro podpis CRL.
- Vydavatel: identifikace vydavatele seznamu.
- Čas vydání: specifikace, kdy byl tento seznam vydán.
- Předpokládány čas vydání následujícího CRL: upřesňuje nejpozdější vydání příštího seznamu, následující seznam může být vydán dříve, ale ne později, než zde uvedený čas.
- Odvolané certifikáty: seznam odvolávaných certifikátů, které jsou specifikovány následujícími údaji:
    - pořadové číslo,
    - datum a čas podání žádosti o odvolání certifikátu,
    - rozšíření týkající se odvolávaného certifikátu.
- Položka Rozšíření CRL, která je nepovinná a je v ní specifikován identifikátor klíče úřadu, číslo seznamu CRL a je také možné určit, zda se jedná o rozdílový seznam, apod.

[28] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 90-93.




Obrázek 4.9.1-1: Okno Seznamu odvolaných certifikátů ve Windows a okno podrobného výpisu odvolaných certifikátů.

### 4.9.2 On-line zjišťovaní platnosti certifikátu

Další ale méně využívanou možností je on-line zjišťování stavu certifikátu za pomocí protokolu OCSP – On line Certificate Status protocol. V tomto případě se uživatel (prostřednictvím aplikačního SW) dotáže serveru poskytujícím tyto informace a získá odpověď o platnosti určitého certifikátu. Toto řešení má několik výhod, zejména aktuálnost seznamu odvolaných certifikátů. Seznam udržuje certifikační autorita v aktuální podobě, není nutné čekat na další pravidelné vydání seznamu CRL. Objem přenášených dat je podstatně menší, přenáší se pouze informace o jednom konkrétním certifikátu na rozdíl od úplného seznamu všech odvolaných certifikátu v případě CRL.

## 4.10 Obnovení certifikátů

Důvodů pro obnovení certifikátu může být více. Uživatel by si mohl přát obnovit svůj certifikát, který byl zneplatněn, protože byl zdiskreditován jeho soukromý klíč a certifikát se již objevil v seznamu zneplatněných certifikátů (CRL). Tuto možnost však žádná spolehlivá certifikační autorita z bezpečnostních důvodů nenabízí a není potřeba se tímto problém dále zabývat.

Každý certifikát má svou dobu platnosti, která je jasně definována položkou *Validity* a parametry *notBefore* a *notAfter* obsažených v digitálním certifikátu. A právě vypršení této lhůty je důvodem pro obnovení jeho platnosti. Tuto činnost můžeme přirovnat k výměně občanského průkazu. Pokud vlastníte (svůj) občanský

průkaz, kterému končí platnost, stačí navštívit příslušný úřad, který vám vystaví nový průkaz. Pokud však již pozbyl platnosti, musíte svou totožnost doložit dalšími dokumenty.

### 4.10.1 Obnovení certifikátu koncového uživatele

Obnovení certifikátu koncového uživatele probíhá podle podobného principu jako u občanského průkazu. Pokud má uživatel k dispozici platný certifikát pak [29]

- jeho identifikace byla již provedena při vystavování původního platného certifikátu,
- autentizaci může provést např. na základě digitálního podpisu vytvořeného pomocí starých ale platných párových dat,
- Navíc se provede důkaz o držení nového soukromého klíče.

Pokud však již starý certifikát pozbyl platnosti, je nutné provést všechny kroky, jako v případě vydání prvního certifikátu. Tzn. dostavit se na registrační autoritu, předložit všechny dokumenty potřebné pro prokázání své totožnosti. Této situaci se snaží certifikační autority předcházet včasným upozorněním uživatelů, např. emailem o blížícím se konci platnosti jejich certifikátu. Uživatel má dost času na obnovení svého certifikátu pomocí starého certifikátu a je ušetřen návštěvy certifikační autority.

### 4.10.2 Obnovení certifikátu certifikační autority

Platnost certifikátu je určena nejen pro uživatele ale také pro samotné certifikační autority. Pro certifikační autoritu platí podmínka, aby platnost certifikátu certifikační autority neskončila dříve, než platnost koncového uživatele. V takovém případě by nastala situace, kdy uživatel vlastní platný certifikát, který je však podepsán již neplatným certifikátem certifikační autority.

Certifikační autorita tak má po poměrně dlouhou dobu dva certifikáty, které se překrývají. Někteří uživatelé mají svůj certifikát podepsán starým certifikátem a jiní novým certifikátem certifikační autority. Oba certifikáty budou mít stejný předmět. Budou se lišit pořadovým číslem a veřejným klíčem. V certifikátu uživatele je v položce Vydavatel (Issuer) uveden předmět z certifikátu certifikační autority,

[29] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 117.

kterým je certifikát uživatele podepsán. A ten je pro nový i starý certifikát certifikační autority stejný. [30]

Doba platnosti certifikátu je kompromisem mezi bezpečností a častým obnovováním certifikátu certifikační autority. Pokud je zvolena dlouhá doba platnosti, hrozí bezpečnostní riziko kryptografické nedostatečnosti párových dat. Pokud je platnost příliš krátká je nutné často obnovovat certifikát certifikační autority. Při rozhodování se přihlíží k aktuálnímu stavu výpočetních možnosti, potřebných k prolomení šifrování a účelu certifikátu. Doba platnosti je jiná u komerčních a kvalifikovaných certifikátů.

[30] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 118-119.

# 5 Certifikační autority

## 5.1 Činnost certifikační autority

Činnost certifikační autority můžeme přirovnat k činnosti notáře, který ověřuje klasický vlastnoruční podpis. Zatímco notář ověřuje každý jednotlivý podpis, certifikační autorita neověřuje vlastní podpis, ale data pro vytváření digitálního podpisu. Potom je již možné využívat certifikát neomezeně. Prvotní postup je však velice podobný, certifikační autorita musí ověřit totožnost žadatele, čímž potvrzuje pravdivost údajů, které jsou svázány s příslušným certifikátem. Žadatel o digitální certifikát proto musí předložit potřebné dokumenty, které stvrzují uvedené skutečnosti. Fyzická osoba se zpravidla prokazuje občanským průkazem případně pasem. Právnická osoba předložením výpisu z obchodního rejstříku.

Certifikační autorita vydává digitální certifikáty, které představují elektronicky podepsané veřejné šifrovací klíče, které obsahují identifikační údaje svého majitele, za jejichž správnost se certifikační autorita zaručila. Na základě principu přenosu důvěry tak můžeme důvěřovat údajům uvedeným v digitálním certifikátu za předpokladu, že důvěřujeme samotné certifikační autoritě.

## 5.2 Důvěryhodnost certifikátu a certifikační autority

Posouzení důvěryhodnosti certifikační autority není lehkým úkolem, zvláště v případě, kdy nemáme dostatek informací. Prvním krokem by měla být návštěva webových stránek certifikační autority, o jejíž služby máme zájem. Podrobně je potřeba prostudovat popis nabízených služeb a podmínky jejich poskytování. Míru důvěryhodnosti můžeme posoudit také podle mechanizmu ověřování údajů žadatele o certifikát. Dalším zdrojem informací může být tisk, diskusní fóra a zkušenosti dalších uživatelů. Také by nás měla zajímat dostupnost, technická podpora, nápověda. Tímto srovnáním se bude zabývat další kapitola.

Hlavním dokumentem, který přesně specifikuje služby, certifikační autority je tzv. certifikační politika, která obsahuje tyto informace:

- úplný výčet nabízených služeb,
- informace o struktuře vydávaných certifikátů,
- možnosti použití vydaných certifikátů,
- postupy práce souvisejícími s životním cyklem certifikátů,
- zásady nakládání s certifikáty,

- vymezení odpovědnosti zainteresovaných osob.

## 5.3 Proces vydání a použití certifikátu

### 5.3.1 Počáteční ověření identity

Při ověřování identity právnické osoby vyžadují certifikační autority předložení ověřené kopie výpisu obchodního rejstříku, živnostenského listu nebo dalšího dokladu, který musí obsahovat:

- obchodní jméno,
- identifikační číslo (IČ),
- adresu sídla,
- jména osob oprávněných k zastupování.

V případě doménového jména serveru se požaduje hodnověrně doložený souhlas vlastníka nebo čestné prohlášení žadatele o certifikát, potvrzující vlastnictví doménového jména.

Fyzické osoby předkládají následující údaje:

- celé jméno,
- datum narození, nebo rodné číslo,
- číslo dokladu (např. občanského průkazu),
- adresa trvalého bydliště.

Tyto údaje se prokazují předložením platného občanského průkazu, cestovního pasu nebo jiným dokladem stejné právní váhy.

### 5.3.2 Ověření identity v žádosti o následný certifikát

Identifikace a autentizace žadatele o vydání následného certifikátu je prováděna ověřením zaručeného elektronického podpisu žádosti o vydání následného certifikátu. V procesu ověřování elektronického podpisu žádosti o následný certifikát musí být použit platný certifikát, ke kterému je vydáván tento následný certifikát. Není možné akceptovat žádost o následný certifikát podepsaný zneplatněným nebo s prošlým obdobím platnosti certifikátu. V tomto případě je nutné provést stejné ověření jako při počátečním ověřování.

### 5.3.3 Zneplatnění certifikátu

Žádost se o zneplatnění certifikátu může bát podána několika způsoby.

- Osobní předání žádosti, kde žadatel prokazuje vlastnictví certifikátu, např. občanským průkazem.
- Elektronicky podepsaná zpráva příslušným soukromým klíčem certifikátu, který má být zneplatněn.
- Prostřednictvím webového formuláře příslušné certifikační autority, která certifikát vydala.
- Pomocí datové schránky.
- Elektronicky nepodepsanou zprávou, obsahujícím heslo pro zneplatnění certifikátu.

## 5.4 Významné české certifikační autority

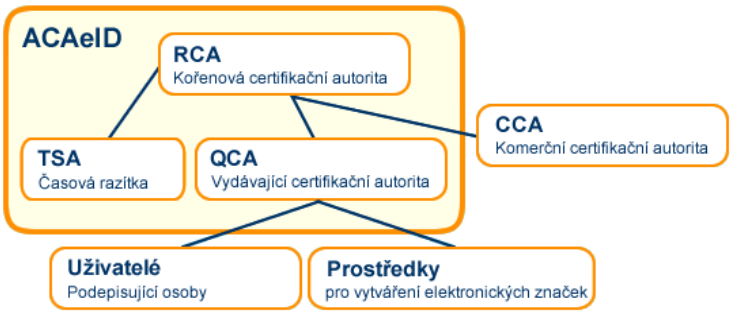
Aktuální udržovaný seznam celosvětových certifikačních autorit je možné nalézt na adrese http://www.tractis.com/countries. Pokud se zaměříme na české certifikační autority, najdeme tyto společnosti, které se vydáváním digitálních certifikátu zabývají:

- APCS identity, a. s., (ACAeID),
- Česká pošta, s. p., (PostSignum),
- První certifikační autorita, a.s., (I.CA).

### 5.4.1 eIdentity

**Akreditované služby**

Jedním ze základních nabízených produktů je poskytování certifikačních služeb fyzickým a právnickým osobám i technologickým komponentám. Společnost eIdentity a.s. provozuje více certifikačních autorit.




Obrázek 5.4.1-1: Znázornění certifikačních autorit v hierarchii APCS identity.[31]

ACAeID je tvořena kořenovou certifikační autoritou (RCA) a autoritou vydávající kvalifikované a kvalifikované systémové certifikáty pro podepisující a označující osoby (QCA). RCA vydává kvalifikované systémové certifikáty pouze podřízeným certifikačním autoritám (tedy i QCA a CCA). QCA vydává kvalifikované certifikáty a kvalifikované systémové certifikáty jednotlivým žadatelům. Kořenová certifikační autorita (RCA) vydala kvalifikovaný systémový certifikát pro autoritu vydávající kvalifikovaná časová razítka (TSA).

**Komerční služby**

Pro účely šifrování, identifikace, ale také pro vytváření a ověřování elektronických podpisů v oblasti běžné komerční komunikace lze využít elektronických certifikátů, vydaných Komerční certifikační autoritou (CCA). Tato certifikační autorita vydává také elektronické certifikáty pro technologické komponenty informačních systémů (např. pro webové servery či servery elektronické pošty, zabezpečeně komunikující pomocí SSL/TLS).

**Podpora uživatelů prostřednictvím webové prezentace**

Webové stránky nabízí přesný postup při typických činnostech jako je obnovení nebo zneplatnění certifikátu. Dále je možnost technické podpory pomocí elektronické pošty nebo webového fóra. Dostupná je také služba pro vyhledávání vydaných kvalifikovaných i komerčních certifikátů. Vyhledávání je možné podle emailové adresy, sériového čísla i podle subjektu certifikátu.

Samozřejmostí je možnost stažení zneplatněných certifikátů ve formátu CRL.

**Vytvoření žádosti**

Vytvoření žádosti je možné online pomocí webové aplikace. V procesu pořízení certifikátu je potřeba projít několik kroků:

[31] Identity a.s. *Popis poskytovaných služeb* [online]. [cit. 2011-10-10]. Dostupné z WWW <http://www.eidentity.cz/ServicesDescription.html>.

- 1. fáze - Vytvoření zákaznického účtu: registrace a založení zákaznického účtu, zvolení přihlašovacího jména a hesla.
- 2. fáze – Zákaznický účet: zákaznický účet obsahuje osobní údaje, seznam rozpracovaných objednávek a poskytnutých služeb s možností jejich objednání. Součástí seznamu jsou i informace o stavu, ve kterém se ta která položka nachází. Je zde také možné požádat o zneplatnění certifikátu a o změnu osobních údajů.
- 3. fáze - Objednání služby: doplnění požadovaných údajů a objednaných služeb, formální kontrola a vydání návrhu smlouvy. Po platbě je uvolněna možnost generování páru klíčů a volba termínu návštěvy registračního místa.
- 4. fáze - Návštěva Registračního místa: doložení pravdivosti uvedených údajů, pořízení kopií dokladů. Pokud je vše v pořádku následuje vydání certifikátu.

**Online podpora**

Dotazy prostřednictvím emailu nebyly zodpovězeny ani po opakované urgenci. Při telefonickém kontaktu operátor poskytl potřebné informace.

**Registrační místa**

Společnost v současné době provozuje tři registrační místa:

- Vodičkova 681/18, Praha 1,
- Vinohradská 184, Praha 3,
- Bechyňská 639, Praha 9 – Letňany.

Registrační místa jsou omezena pouze a hlavní město, uživatelé v jiných oblastech republiky jsou odkázáni na mobilní registrační autority, což přináší další vícenáklady na pořízení certifikátu.

Dále je možné využit služeb mobilní registrační autority v určeném čase a místě na žádost objednatele.

**Reklamace**

Podmínky pro reklamace nejsou přesněji specifikovány. Podle informace infolinky podléhají platným zákonům České republiky.

**Ceny**

| | |
|---|---|
| Kvalifikovaný osobní certifikát | 474 Kč / rok |
| Kvalifikovaný systémový certifikát | 3480 Kč / rok |
| Komerční osobní certifikát | 354 Kč / rok |
| Komerční serverový certifikát | 1074 Kč / rok |
| Cena prodloužení platnosti vydaného certifikátu | Stejná jako první vydání |
| Zneplatnění certifikátu | Zdarma |
| Vydání certifikátu mobilním operátorem registrační autority | Podle počtu vydaných certifikátů |
| Technická podpora | Zdarma |
| Zákaznická telefonická linka | Zpoplatněna podle tarifu |
| Školení | Podle počtu uživatelů |
| Zřízení klientské certifikační autority | Nenabízí |

Tabulka 5.4.1-1: Tabulka parametrů.

**Významní zákazníci**

Společnost nezveřejňuje seznam svých významných zákazníků.

**O společnosti**

Společnost byla založena v roce 2004, akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb získala 12. září 2005.[32]

- Sídlo: eIdentity a.s., Vinohradská 184, Praha 3
- Email: info@eidentity.cz nebo info@ie.cz
- Web: http://www.eidentity.cz nebo http://www.ie.cz.

### 5.4.2 PostSignum

**Akreditované a komerční služby**

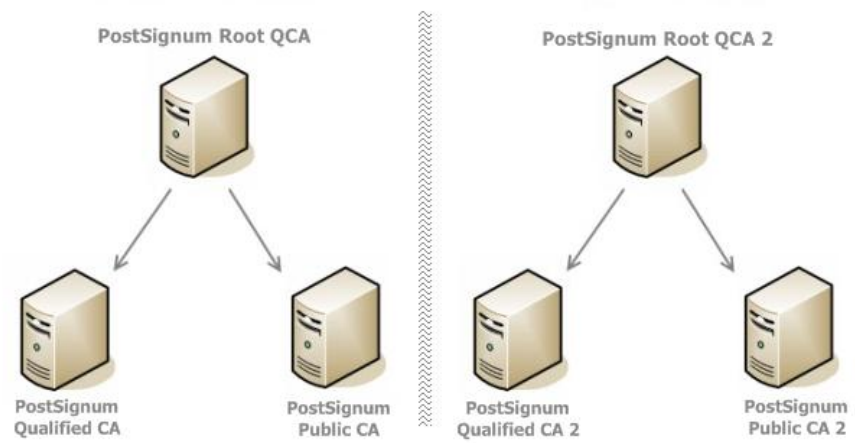
Kořenem stromu jsou autority PostSignum Root QCA (SHA 1) a PostSignum Root QCA2 (SHA 256), které vydaly kvalifikované systémové certifikáty pro podřízené certifikační autority, které již vydávají certifikáty koncovým zákazníkům:

- PostSignum Qualified CA tato autorita již certifikáty nevystavuje,
- PostSignum Public CA vydávající komerční certifikáty SHA 1,

[32] Ministerstvo vnitra. *Přehled udělených akreditací* [online]. Praha: 2010, aktualizováno 21.5.2010. [cit. 2011-10-11]. Dostupné z WWW: <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>.

- PostSignum Qualified CA2 vydávající kvalifikované certifikáty SHA 256,
- PostSignum Public CA2 vydávající komerční certifikáty SHA 256.

Jádro všech tří certifikačních autorit je založeno na software UniCERT od firmy CyberTrust. Dále jsou používány specializované aplikace navržené a vyvinuté společností ICZ, a.s.




Tabulka 5.4.2-1: Znázornění certifikačních autorit v hierarchii PostSignum.[33]

**Podpora uživatelů prostřednictvím webové prezentace**

Webové stránky jsou rozděleny podle typu osob, které žádají o vydání certifikátu na:

- fyzické osoby,
- podnikatelé,
- firmy a organizace,
- veřejná správa.

Pro každý typ žadatele je jasně definovaný postup. Stejně tak jsou zde popsány podrobně kroky pro obnovení nebo zneplatnění certifikátu. Také je zde k dispozici poměrně rozsáhlý seznam častých otázek (FAQ), ve kterém lze snadno dohledat řešení běžných problémů. Velmi dobře je zpracována sekce „Příručky a návody“, kde jsou popsány typické postupy instalace certifikátů do nejčastěji používaných mailových klientů a další práce s certifikáty, např.:

- instalace kořenového certifikátu PostSignum Root QCA,

[33] Česká pošta s.p. *Technické řešení* [online]. [cit. 2011-10-12]. dostupné z WWW: <http://www.postsignum.cz/technicke_reseni.html>.

- záloha soukromého klíče,
- obnova soukromého klíče ze zálohy po generování žádosti o certifikát,
- záloha certifikátu v aplikaci Internet Explorer.

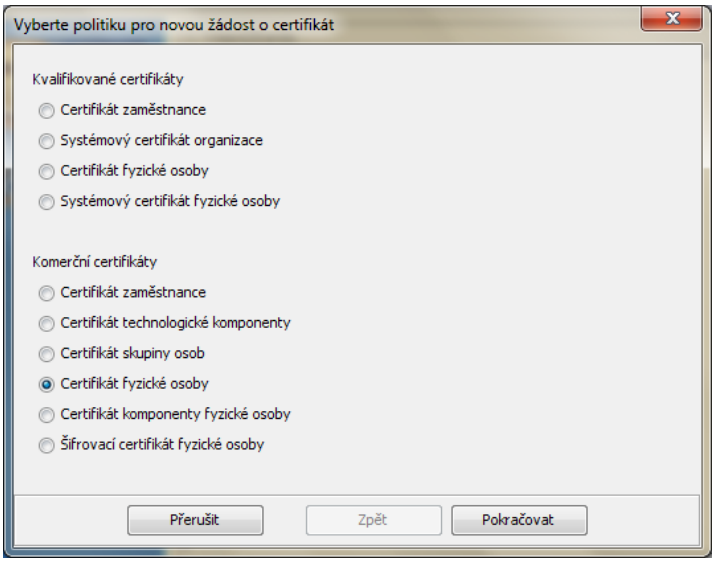
Je zde možnost dohledání platného certifikátu podle sériového čísla nebo podle emailové adresy. Není možné vyhledávat podle subjektu certifikátu.

Stažení zneplatněných certifikátů je možné i s omezením na časové rozmezí.

**Vytvoření žádosti**

Vytvoření žádosti je možné prostřednictvím webové aplikace, je podporován pouze Internet Explorer. Další možností je off-line žádost pomocí aplikace PostSignum Tool, která je k dispozici pro Windows XP, Vista, 7 (i 64 bitová verze) dále pro operační systémy Linux a MAC OS. K dispozici jsou i uživatelské příručky.

V prvním kroku uživatel zvolí typ požadovaného certifikátu.




Obrázek 5.4.2-1: Výběr typu certifikátu v programu PostSignum Tool.

V dalším kroku je potřeba vyplnit požadované údaje v závislosti na vybraném typu certifikátu. Na závěr se vytvoří klíče a žádost je uložena do souboru *.req ve formátu PEM nebo DER.

**Online podpora**

Dotazy prostřednictvím emailu nebyly zodpovězeny ani po opakované urgenci. Při telefonickém kontaktu bylo přislíbeno zpětné zavolání, které skutečně proběhlo, a operátor poskytl požadované odpovědi na otázky, které byly původně zaslány emailem.

**Registrační místa**

Žadatel o certifikát může využít kteroukoliv pobočku České pošty se službou Czech POINT, které v současné době čítají bezmála 1000 poboček. Na stránkách certifikační autority je k dispozici úplný seznam poboček s adresou a otvírací dobou.

Při osobní návštěvě jedné z poboček uvedených v seznamu, mi bylo doporučeno dohodnout se na konkrétním termínu, kdy bude možné žádost o certifikát přijmout, případně navštívit jinou „specializovanou" pobočku.

**Reklamace**

Reklamace se podává pomocí emailu nebo osobně na kterékoliv pobočce. V žádosti je potřeba uvést sériové číslo certifikátu a popis důvodu k reklamaci. Reklamace je vyřízena nejpozději do 14 dnů od podání žádosti.

**Ceny**

| | |
|---|---|
| Kvalifikovaný osobní certifikát | 396 Kč / rok |
| Kvalifikovaný systémový certifikát | 1788 Kč / rok |
| Komerční osobní certifikát | 348 Kč / rok |
| Komerční serverový certifikát | 800 Kč / rok |
| Cena prodloužení platnosti vydaného certifikátu | Stejná jako první vydání |
| Zneplatnění certifikátu | Zdarma |
| Vydání certifikátu mobilním operátorem registrační autority | Mezi 1180 – 1600 Kč, podle počtu vydaných certifikátů. |
| Technická podpora | Zdarma |
| Zákaznická telefonická linka | Zpoplatněna podle tarifu |
| Školení | Podle počtu uživatelů |
| Zřízení klientské certifikační autority | Nenabízí |

Tabulka 5.4.2-2: Tabulka parametrů.

**Významní zákazníci**

Společnost nezveřejňuje výčet svých významných zákazníků.

**O společnosti**

Česká pošta, s. p. se stala akreditovaným poskytovatelem certifikačních služeb dne 15. července 2005.[34] Certifikační autorita Postsignum poskytuje služby vydávání

[34] Ministerstvo vnitra. *Přehled udělených akreditací* [online]. Praha: 2010, aktualizováno 21.5.2010. [cit. 2011-10-12]. Dostupné z WWW: <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>.

kvalifikovaných, komerčních certifikátů a poskytování kvalifikovaného časového razítka.

- Sídlo: Politických vězňů 909/4, Praha 1
- Email: info@cpost.cz nebo helpdesk-ca@cpost.cz
- Web: http://www.postsignum.cz

### 5.4.3 První certifikační autorita

**Akreditované a komerční služby**

Společnost nabízí také několik „balíčků“, kde se jedná o různé kombinace kvalifikovaných a komerčních certifikátů, včetně hardwarového řešení:

- Twins je kombinací kvalifikovaného a komerčního certifikátu,
- produkt „e-Já“ je dvojice komerčního a kvalifikovaného certifikátu doplněna o čipovou kartu s obslužnou aplikací,
- produkt I. CA Premium je navíc doplněn o USB token,
- zřízení klientské certifikační autority.

Poslední zmíněná služba přestavuje dodání a zprovoznění kompletní klientské certifikační autority přímo u zákazníka. Certifikační autorita je postavena na software, který vyvinula společnost sama. Zákazník má po zřízení klientské certifikační autority vydávání vlastních certifikátů i ostatní služby (vydávání CRL, ověřování identity žadatele při nové žádosti o certifikát…) ve své režii. Po celou dobu trvání smluvního vztahu mezi klientem a společností má zákazník přednostní technickou podporu a možnost kontaktovat V.I.P. help-desk společnosti.

**Podpora uživatelů prostřednictvím webové prezentace**

Sekce podpora je rozdělena do několika částí:

- časté dotazy,
- návody,
- aplikace ke stažení,
- ovladače HW,
- legislativa.

Zde je možné nalézt odpovědi na nejčastější otázky (FAQ), jak technického charakteru, tak i z oblasti metodiky, např. jak obnovit certifikát, nebo jak nainstalovat certifikát.

V Návodech je možné získat velké množství nejčastěji prováděných činnosti souvisejících s vydáním a následným používáním certifikátů. Je zde velmi široká podpora webových prohlížečů i mailových klientů. Připravené postupy velmi detailně popisují krok za krokem např. Žádost o certifikát, Zálohování privátního klíče apod.

V sekci Ovladače HW jsou k dispozici ovladače pro hardwarové vybavení, např. čtečky čipových karet, nebo USB tokenů.

Velmi užitečné aplikace pro práci s digitálními certifikáty je možné najít v sekci Aplikace ke stažení. Jsou zde aplikace pro správu čipových karet, tvorbu žádostí o certifikát offline, klientská aplikace umožňující získání časového razítka a aplikace která je určena pro tvorbu a obnovu kvalifikovaných certifikátů. Ke každé aplikaci je dostupná uživatelská příručka.

V sekci Legislativa je možné stáhnout aktuální nejvýznamnější normy pro činnost akreditovaného poskytovatele certifikačních služeb:

- zákon č. 227/2000 Sb., o elektronickém podpisu,
- vyhláška č. 378/2006 Sb. ze dne 19. 7. 2006,
- směrnice Evropského parlamentu a Rady 1999/93/ES.

**Vytvoření žádosti**

Uživatel má možnost vytvořit žádost o nový certifikát prostřednictvím webové aplikace případně po instalaci pomocného programu. V obou případech je vyplnění žádosti jednoduché a přehledné. U položek formuláře je připravena nápověda. Uživatel má možnost si vybrat druh certifikátu a úložiště privátního klíče. V další části vyplní informace o žadateli a heslo pro zneplatnění. Po odsouhlasení zadaných údajů je vygenerována žádost ve formátu PEM a uložena do souboru *.req. S touto žádostí a potřebnými doklady se musí uživatel dostavit na pracoviště registrační autority.

**Online podpora**

Odpověď na dotaz položený emailem byla doručena první pracovní den, po odeslání dotazu. Při telefonickém kontaktu poskytl operátor odpovědi na otázky a doporučil vhodná řešení problémů. V případě dotazu na poskytování OCSP, slíbil předání dotazu specialistovi, který se vzápětí sám ozval a poskytl chybějící informaci.

**Registrační místa**

Společnost disponovala velkým množstvím registračních autorit, které provozovala prostřednictvím svého partnera. V současné době provozuje registrační autority samostatně a jedná se o přibližně 35 míst, většinou v krajských městech. Vyhledávání nejbližší registrační autority je možné podle jednotlivých krajů České republiky. U všech autorit je uvedena kontaktní adresa, email, telefon a provozní doba pobočky.

**Reklamace**

Reklamaci je možné podat pomocí emailu, doporučenou poštovní zásilkou nebo osobně v sídle společnosti. V reklamaci je nutné uvést číslo smlouvy, číslo příjmového dokladu a výstižný popis závady. Reklamace bude vyřízena nejpozději do jednoho měsíce ode dne uplatnění reklamace. Nový certifikát bude uživateli poskytnut zdarma v případě kompromitace dat certifikační autority, nebo v případě, kdy při generování nové žádosti bude zjištěno, že existuje certifikát se stejným veřejným klíčem.

**Ceny**

| | |
|---|---|
| Kvalifikovaný certifikát | 495 Kč / rok |
| Kvalifikovaný systémový certifikát | 780 Kč / rok |
| Komerční certifikát | 395 Kč / rok |
| Komerční serverový certifikát | 1170 Kč / rok |
| Cena prodloužení platnosti vydaného certifikátu | Stejná jako první vydání |
| Zneplatnění certifikátu | Zdarma |
| Vydání certifikátu mobilním operátorem registrační autority | 6000 Kč |
| Technická podpora | Zdarma |
| Zákaznická telefonická linka | Zpoplatněna podle tarifu |
| Školení | Podle počtu uživatelů |
| Zřízení klientské certifikační autority | 100 000 – 150 000 Kč |

Tabulka 5.4.3-1: Tabulka parametrů.

**Významní zákazníci**

Mezi významné zákazníky patří:

- ČSOB Pojišťovna – možnost zabezpečené komunikace mezi pojišťovnou a klienty, platby pojistného,
- ČSOB, a.s. – podpora služby Internetbanking 24,
- Kraj Vysočina – provozování klientské certifikační autority,

- Státní tiskárna cenin - provozování klientské certifikační autority,
- T-Mobile Czech republic a.s. – elektronická fakturace,
- Ministerstvo financí – využívání časových razítek,
- několik dalších, např.: Ministerstvo zahraničních věcí, Narodný bezpečnostný urad SR, Agentura pro podporu podnikání a investic Czechinvest.

**O společnosti**

zahájila poskytování služeb v roce 1996 jako součást produktového portfolia společnosti PVT, a.s. Postupně přerostla hranice projektu a počátkem roku 2001 byla založena dceřiná společnost PVT, a.s., s názvem První certifikační autorita, a.s. Tato společnost převzala od mateřské společnosti veškeré činnosti, které bezprostředně souvisejí s poskytováním certifikačních služeb. I. CA získala jako první v České republice osvědčení pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu. Akreditace byla udělena dne 15. března 2002.[35] V roce 2006 získala akreditaci také pro vydávání kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. Rovněž v roce 2006 získala společnost akreditaci pro vydávání kvalifikovaných certifikátů a pro poskytování služby časové autority na Slovensku.

Počty vydaných certifikátů jsou dnes evidovány řádově ve statisících. Podle informací help-desku společnosti se průměrně jedná o 170 – 190 tisíc vydaných certifikátů ročně.

- Sídlo: Podvinný mlýn 2178/6, Praha 9 – Libeň
- Email: info@ica.cz
- Web: www.ica.cz

## 5.5 Vlastní certifikační autorita

Pokud služby nabízené certifikační autoritou nevyhovují potřebám uživatelů, je další možností vystavění vlastní certifikační autority. Existuje několik možných řešení:

- zřízení klientské certifikační autority „na klíč“,

[35] Ministerstvo vnitra. *Přehled udělených akreditací* [online]. Praha: 2010, aktualizováno 21. 5. 2010. [cit. 2011-10-14]. Dostupné z WWW: <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>.

- využití open source software,
- využití komerčních produktů.

Vybudování vlastní certifikační autority má samozřejmě smysl jen u společností, kde se množství vydaných certifikátů pohybuje v řádech tisíců. Jedná se především o banky, obchodní společnosti a samozřejmě ve školství.

### 5.5.1 Samostatná kořenová certifikační autority

Samostatná kořenová certifikační autorita je postavena na kořenovém certifikátu, který si sama podepsala. Výhoda této možnosti spočívá, v nezávislosti na pravidlech nadřízené certifikační autority. Nepotřebuje certifikát vydaný nadřízenou certifikační autoritu. Velkou nevýhodou však je, že certifikát takové certifikační autority není uložen v konfiguraci operačního systému a webového prohlížeče. Je tedy na každém uživateli, který nechce být vyrušován potvrzováním upozornění, že certifikační autorita není důvěryhodná, aby do svého prohlížeče importovat certifikát certifikační autority.

### 5.5.2 Podřízená certifikační autorita

Podřízená certifikační autorita je podepsána certifikátem nadřízené certifikační autority. Pokud je tato nadřízená certifikační autorita uvedena v seznamu důvěryhodných kořenových certifikačních autorit, nemusí uživatel provádět import certifikátu certifikační autority a autorita je automaticky vedena jako důvěryhodná. Další výhodou této možnosti může být záruka v případě chybného vydání certifikátu a vzniku škody. Využívání této výhody je podmínkou dodržování pravidel, která si stanovuje nadřízená certifikační autorita. Např. podmínky ověřování identity žadatele, technického zabezpečení apod.

Toto řešení samozřejmě přináší i vyšší náklady na zřízení certifikační autority spojené s vydáním certifikátu od nadřízené certifikační autority.

### 5.5.3 Zřízení klientské certifikační autority

Tuto službu mohou využít zákaznici, kteří nemají dostatek znalostí nebo nedisponují silnou podporou ze strany IT. Služba zahrnuje kompletní dodání technického i softwarového řešení „na klíč“. Po zprovoznění a otestování je celá certifikační autorita ve správě zákazníka, který si sám řídí všechny kroky spojené se správou certifikační autority:

- příjem žádostí o certifikát,
- ověření správnosti a úplnosti žádosti,
- ověření identity žadatele,

- vydání certifikátu,
- udržování databáze vydaných certifikátů,
- příjem žádostí o zneplatnění certifikátu,
- udržování a vydávání seznamu zneplatněných certifikátů.

Toto službu nabízí např. společnost I. CA, která dodává nejen technické řešení (server), ale samozřejmě i software. V případě společnosti I. CA se jedná o speciální software, který je jejich produktem. Cena takové služby se pohybuje mezi 100 – 150 tisíci Kč (bez DPH). Platbu je možné rozložit do více let formou pronájmu zařízení.

### 5.5.4 Komerční produkty

Komerční produkty pro komplexní správu certifikační autority představují poměrné nákladná řešení a jsou proto vhodná pro větší organizace nebo společnosti, která preferují vysokou úroveň spolehlivosti a zabezpečení před cenou. Typickým uživatelem mohou být banky nebo armáda.

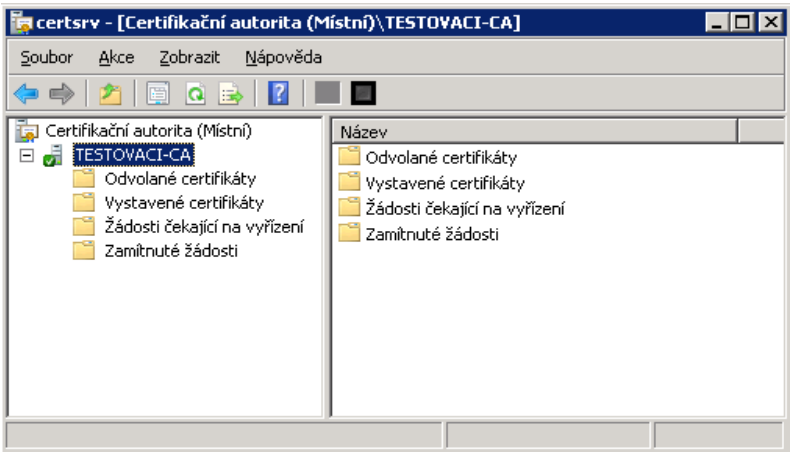
Nejznámějšími komerčními produkty pro správu digitálních certifikátů jsou řešení RSA Certificate Manager, Entrust PKI, Baltimore uniCERT a další. Tyto produkty integrují moduly, které plní základní úkoly:

- správa digitálních identit uživatelů,
- správa životního cyklu digitálního certifikátu,
- automatizace správy šifrovacích klíčů a digitálních podpisů,
- řízení procesů registrace a zpracování žádosti o vydání certifikátu,
- archivace a obnovení uživatelských klíčů.

### 5.5.5 Certifikační autorita Microsoft

Operační systém Windows Server disponuje službou, jejíž pomocí lze vytvořit certifikační autoritu, která:

- přijímá žádosti o certifikáty,
- ověřuje informace uvedené v žádostech a totožnost žadatelů,
- vystavuje certifikáty,
- zneplatňuje certifikáty a vydává seznam zneplatněných certifikátů.




Obrázek 5.5.5-1: Správa certifikační autority v operačním systému Windows Server

### 5.5.6 Certifikační autorita na bázi Open source

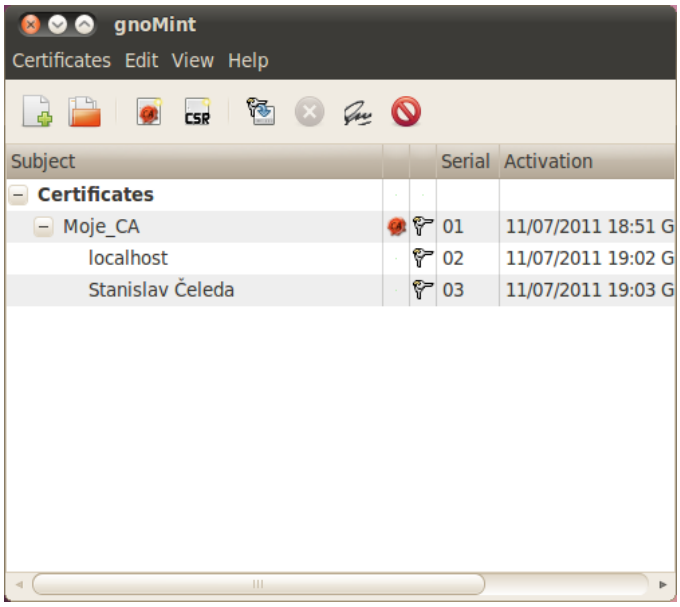
OpenSSL je multi-platformní open source implementace protokolů SSL a TLS. Knihovny systému jsou napsány v jazyce C, je však možné jej provozovat v prostředí jazyka Java.

Z domovských stránek http://www.openssl.org je možné získat zdrojové kódy pro různé operační systémy, ať už jsou to unixové systémy tak i pro systémy Microsoft.

OpenSSL je možné používat dvěma způsoby. Buďto jako utilitu příkazové řádky pro provádění kryptografických operací anebo jako knihovnu (API) pro využití v dalších aplikacích.

### 5.5.7 Certifikační autorita v operačním systému Linux

V operačním systému Linux lze pro vytvoření certifikační autority a správu digitálních certifikátů využít aplikaci gnoMint, která je volně dostupná na stránkách http://gnomint.sourceforge.net/ při dodržení licenčních podmínek GNU/GPL. Je možné volit verzi pro distribuci Linux Fedora Core, Debian nebo Ubuntu. V této práci je praktické odzkoušení provedeno pod operačním systémem Linux Ubuntu 10.04 a nejaktuálnější verzí aplikace gnoMint 1.2.1.




Obrázek 5.5.7-1: Grafické prostředí aplikace gnoMint.

Práce probíhá v plně grafickém rozhraní, k dispozici je jednoduché menu, kterým lze provést veškeré úkony související s vytvořením certifikátu certifikační autority a samozřejmě certifikátů klientských i serverových. Dále je možné provést revokaci vystaveného certifikátu a vygenerovat seznam zneplatněných certifikátů.

## 5.6 Hodnocení služeb

### 5.6.1 Vstupy pro komparaci

Vstupem pro komparaci parametrů jsou informace získané analýzou činnosti certifikačních autorit, studiem jejich webových prezentací a především certifikačních politik. Každý vstupní parametr je navíc ohodnocen svou váhou, která udává důležitost parametru. Váhy jsou v rozsahu 1 - 3, kdy nejvyšší váha má také nejvyšší stupeň závažnosti.

Váha se stupněm 3 je nejvyšší a je přiřazena pouze parametrům, které mají přímý vliv na kvalitu a bezpečnost vydávaných certifikátů. Tzn. především mohutnost klíče, dobu platnosti certifikátu a splnění podmínek pro ochranu kryptografického modulu.

Váha se stupněm 2 je nastavena u parametrů, která určují kvalitu a komfort nabízených služeb. Např. perioda zveřejňování seznamu zneplatněných certifikátů, nebo počet registračních autorit.

Poslední stupeň 1 je u zbytku parametrů, které nemají přímý vliv na kvalitu, nebo se jedná pouze o doplňkové služby. Např. vyřizovaní reklamací, nebo zpracování žádostí.

Na základě výsledků hodnocení jednotlivých položek, jsou uděleny body v rozsahu 0 – 3, které představují pořadí kvality certifikačních autorit v rámci každého hodnoceného parametru. Více bodů, znamená lepší hodnocení. Pokud služba není nabízena, je ohodnocena nulovým počtem bodů. Pokud je hodnocený parametr u všech certifikačních autorit shodný, je také ohodnocen shodným počtem bodů. Např. parametr počet registračních autorit je ohodnocen třemi body za nejvyšší počet, (<900 registračních autorit) pro certifikační autoritu PostSignum, dva body (35 registračních autorit) pro I. CA, a pouze jeden bod pro eIdentity (3 registrační autority).

Body jednotlivých položek jsou násobeny nastavenou váhou, součet tvoří celkové bodové hodnocení certifikační autority. Výsledky jsou v tabulce 5.6.1-1. Parametry vlastní certifikační autority je v tabulce uvedeny pouze pro možnost porovnání parametrů.

Hodnoceny jsou tyto parametry:

**Druhy vydávaných certifikátů**

Z důvodu omezení využití kvalifikovaných certifikátů zákonem o elektronickém podpisu podle §12 zákona č. 227/2000 Sb., je nutné pro některé činnosti vydávat komerční certifikáty. Pro vydávání kvalifikovaných certifikátu však musí příslušná certifikační autorita získat akreditaci Ministerstva vnitra. Proto je možnost vydávání kvalifikovaných certifikátu ohodnocena váhou 2.

**Mohutnost klíče**

Mohutnost klíče určuje stupeň bezpečnosti. Podle doporučení RSA je do roku 2030 dostačující velikost klíčů 2048 bitů. Vyšší hodnoty znamenají větší výpočetní nároky potřebné pro šifrování a dešifrování ale vyšší stupeň zabezpečení, nižší hodnoty přináší zvýšené riziko prolomení šifry. V současné době je tedy optimální velikostí klíče 2048 bitů, nižší hodnota bude znamenat horší hodnocení. Tento parametr určuje kvalitu celého procesu práce s digitálním certifikátem a jeho bezpečnost, proto má váhu na stupni 3.

**Doba platnosti certifikátu**

Optimální dobu platnosti klíče určuje mohutnost klíče, delší doba platnosti zvyšuje riziko prolomení šifry. Optimální hodnotou při velikosti klíče 2048 bitů je 1 rok. Delší platnost snižuje hodnocení. Protože tento parametr je spjat s mohutností klíče a má přímý vliv na bezpečnost, má také stejnou váhu, stupeň 3. Platnost certifikátu certifikačních autorit je delší, ale pouze za předpokladu delšího klíče (typicky 4096 bitů).

**Odolnost kryptografického modulu**

Privátní klíč certifikační autority je uložen v kryptografickém modulu, který musí splňovat odolnost vůči fyzickému útoku podle normy FIPS. V současné době je doporučeno zabezpečení podle FIPS 140-2 level 3. Nižší stupeň znamená horší hodnocení. Kvalita zabezpečení modulu určuje riziko diskreditace privátního klíče a určuje tak bezprostředně kvalitu práce celé certifikační autority, proto má váha nejvyšší stupeň 3.

**Perioda zveřejňovaní seznamu zneplatněných certifikátů**

Od chvíle, kdy vlastník certifikátu oznámil kompromitaci svého privátního klíče a požádal tak o předčasné ukončení platnosti certifikátu, běží čas, za který se certifikát dostane na seznam zneplatněných certifikátu a dojde tak ke skutečnému zneplatnění. Pokud si chceme být jisti, že protistrana nepoužila certifikát, u kterého byla podána žádost o zneplatnění, ale zatím se nedostal na seznam zneplatněných certifikátu, musíme počkat na vydání aktuálního seznamu. Průměrná hodnota tohoto intervalu se pohybuje kolem 12 hodin. Delší interval bude znamenat horší hodnocení. Tento parametr určuje rychlost práce s certifikátem, ale nemá přímý vliv na bezpečnost, proto má váhu na stupni 2.

**Využití protokolu OCSP**

Pro ověřování platnosti certifikátu je možné využít protokol OCSP, který má řadu výhod oproti seznamu zneplatněných certifikátů. V případě využití tohoto protokolu nedochází ke zpoždění mezi žádostí o zneplatnění certifikátu a jeho uveřejněním v seznamu zneplatněných certifikátů. Certifikát je zneplatněn okamžitě po podání žádosti. Uživatel se tímto protokolem dotazuje na konkrétní certifikát v online databázi zneplatněných certifikátů. Není proto nutné stahovat vždy celý seznam zneplatněných certifikátů, což snižuje nároky na kapacitu sítě. Možnost využití tohoto protokolu znamená lepší hodnocení. Váha tohoto parametru je také na stupni 2 z důvodu vyšší kvality služeb, která však nemá přímý vliv na bezpečnost.

**Heslo pro zneplatnění**

Při podání žádosti o zneplatnění je možné využít heslo vytvořené již v žádosti o vydání certifikátu. Toto řešení je jednoduché a rychlé. V případě zapomenutí tohoto hesla, je nutná osobní návštěva certifikační autority. Možnost využití této služby znamená lepší hodnocení. Váha je pouze na stupni 1, jedná se pouze o doplňkovou službu, která nemá vliv na celkový proces použití certifikátů.

**Pozastavení platnosti**

Možnost obnovení zneplatněného certifikátu, přináší velké bezpečnostní riziko, a proto by se v praxi nemělo nevyužívat. Pokud toto službu společnost nabízí, znamená to snížení hodnocení. Protože se jedná o bezpečnostní riziko, je váha na stupni 3.

**Forma žádosti o zneplatnění**

Možnosti, jak požádat o zneplatnění certifikátu. Certifikační autority nabízejí více možností jak podat žádost o zneplatnění, záleží na uživateli, kterou možnost si zvolí a která mu nejvíce vyhovuje. Více možnosti znamená lepší hodnocení. Protože parametr nemá vliv na bezpečnost, je váha pouze na stupni 1.

**Počet registračních autorit**

Při prvním vydání certifikátu je nutná osobní návštěva registrační autority. Tento parametr hodnotí počet a rozmístění registračních autorit, kde je možné ověřit identitu žadatele o nový certifikát. Větší počet registračních míst snižuje náklady na prvotní žádost o nový certifikát, případně o náklady na mobilní registrační autoritu. Hustší síť registračních autorit znamená lepší hodnocení. Parametr má velký význam pro kvalitu služeb, proto má váha stupeň 2.

**Uživatelská podpora**

Tento parametr hodnotí možnosti kontaktování uživatelské podpory, rychlost a správnost odezvy. Hodnocení probíhalo na základě poležených dotazů pomocí emailu nebo telefonicky. Rychlejší odezva a kvalita odpovědi znamená lepší hodnocení. Váha je stanovena na stupeň 2, protože má velký vliv na kvalitu služeb.

**Reklamace**

Parametr hodnotí možnosti podání reklamace a termíny vyřízení oprávněné reklamace. Maximální doba na vyřízení je stanovena na 1 měsíc od podání žádosti. Lepší hodnocení je na základně rychlejšího zpracování žádostí. Tento parametr má nastavenu váhu 1, protože má jen vedlejší dopad na kvalitu služeb. Pokud není v certifikační politice společnosti uveden jiný termín, uvažuje se stanovena maximální doba 1 měsíc.

**Doba zpracování žádosti o nový certifikát**

Doba potřebná k vystavení nového certifikátu. Pozitivně je hodnocena rychlejší odezva od podání žádosti až k vytvoření certifikátu. Tento parametr má nastavenu váhu na stupeň 1, protože má jen vedlejší dopad na kvalitu služeb.

**Ceny služeb**

Jsou hodnoceny ceny jednotlivých druhů vydávaných certifikátů. Lépe hodnoceny jsou služby s nižší cenou. Váha parametru je stanovena na stupeň 2, protože při větším množství použitých certifikátů, může rozdíl cen znamenat velký nárůst nákladů na pořízení. Ceny uvedené v hodnotící tabulce jsou uvedeny s DPH s platností certifikátu na 1 rok.

**Důvěryhodnost**

Hodnocení důvěryhodnosti certifikační autority vychází z referencí významných zákazníků, z celkové doby poskytovaní certifikačních služeb a z objemu vydaných certifikátů. Tento parametr je poměrně důležitý, protože práce certifikační autority je právě založena na přenosu důvěry. Z tohoto důvodu je váha nastavena na hodnotu 2.

**Celkové hodnocení.**

V celkovém hodnocení jsou sečteny body jednotlivých položek násobených váhou položky. Výsledky jsou v tabulce 5.6.1-1.

| Společnost | Váha | eIdentity | | | PostSignum | | | I.CA | | | Vlastní certif. autorita |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | body | body* váha | | body | body* váha | | body | body* váha | |
| Komerční certifikát | 1 | Ano | 3 | 3 | Ano | 3 | 3 | Ano | 3 | 3 | Ano |
| Komerční serverový certifikát | 1 | Ano | 3 | 3 | Ano | 3 | 3 | Ano | 3 | 3 | Ano |
| Kvalifikovaný certifikát | 2 | Ano | 3 | 6 | Ano | 3 | 6 | Ano | 3 | 6 | Ne |
| Kvalifikovaný systémový certifikát | 2 | Ano | 3 | 6 | Ano | 3 | 6 | Ano | 3 | 6 | Ne |
| Mohutnost klíče | 3 | 2048 bitů | 3 | 9 | 2048 bitů | 3 | 9 | 2048 bitů | 3 | 9 | Vlastní |
| Doba platnosti certifikátu | 3 | 1 rok | 3 | 9 | 1 rok | 3 | 9 | 1 rok | 3 | 9 | Vlastní |
| Odolnost kryptografického modulu | 3 | FIPS 140-1 Level 3 | 3 | 9 | FIPS 140-2 Level 3 | 3 | 9 | FIPS 140-2 Level 3 | 3 | 9 | Vlastní |
| Perioda zveřejňování CRL | 2 | Max. 24hod | 1 | 2 | Max. 12 hod. | 2 | 4 | Max. 24hod. typicky 8 hodin | 3 | 6 | Vlastní |
| Využití protokolu OCSP | 2 | Ne | 0 | 0 | Ne | 0 | 0 | Na požadavek | 3 | 6 | Vlastní |
| Heslo pro zneplatnění | 1 | 4 a více znaků | 3 | 3 | 8 a více znaků | 3 | 3 | 4-32 znaků | 3 | 3 | Vlastní |
| Pozastavení platnosti | 3 | Ne | 3 | 9 | Ne | 3 | 9 | Ne | 3 | 9 | Vlastní |
| Forma žádosti o zneplatnění | 1 | Elektronicky, písemně, mail, fax | 3 | 3 | Elektronicky, písemně, mail, fax | 3 | 3 | Elektronicky, písemně, mail, fax | 3 | 3 | Vlastní |
| Počet registračních autorit | 2 | 3 místa | 1 | 2 | <900 míst | 3 | 6 | 35 míst | 2 | 4 | Vlastní |
| Uživatelská podpora | 2 | Vyhovující | 2 | 4 | Vyhovující | 2 | 4 | Vysoká | 3 | 6 | Vlastní |
| Reklamace | 1 | Není specifikováno | 2 | 2 | Do 14 dnů | 3 | 3 | Do 1 měsíce | 2 | 2 | Vlastní |
| Doba zpracování žádosti o nový certifikát | 1 | Není specifikováno | 1 | 1 | 2. pracovní dny | 2 | 2 | První pracovní den | 3 | 3 | Vlastní |
| Cena za kvalifikovaný certifikát | 2 | 474 Kč / rok | 2 | 4 | 396 Kč / rok | 3 | 6 | 495 Kč / rok | 1 | 2 | Nelze |
| Cena za kvalifikovaný systémový cer. | 2 | 3480 Kč / rok | 1 | 2 | 1788 Kč / rok | 2 | 4 | 780 Kč / rok | 3 | 6 | Nelze |
| Cena za komerční certifikát | 2 | 354 Kč / rok | 2 | 4 | 348 Kč / rok | 3 | 6 | 395 Kč / rok | 1 | 2 | Vlastní |
| Cena za komerční serverový certifikát | 2 | 1074 Kč / rok | 2 | 4 | 800 Kč / rok | 3 | 6 | 1170 Kč / rok | 1 | 2 | Vlastní |
| Důvěryhodnost | 2 | Nízká | 1 | 2 | Střední | 2 | 4 | Vysoká | 3 | 6 | Vlastní |
| **Celkové hodnocení** | | **Dobré** | | **87** | **Výborné** | | **105** | **Výborné** | | **105** | |

Tabulka 5.6.1.-1: Srovnání parametrů certifikačních autorit

### 5.6.2 Výsledky komparace

V závislosti na podrobné teoretické analýze certifikačních autorit jsem došel k těmto závěrům:

- Komerční i kvalifikované certifikáty vydávají všechny společnosti, vlastní certifikační autorita však může vydávat pouze komerční certifikáty. Mohou vydávat i časová razítka. V tomto parametru není v porovnávaných certifikačních autoritách žádný rozdíl.
- Všechny autority používají doporučenou mohutnost klíče 2048 bitů a maximální dobu platnosti 1 rok.
- Kryptografické moduly splňují bezpečnostní požadavky podle FIPS 140-2 Level 3, společnost se odkazuje na starší normu FIPS 140-1 ale se stejným stupněm. Ani v tomto parametru nejsou žádné rozdíly.
- Důležitý parametr zveřejňování seznamu odvolaných certifikátů splňuje nejlépe I. CA, která uvádí typickou periodu 8 hodin a navíc na vyžádání podporuje zveřejňování zneplatněných certifikátů pomocí protokolu OCSP, který je velkou výhodou. Ostatní autority tuto službu nenabízí.
- Všechny certifikační autority nabízí využití hesla pro zneplatnění, liší se pouze v požadavcích na počet znaků hesla.
- Žádná společnost nenabízí službu pozastavení platnosti, což je z bezpečnostního hlediska správné.
- Všechny společnosti nabízejí stejné formy podání žádost o zneplatnění.
- Počet registračních autorit jednotlivých certifikačních autorit se velmi liší. Bezkonkurenčně nejlepší je společnost PostSignum s více než 900 místy. Společnost I. CA, bohužel snížila počet svých registračních autorit na 35, která však pokrývají alespoň krajská města. Společnost eIdentity nabízí pouze 3 místa omezená na hlavní město.
- Podle průzkumu kvality uživatelské podpory vychází nejlépe společnost I. CA, která reagovala na vznesené dotazy pomocí emailu. Operátoři I. CA se zpětným telefonickým dotazem ujišťují, zda byli odpovědi dostatečné. Ostatní společnosti podali odpovědi pouze po urgenci dotazů.
- Dobu vyřízení reklamace nejlépe splňuje společnost PostSignum, která slibuje vyřízení reklamace do 14 dnů. Ostatní společnosti se drží stanované lhůty 1 měsíc.

- Nejrychlejší vyřízení žádosti o nový certifikát slibuje společnost I. CA – první pracovní den. Dva dny si stanovila společnost PostSignum. Společnost eIdentity nemá své certifikační politice tento termín stanoven.
- Ceny za vydávané komerční i kvalifikované certifikáty se liší jen minimálně. Nejlevnější certifikáty nabízí PostSignum, následuje společnost eIdentity, poslední je I. CA, jejíž kvalifikovaný certifikát je o 99 Kč dražší než u PostSignum. Větší rozdíl v cenách je pouze u kvalifikovaného systémového certifikátu, kde je I. CA naopak nejlevnější.
- Nejvyšší důvěryhodnost zcela jistě nabízí společnost I. CA, díky referencím svého portfolia významných zákazníků, počtu vydaných certifikátu a nejdelšího působení na trhu.

Na základě bodového hodnocení je možné sestavit žebříček kvality certifikační autority. Nejvíce bodů získala I. CA spolu s PostSignum. I. CA navíc nabízí službu online zjišťování stavu neplatných certifikátů (OCSP) a také má vysoký stupeň důvěryhodnosti, díky svým významným zákazníkům, nejdelšímu působení na trhu a objemu vydaných certifikátů. Také kvalita uživatelské podpory je vynikající. Vydávané certifikáty však mají nejvyšší cenu s výjimkou ceny za kvalifikovaný systémový certifikát.

Certifikační autorita PostSignum má výhodu ve velkém počtu registračních autorit a také v nejnižší ceně za vydávané certifikáty.

Certifikační autorita eIdentity nabízí technicky i bezpečnostně plně vyhovující služby, její slabinou je velmi malý počet registračních autorit. Podle ujištění jejich uživatelské podpory se však pracuje na dalším rozvoji.

## 5.7 Doporučení

Na základě hodnocení certifikačních autorit je možné provést doporučení pro zákazníky z různých oblastí. Certifikační autority sami omezují použití svých certifikátů pro komunikace a transakce v oblastech, kde je zvýšené riziko škod na zdraví nebo majetku. Jedná se o letecký provoz, provoz jaderných nebo chemických zařízení apod. Také omezují své služby pro činnosti, které souvisí s bezpečností nebo obranyschopností státu. Tyto služby poskytují jen za zvláštních podmínek, které je potřeba sjednat individuálně.

Využití digitálních certifikátů je poměrně široké. V hojné míře je mohou využívat především:

- školy,

- pojišťovny, banky,
- obchodní společnosti,
- zdravotnictví,
- orgány státní správy a samosprávy,
- právnické osoby,
- fyzické osoby.

Využití digitálních certifikátů by mělo být samozřejmé u všech internetových aplikací, kde se manipuluje s citlivými údaji uživatelů. Může se jednat o adresy, osobní nebo zdravotní údaje, bankovní nebo obchodní transakce apod.

Každý uživatel, který stojí před volbou vhodné certifikační autority, by si měl položit několik základních otázek.

- Jaký certifikát potřebuji?
- Je pro mě certifikační autorita důvěryhodná?
- Vyhovuje mi rozsah nabízených služeb a cena?

Všechny porovnávané společnosti nabízejí všechny druhy certifikátů, tzn. jak kvalifikované tak i komerční, klientské i systémové. V tomto ohledu je tedy možné volit kteroukoliv společnost.

Z hlediska důvěryhodnosti jednoznačně nejlépe vychází společnost I. CA, která spolupracuje s velkou řadou významných společností. Plusem pro tuto společnost je i nejdelší působení v této oblasti. Společnosti Česká pošta s. p. (PostSignum) a Identity nezveřejňují seznam svých zákazníků. U společnosti Česká pošta však musíme přihlédnout k velikosti celé společnosti, která tímto faktorem také získává vysokou důvěryhodnost.

Pro společnosti, kde je počet vydávaných certifikátů vysoký, je určitě důležitá i otázka ceny za vydaný certifikát. Vzhledem k ceně klientské certifikační autority je vhodné už od stovky vydaných certifikátů ročně, uvažovat o zřízení vlastní certifikační autority.

Ve školství, kde by se uvažovalo o využití digitálních certifikátů jednotlivými studenty, jsou samozřejmě služby certifikačních autorit nevhodné a jediným řešením v takovém případě je zřízení vlastní certifikační autority. Podle možností daného zařízení (fakulty, školy) záleží kterou možnost zvolit. Pokud škola disponuje dobrou podporou ze strany IT, může zvolit řešení postavené na certifikačních

autoritách dostupných podle typu již využívané infrastruktury, tzn. řešení pomocí Windows Server, Linuxový systém nebo řešení na bázi Open source. Komerční řešení třetích stran jsou pro školství bohužel nedostupná, pro svou velmi vysokou cenu. Pokud škola nemá možnost využívat svou vlastní IT podporu, může zvolit zřízení vlastní klientské certifikační autority, kterou nabízí společnost I. CA. V tomto případě implementaci technického i softwarového zajišťuje dodavatel služby.

Pokud vydávávaný počet certifikátu není vysoký, je vhodné se spolehnout na služby certifikační autority. V tomto případě bude hlavním kritériem pro rozhodování dostupnost služeb, tzn. počet registračních certifikačních autorit a samozřejmě kvalita podpory a cena. Pokud se často mění osoby, které certifikáty využívají, tzn. je potřeba vystavovat nové certifikáty a uživatelé jsou rozmístěni na různých lokalitách, je nutné zvolit autoritu s velkým počtem a hustou sítí registračních autorit. Hustou sítí disponuje především autorita PostSignum s více než 900 registračních míst nebo I. CA s 35 místy v krajských městech.

Zákazník, který nemá potřebné znalosti nebo zkušenosti v oblasti IT, bude hledat služby s dobrou uživatelskou podporou. Všechny certifikační autority nabízejí výborné webové prezentace, kde se uživatel může seznámit se všemi podrobnostmi. Nejlépe však v hodnocení vychází společnost I. CA s výbornou uživatelskou podporou prostřednictvím emailu a telefonu.

Webové servery JČU neposkytují informace o své identitě. Ani aplikace, které spravují osobní údaje studentů JČU (IS/STAG), nejsou zabezpečeny a komunikace mezi klientem a serverem není šifrována. Server by měl být opatřen svým digitálním certifikátem, vydaným certifikační autoritou, která je uvedena v seznamu důvěryhodných certifikačních autorit a komunikace zabezpečena pomocí protokolu HTTPS.

V dalším kroku by bylo možné zajistit studentům čipové karty s vlastním komerčním certifikátem a zajistit tak, v kombinaci s autentizací heslem, přihlašování pomocí dvoufaktorové autentizace. Pokud by tato možnost měla být realizována, pak jediným vhodným řešením je využití buď vlastní certifikační autority, nebo klientské certifikační autority. Vlastní certifikační autorita by měla vycházet z již nainstalované a využívané infrastruktůry.

Využívání služeb komerčních certifikačních autorit by nebylo vhodné ani z hlediska ceny ani z důvodů praktických. Hromadné prvotní vystavení certifikátu za pomocí registrační autority při velkém počtu studentů by nebylo organizačně ani cenově únosné.

# 6 Praktická část

V praktické části, s použitím digitálního certifikátu, vytvoříme šifrované spojení mezi serverem a klientem, za podpory protokolu SSL.

## 6.1 Vytvoření certifikátů za pomoci Open SSL

Pomocí Open SSL lze spustit následující aplikace:[36]

| | |
|---|---|
| ans1parse | Pitvání BER/DER/PEM zpráv v jazyce ASN.1 |
| ca | Podepisování žádosti o certifikáty a CRL, udržování databáze vydaných certifikátů |
| ciphers | Seznam podporovaných šifer |
| crl | Práce s CRL |
| crl2pkcs7 | Konverze CRL a certifikátu do zpráv tvaru PKCS#7 |
| dgst | Výpočet otisku |
| dsa | Manipulace s DSA |
| enc | Šifrování/dešifrování a kodování/dekodování Base64 |
| errstr | Převod chybových kódů na text |
| gendsa | Generování párových dat DSA |
| genrsa | Generování párových dat RSA |
| passwd | Práce s hesly |
| pkcs12 | Práce s daty ve formátu dle normy PKCS#12 |
| pkcs7 | Práce se zprávami dle normy PKCS#7 |
| pkcs8 | Práce s privátním klíčem dle normy PKCS#8 |
| rand | Generování pseudonáhodných čísel |
| req | Generování žádosti o certifikáty dle PKCS#10 |
| rsa | Manipulace s RSA klíči |
| smime | Práce s e-maily dle normy S/MIME |
| speed | Benchmark testy |
| verify | Verifikace certifikátu |
| version | Vypíše aktuální verzi OpenSSL |
| x509 | Práce s certifikáty dle X509 včetně jejich podepisování |

Tabulka 5.6.2-1: Přehled aplikací OpenSSL

[36] Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2.akualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6. strana 140.

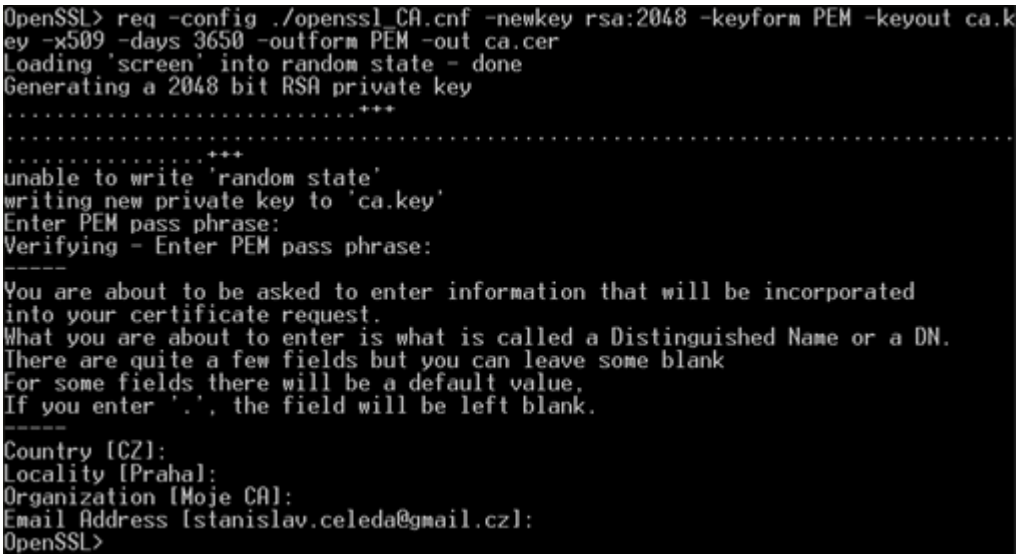
Vytvoření certifikátů a jejich instalace bude provedena na open source webovém serveru. Konkrétně se jedná o instalaci WampServer ve verzi 2.2a 64bits pro Windows. Tato instalace obsahuje všechny potřebné komponenty pro vytvoření certifikátů i pro samotný běh redakčního systému:

- Apache 2.2.17 – webový server s podporou openssl,
- PHP 5.3.8 – interpret jazyka PHP,
- MySQL 5.5.16 – databázový systém,
- PhpMyadmin 3.4.5 – nástroj pro správu databáze MySQL.

### 6.1.1 Vytvoření certifikátu certifikační autority

V prvním kroku je potřeba vytvořit certifikát certifikační autority, který je podepsaný sám sebou.

```
req -config ./openssl_CA.cnf -newkey rsa:2048 -keyform PEM -keyout ca.key -x509 -days 3650 -outform PEM -out ca.cer
```



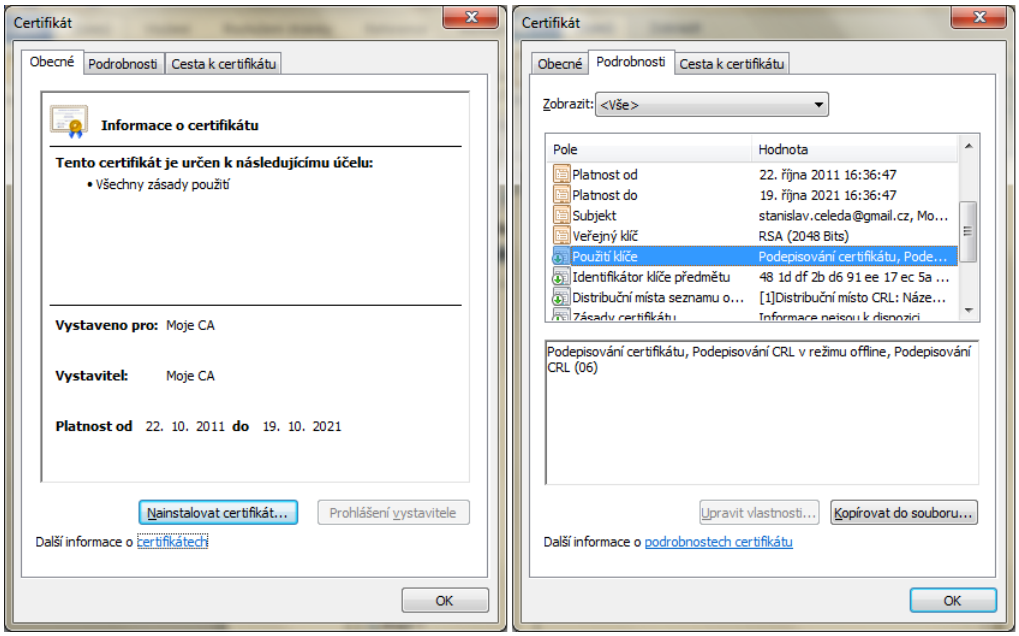

Obrázek 6.1.1-1: Vytoření certifikátu CA

Pro usnadnění práce je možné parametrem –config načíst konfigurační soubor, který si dopředu připravíme a v případě chyby snadno opravíme a znovu použijeme. Je vhodné vyjít ze standardního souboru, který je po instalaci připraven v adresáři conf. V tomto případě se jedná o soubor openssl_CA.cnf.

```
[ req ]
default_md = sha1
distinguished_name = req_distinguished_name
x509_extensions = v3_ca
```

```
string_mask = nombstr
reg_extensions = v3_req
policy = policy_match
[ req_distinguished_name ]
countryName = Country
countryName_default = CZ
countryName_min = 2
countryName_max = 2
localityName = Locality
localityName_default = Praha
organizationName = Organization
organizationName_default = Moje CA
CommonName = Common Name
CommonName_default = Moje_CA
commonName_max = 64
emailAddress = Email Address
emailAddress_default = stanislav.celeda@gmail.cz
[ v3_ca ]
basicConstraints = critical,CA:true
keyUsage = cRLSign, keyCertSign
subjectKeyIdentifier = hash
crlDistributionPoints = URI:http://crl.mojeCA.cz/list.crl
certificatePolicies = ia5org
[ v3_req ]
nsCertType = objsign,email,server
[ policy_match ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationUnitName = optional
commonName = supplied
emailAddress = optional
```

Pokud vše proběhlo bez problému, měl by se v adresáři vytvořit nový soubor s certifikátem s názvem CA.cer.

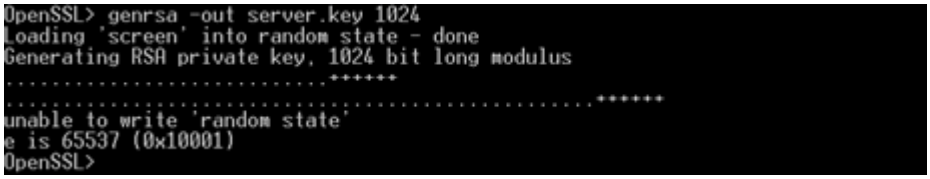



Obrázek 6.1.1-2: Nový certifikát CA

### 6.1.2 Vytvoření certifikátu serveru

K vytvoření certifikátu serveru použijeme certifikát „Mojí CA“. Nejprve je potřeba vytvořit klíče:

```
genrsa -out server.key 1024
```




Obrázek 6.1.2-1: Vytvoření klíčů serveru

Pak je možné vytvořit žádost o serverový certifikát.

```
req -new -key server.key -out server.req -config openssl_server_req.cnf
```


Obrázek 6.1.2-2: Vytvoření žádosti o certifikát

V souboru open_ssl_server.cnf je především specifikováno použití klíče:

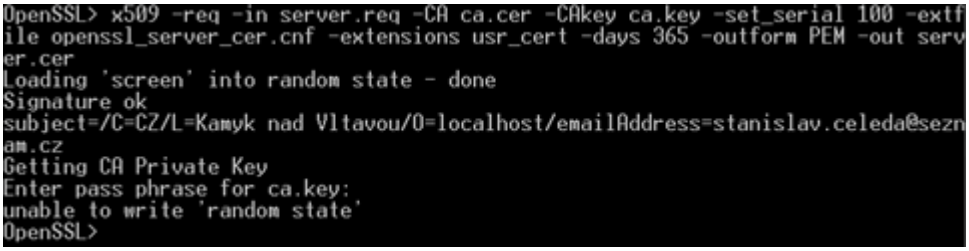
```
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncypherment, keyAgreement

extendedKeyUsage = serverAuth, clinetAuth, ipsecEndSystem, ipsecTunnel
```

V posledím kroku vytvoříme samotný serverový certifikát:

```
x509 -req -in server.req -CA ca.cer -CAkey ca.key -set_serial 100 -extfile openssl_server_cer.cnf -extensions usr_cert -days 365 -outform PEM -out server.cer
```

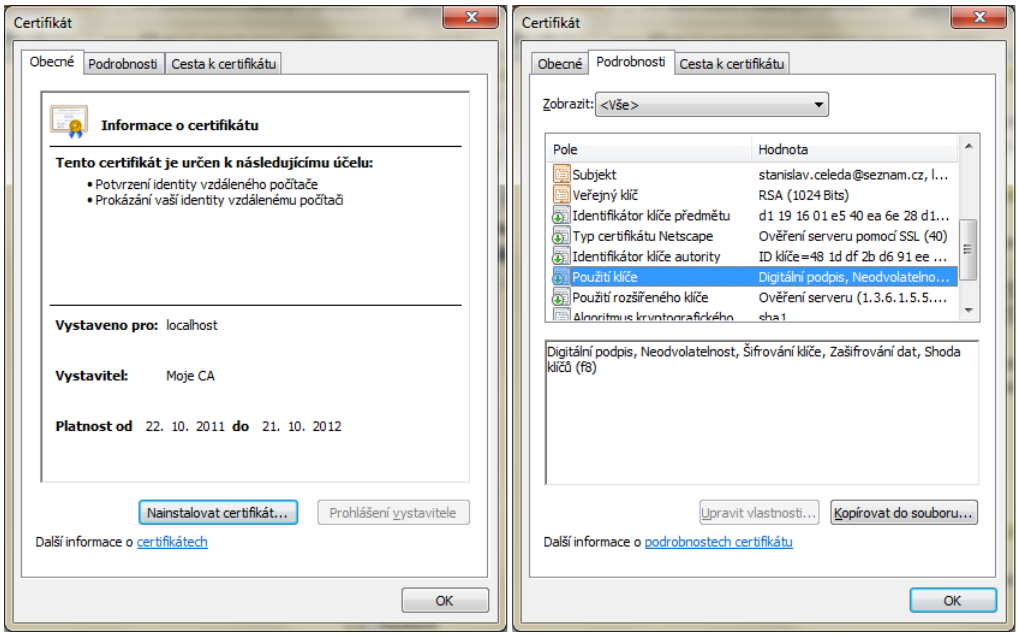
Parametr –extesions přestavuje rozšíření certifkátu, která jsou uvedena v souboru openssl_server_cer.cnf.

```
subjectKeyIdentifier = hash

nsCertType = server

authorityKeyIdentifier = keyid,issuer:always

keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement

extendedKeyUsage = serverAuth, clientAuth
```




Obrázek 6.1.2-3: Vytvoření certifikátu serveru

Certifikát serveru by měl být vytvořen. Pokud dojde k chybě je potřeba znovu prověřit hlavně konfigurační soubor. Některé parametry jsou „case sensitive“!




Obrázek 6.1.2-4: Nový certifikát serveru

Bohužel „Moje CA“ není samozřejmě zahrnuta v důvěryhodných autoritách. Uživateli se tedy zobrazí hlášení o nedůvěryhodnosti certifikační autority.

### 6.1.3 Vytvoření zabezpečeného spojení mezi serverem a klientem

Pokud má server vystaven svůj certifikát, nebrání již nic k vytvoření zabezpečeného spojení mezi serverem a klientem. Zbývá provést změnu nastavení webového serveru. Především je nutné zapnout podporu SSL. V souboru httpd.conf umístěném v adresáři /conf je potřeba zrušit komentář (#) před direktivou

```
LoadModule ssl_module modules/mod_ssl.so
```

V nových verzích je konfigurace rozdělena do více souborů, např. konfigurace SSL je v souboru httpd-ssl.conf v adresáři /conf/extra. Zde je nutné zkontrolovat nastavení portu 443, na kterém webový server bude očekávat požadavky na zabezpečené spojení protokolem HTTPS, tzn. doplnit řádek popř. zrušit komentář u řádku:

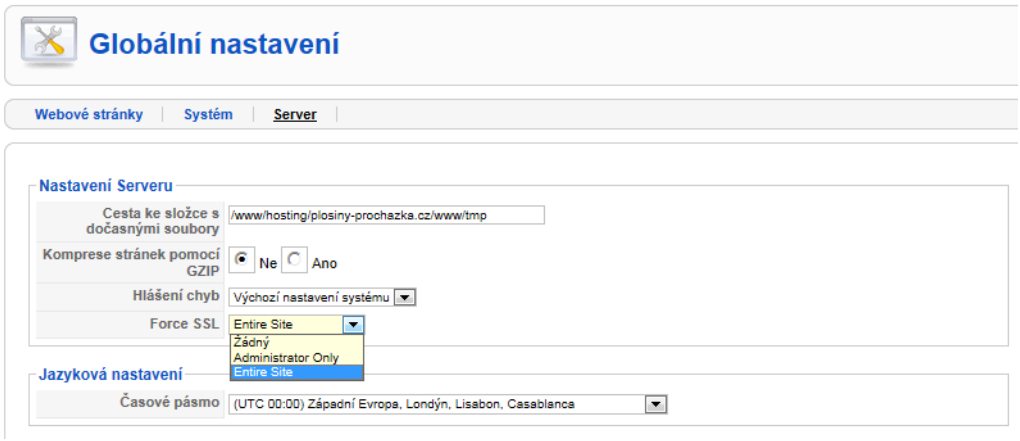
```
Listen 443
```

Dále je potřeba doplnit řádky s cestou k certifikátu a klíči serveru.

```
SSLEngine on
SSLCertificateFile /…/server.cer
SSLCertificateKeyFile /…/server.key
```

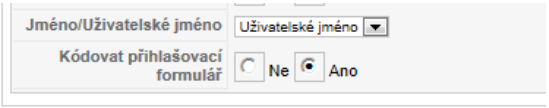
V posledním kroku je potřeba zabezpečit přepnutí na protokol HTTPS. Předpokládá se, že na webovém serveru již běží webová prezentace např. v redakčním systému Joomla! Je více možností jak změnu nastavení provést.

Po přihlášení do administrátorského rozhraní, volbou Globální nastavení a Server. Zde je možnost nastavení zabezpečeného spojení pro celý web, pouze pro administrátorské rozhraní nebo žádné.




Obrázek 6.1.3-1: Nastavení šifrovaného spojení

Pokud je potřeba zabezpečit pouze určité stránky (články), je potřeba stránky označit pro registrované a tím podmínit přístup. V modulu mod_login stačí přepnout přepínač „Kódovat přihlašovací formulář“.




Obrázek 6.1.3-2: Modul mod_login ze redakčního systému Joomla!

Bohužel práce v příkazovém řádku není příliš pohodlná a vytvoření a vyladění certifikátů trvalo několik hodin. Velké usnadnění přináší možnost použití konfiguračních souborů *.cnf.

## 6.2 Vytvoření certifikátů v prostředí Linux

Vytvoření vlastní certifikační autority a generování certifikátů v prostředí Linux je možné za použití grafické aplikace gnoMint. Odzkoušení bylo provedeno pod operačním systémem Linux Ubuntu 10.04 CZ 64 bit. Verze gnoMint 1.2.1.

V prvním kroku je třeba založit databázi certifikační autority, ve které jsou později uloženy jak klíče, tak samotné certifikáty. Vytvoření databáze se provede přímo z nástroje gnoMint volbou z menu *Certificates* a *New certificate database*.

### 6.2.1 Vytvoření certifikátu certifikační autority

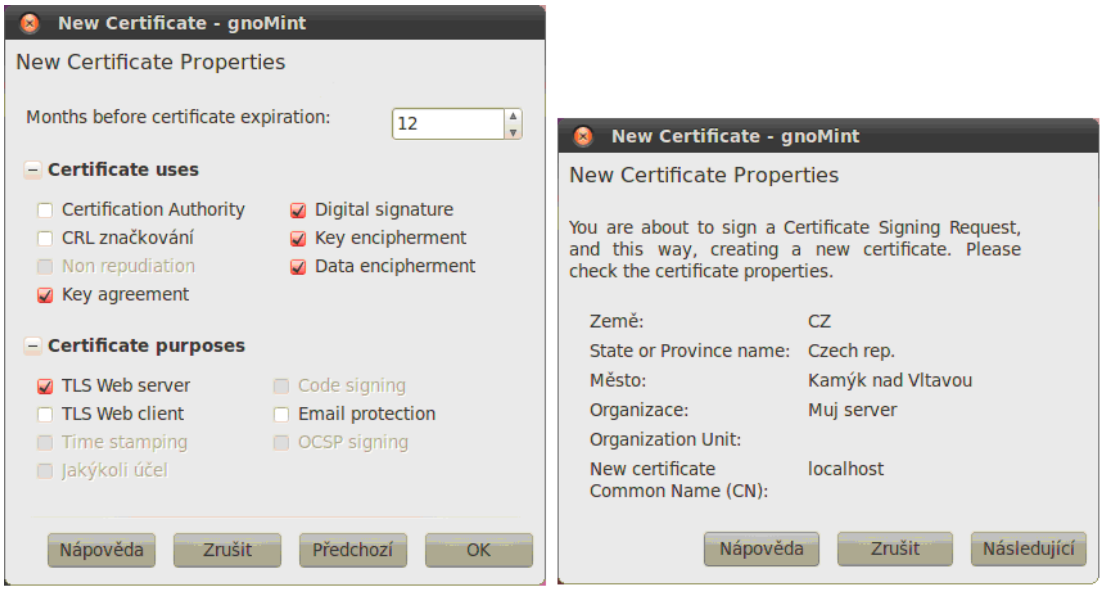
Vytvoření certifikátu certifikační autority se spustí pomocí volby *Certificates – Add – Add self-digned CA*. Poté jsou třeba vyplnit vlastnosti certifikační autority.


Obrázek 6.2.1-1: Generování certifikátu certifikační autority.

Aplikace vytvoří pár klíčů, certifikát a uloží vše do databáze.

### 6.2.2 Vytvoření certifikátu serveru

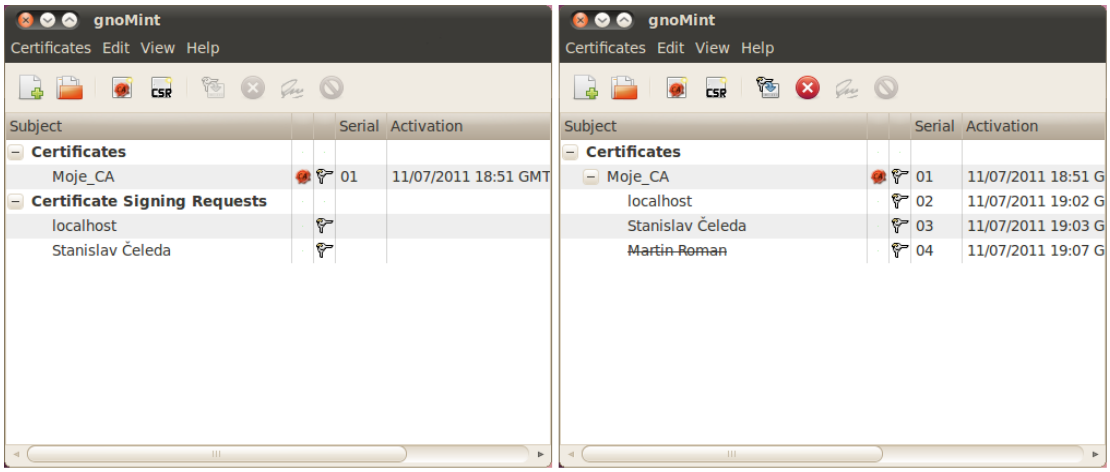
Nejprve je potřeba vytvořit požadavek na certifikát volbou *Certificates – Add – Add certificate request*. Opět je třeba vyplnit žádané vlastnosti. Velmi důležitá je položka Certificate Common Name (CN), která musí obsahovat jméno serveru, pro který je certifikát vystavován. V následujícím okně zvolíme typ a velikost klíče. Žádost je vytvořena a stačí ji pouze podepsat volbou *Sign*, poklepáním na vytvořené žádosti a vybrat požadované vlastnosti certifikátu. V případě serveru je důležitá vlastnost TLS Web server. Po potvrzení zadání je certifikát vytvořen.




Obrázek 6.2.2-1: Podpis žádosti.

### 6.2.3 Vytvoření uživatelského certifikátu

Vytvoření uživatelského certifikátu proběhne podobným způsobem. Při podepisování žádosti je potřeba označit položky TLS Web client a Email protection v sekci Certificate purpose podle obrázku 6.2.2.-1.

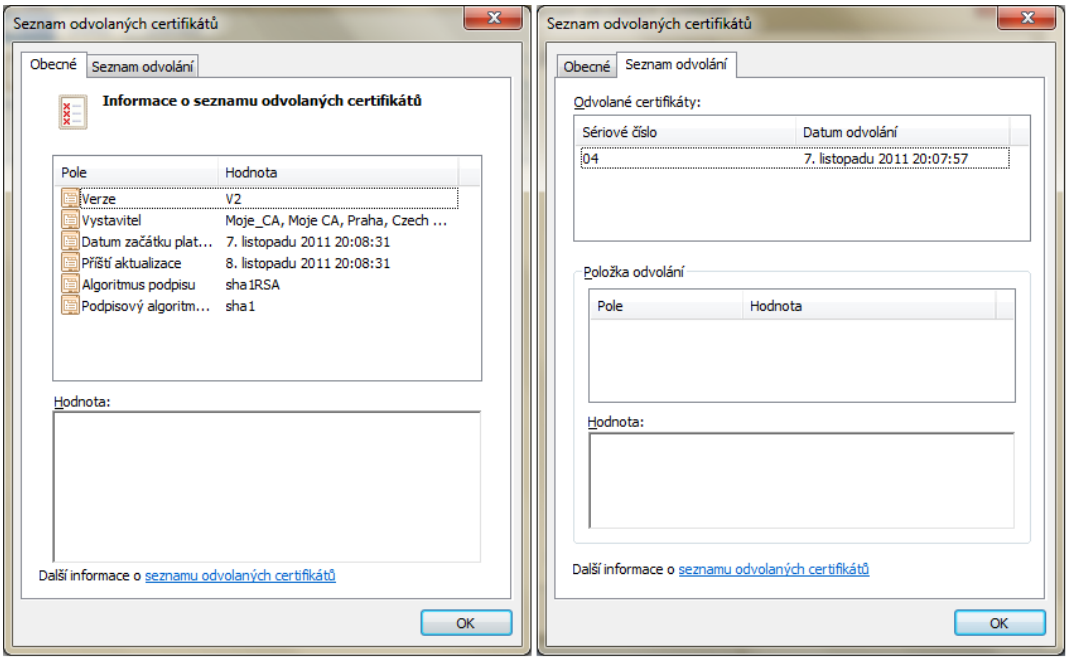



Obrázek 6.2.3-1: Žádosti o certifikát a vystavené certifikáty.

Export certifikátu nebo privátního klíče je možný volbou Export poklepáním na příslušném certifikátu.

### 6.2.4 Revokace certifikátu

Revokace certifikátu se provede volbou *Revoke* poklepáním na příslušném certifikátu. Vydání seznamu odvolaných certifikátu se spustí volbou *Certificates* a *Generate CRL*. V našem případě byl odvolán certifikát se sériovým číslem 04.




Obrázek 6.2.4-1: Seznam odvolaných certifikátů.

Práce s aplikací gnoMint je ve srovnání s příkazovým řádkem nástroje OpenSSL velice jednoduchá. Veškerá nastavení se provádí pomocí grafického rozhraní, které

je přehledné a intuitivní. V případě problémů je dostupná nápověda v anglickém jazyce.

Při generování klíčů však dochází k problémům, které se projevují velice rozdílnou dobou generování páru klíčů. V některých případech je čas potřebný pro generování i několik minut. Není žádoucí tento proces předčasně ukončovat, vždy došlo k úspěšnému dokončení a pár klíčů byl vytvořen. Žádné další problémy se při práci s aplikací gnoMint neprojevily.

## 6.3 Vytvoření certifikátů ve Windows Server 2008

Vytvoření a správa je samozřejmě možná i v prostředí operačního systému Windows Server. Odzkoušení bylo provedeno na verzi Windows Server 2008 Enterprise Edition. Certifikační autorita je dostupná také ve verzích Standart a Datacenter, nikoliv však ve verzi Web.

### 6.3.1 Vytvoření certifikační autority

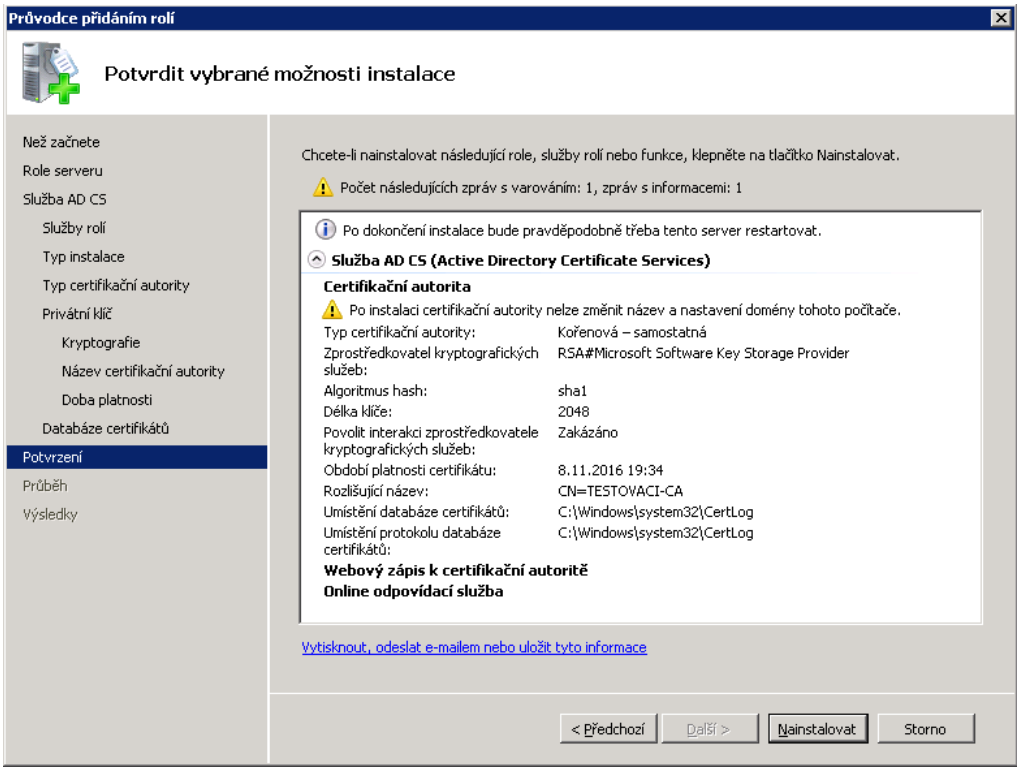
Pro vytvoření certifikační autority je potřeba přidat ve Správě serveru novou roli „Služba AD CS (Active Directory Certificate Services)“.

V kroku Služby rolí je potřeba zaškrtnout minimálně položky Certifikační autorita. Pro snadnější správu je vhodné doplnit i službu Webový zápis k certifikační autoritě, která poskytuje jednoduché webové rozhraní umožňující uživatelům žádat o certifikáty, obnovovat je, stahovat seznamy odvolaných certifikátů apod.

Podle rozsahu sítě se nastavuje typ instalace. V tomto příkladu je uvedena samostatná certifikační autorita. Typ certifikační autority je možné zvolit jako podřízenou certifikační autoritu nebo jako kořenovou. Pro odzkoušení jsem zvolil kořenovou certifikační autoritu.

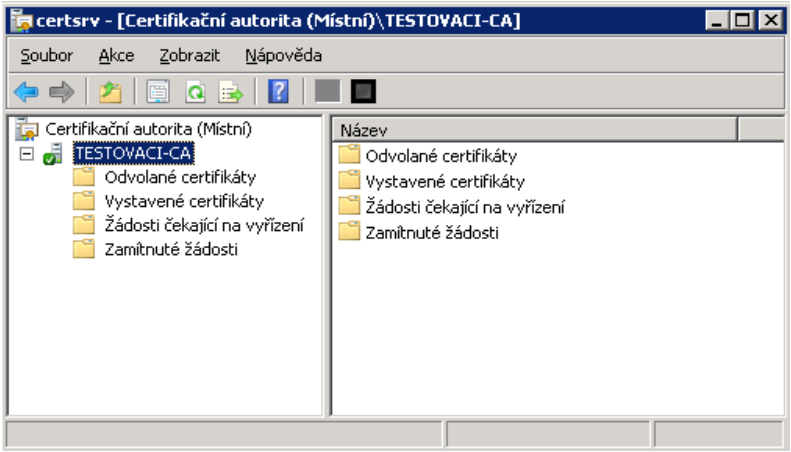
V kroku Privátní klíč je možné vytvořit nový privátní klíč nebo použít existující pro případ reinstalace certifikační autority. Protože se jedná o novou certifikační autoritu, je potřeba vytvořit nový privátní klíč, u kterého se musí vybrat jeho délka a algoritmus pro podepisování. Zvolil jsem délku klíče 2048 bitů a algoritmus sha1. Zbývá doplnit jméno certifikační autority, např. „TESTOVACI-CA“, a dobu platnosti, v tomto případě 5 let.

V kroku Databáze certifikátů se nastavuje cesta k databázi certifikátu a k protokolům.




Obrázek 6.3.1-1: Potvrzení instalace nové role.

V dalších dvou krocích je zobrazen průběh instalace a její výsledky. Instalace proběhla bez problémů. Nyní je již možné volbou *Start* a *Certification Autority* spustit správce právě vytvořené certifikační autority a prohlédnout si její vlastnosti a certifikát.

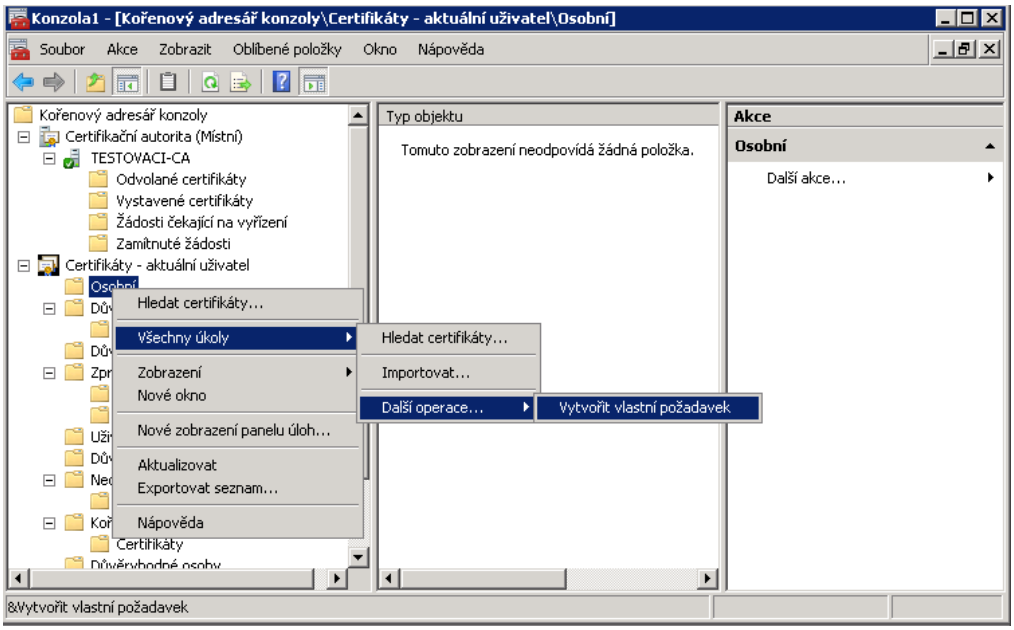



Obrázek 6.3.1-2: Okno správce certifikační autority.

### 6.3.2 Vytvoření požadavku na nový certifikát

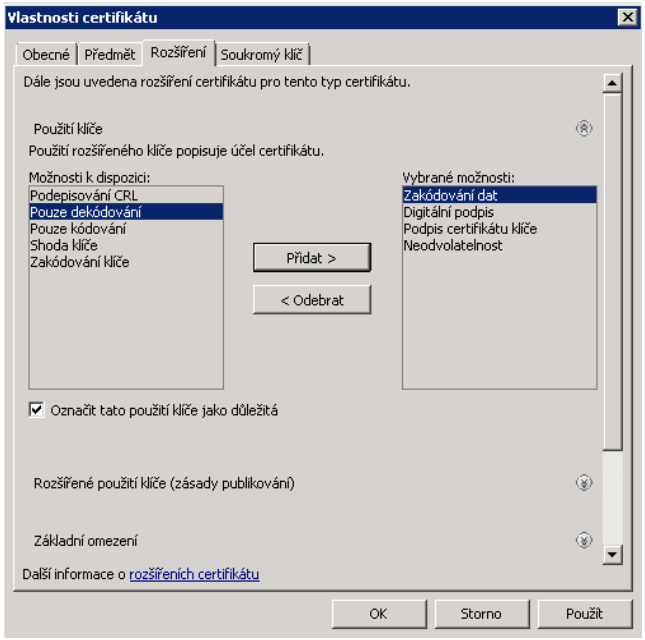
Požadavek na vydání nového certifikátu je možné vytvořit prostřednictvím konzoly nebo webového serveru. Konzola se spustí příkazem *MMC*. Volbou *Soubor* a

*Přidat nebo odebrat modul snap-in* přidáme moduly Certification Authority a Certifikáty. Průvodce na vytvoření nového certifikátu se spustí volbou *Všechny úkoly – Další operace- Vytvořit vlastní požadavek*. Viz obrázek 6.3.2-1.




Obrázek 6.3.2-1 Vytvoření nového požadavku.

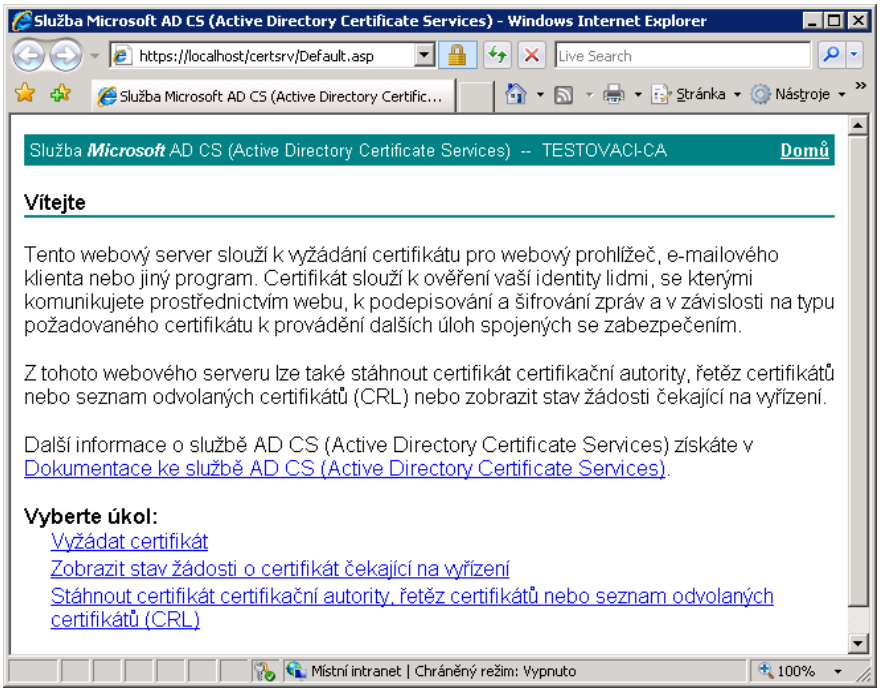
V okně Zápis certifikátu volbou *Podrobnosti* a *Vlastnosti* nastavíme požadované vlastnosti certifikátu. Pokud je žádost připravena, je možné jí uložit do souboru *.req.




Obrázek 6.3.2-2: Nastavení rozšíření certifikátu.

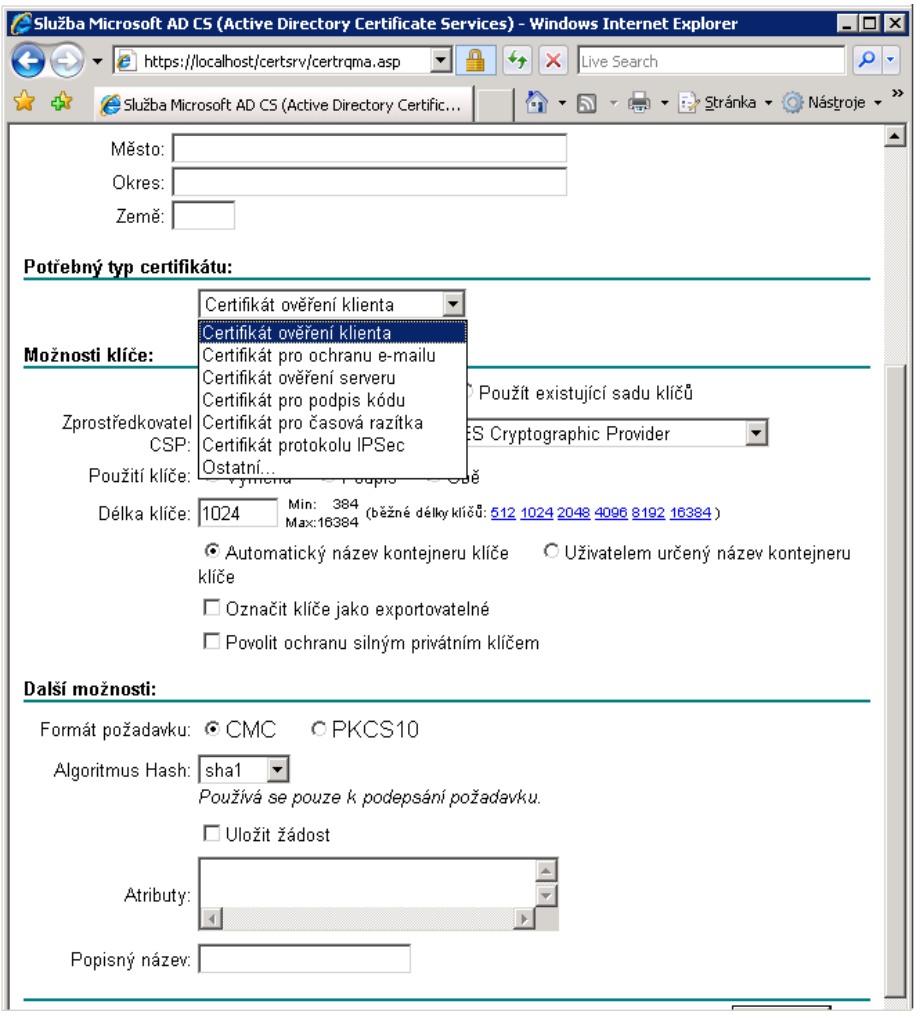
Tento požadavek je potřeba načíst pomocí správce certifikační autority volbou *Akce – Všechny úkoly – Odeslat nový požadavek*. Pokud je žádost formálně v pořádku, zobrazí se ve složce Žádosti čekající na vyřízení, kde je možné potvrdit vystavení certifikátu volbou *Všechny úkoly – Vystavit*. V případě, že žádost neobsahuje povinné vlastnosti certifikátu, je vygenerováno chybové hlášení a je potřeba opakovat celý proces žádosti znovu. Chybné žádosti se zobrazují ve složce Zamítnuté žádosti.

Další možností podání žádosti o certifikát je využití webového serveru, který nabízí jednoduché stránky, kde je možné o certifikáty požádat.




Obrázek 6.3.2-3: Úvodní okno webové služby certifikační autority.

Uživatel má možnost vyplnit základní parametry jako identifikační údaje, zvolit potřebný typ certifikátu, parametry klíče a formát požadavku. Po odeslání se žádost automaticky zobrazí ve Správci certifikační autority, kde se již výše popsaným způsobem potvrdí nebo odmítne.



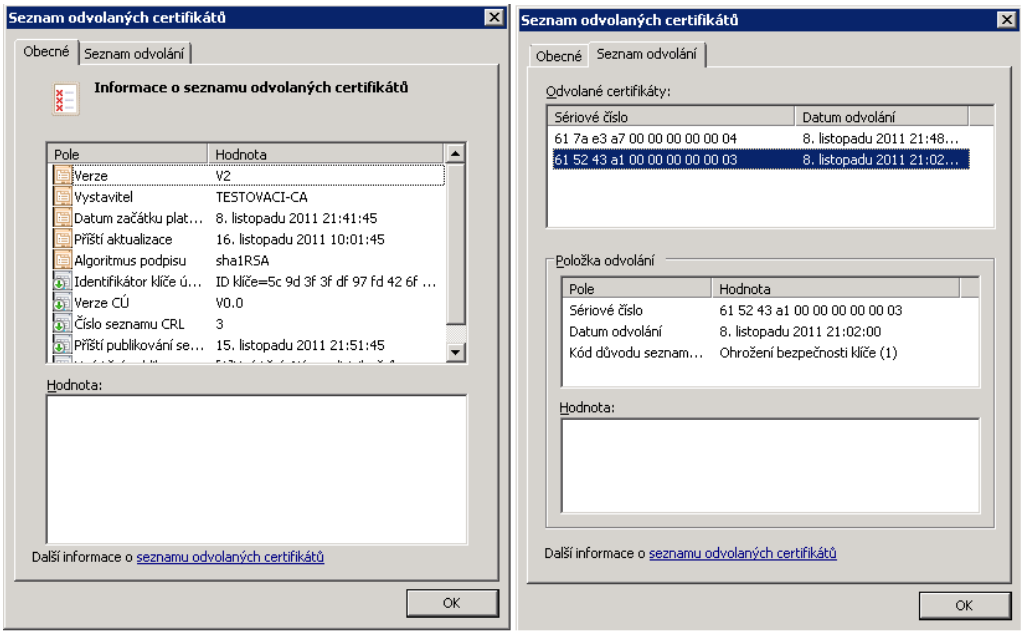

Obrázek 6.3.2-4: Okno žádosti o nový certifikát.

Po zpracování žádosti může uživatel odkazem „Zobrazit stav žádosti o certifikát čekající na vyřízení“ stáhnout a nainstalovat svůj certifikát. Případně odkazem „Stáhnout certifikát certifikační autority, řetěz certifikátů nebo seznam odvolaných certifikátů (CRL)“ stáhnou aktuální seznam odvolaných certifikátů.

### 6.3.3 Revokace certifikátu

Vystavené certifikáty je možné zneplatnit volbou *Všechny úkoly – Odvolat certifikát*. V dialogovém okně je možné zvolit kód důvodu odvolání, datum a čas. Příslušný certifikát se poté zobrazí ve složce Odvolané certifikáty.

Vydání seznamu odvolaných certifikátu se spustí poklepání na složce Odvolané certifikáty volbou *Všechny úkoly – Publikovat*. Volbou *Vlastnosti* je možné nastavit parametry pro publikování seznamu odvolaných certifikátu a zobrazit seznamy CRL.




Obrázek 6.3.3-1: Vygenerovaný seznam odvolaných certifikátů.

Vytvoření certifikační autority, podávávání žádost i generování certifikátů je pomocí Active Directory Certificate Services ve Windows Server 2008 poměrně snadné a intuitivní. V případě nejasností je dostupná kontextová nápověda, pomocí které lze snadno dohledat řešení problému. Služba provádí validaci vystavovaných certifikátů a v případě chybného zadání neumožní jeho podepsání a vygenerování.

Při využití webového serveru pro podávání žádostí o nový certifikát, je potřeba provést přesměrování na zabezpečený port 443. Toto nastavení je ve správě webového serveru.

# 7 Diskuze

Pro analýzu problematiky digitálních certifikátů se podařilo shromáždit potřená data, na jejichž základě byl realizován výzkum českých certifikačních autorit, které mají akreditaci pro vydávání kvalifikovaných certifikátů. Na trhu jsou dostupné i další certifikační autority, které však nejsou akreditovány pro vydávání kvalifikovaných certifikátů a ani nemají přesně specifikovány nabízené služby a technické parametry ve své certifikační politice. Tyto certifikační autority proto nebyly do výzkumu zahrnuty.

Zvolený postup hodnocení certifikačních autorit byl navržen tak, aby parametry, které mají významný vliv na kvalitu a bezpečnost certifikátu, přímo ovlivnily celkové hodnocení. Toho je docíleno přiřazením určitého stupně váhy jednotlivým hodnoceným parametrům. V případě, že by do hodnocení byla zahrnuta další certifikační autorita, je nutné rozšířit i bodové hodnocení, které vychází právě z pořadí kvality hodnocených parametrů.

Žebříček kvality certifikačních autorit, který je v této práci určen, nelze obecně využít pro všechny nároky různých uživatelů. Vždy je potřeba přihlédnout k aktuálním potřebám uživatelů a zamýšlenému využití digitálního certifikátu a podle toho zvolit vhodnou certifikační autoritu. Doporučení pro volbu certifikační autority je uvedeno v kapitole 5.7.

Analýza a hodnocení certifikačních autorit mají pouze omezenou platnost. Pokud dojde ke změnám v certifikační politice hodnocených certifikačních autorit, je nutné provést aktualizaci vstupních parametrů a znovu přepočítat výsledky hodnocení. Verze certifikačních politik, ze kterých byly čerpány informace pro hodnocení, jsou uvedeny v kapitole Literatura a zdroje.

Generování digitálních certifikátů bylo úspěšně odzkoušeno na několika operačních systémech s různými softwarovými nástroji. Vytvořené certifikáty byly použity pro vytvoření zabezpečeného spojení na lokálním webovém serveru.

Nebylo možné prakticky odzkoušet komerční softwarové produkty pro komplexní správu certifikačních autorit. Tyto produkty jsou velice drahé a společnosti je nenabízí k testování ani pro studijní účely.

# 8 Závěr

Cílem této práce bylo zanalyzovat současnou problematiku certifikátů a certifikačních autorit. Pro tuto analýzu je potřebná znalost nejen autentizačních metod ale hlavně obsahu digitálního certifikátu. Proto prvním krokem bylo seznámení s autentizačními metodami, jejich popisem a možnostmi praktického využití. Navazuje rozbor digitálních certifikátu, jeho položek, druhů, využívaných šifrovacích algoritmů, hašovacích funkcí a komunikačních protokolů. V další části byl popsán životní cyklus certifikátu, od vydání, postupu ověřování až po předčasné ukončení platnosti nebo obnovení.

Hlavní část práce byla zaměřena na analýzu certifikačních autorit, které mají akreditaci pro vydávání kvalifikovaných certifikátů. Na základě analýzy jejich certifikačních politik, činnosti, nabízených služeb, uživatelské podpory, technických parametrů a cen bylo provedeno doporučení, které by mělo pomoci koncovým uživatelům při výběru vhodné certifikační autority.

V praktických ukázkách bylo provedeno vytvoření nové certifikační autority a vygenerování klientských a serverových certifikátů a také seznamu zneplatněných certifikátů. Tyto ukázky byly realizovány v několika operačních systémech. Vygenerované certifikáty byly použity k vytvoření zabezpečeného spojení na webovém serveru Apache s nainstalovaným redakčním systémem Joomla!

V současné době jsou digitální certifikáty založeny na matematických a kryptografických technologiích. Ale jak již bylo naznačeno v úvodní části práce, v budoucnosti se počítá s rozšířením technologií hlavně o biometrické metody autentizace, především otisk prstu nebo snímání oční duhovky či sítnice. Tyto metody budou využity ke zvýšení spolehlivosti při vícefaktorové autentizaci. V některých státech se již uvažuje o vydávání občanských průkazů, které zároveň budou obsahovat čip s digitálním certifikátem. Lze tedy očekávat prudký vývoj ve využívání těchto technologií zejména v komerční sféře jako je bankovnictví, elektronické obchodování ale také v komunikaci s úřady státní správy apod. Přínosem ve využívání digitálních certifikátů je nejen zvýšení bezpečnosti elektronické komunikace ale také její zjednodušení a úspora času. Uživatelé budou moci potřebné záležitosti vyřizovat ze svého domova a nebudou muset na úřadech stát ve frontách nebo se podřizovat úředním hodinám.

Bohužel mezi uživateli je zatím malá povědomost o možnostech, které přináší využívání digitálních certifikátů. Znovu je tedy potřeba zopakovat, jak důležité je zahrnout do procesu přípravy budoucích učitelů informatiky i toto téma. Budoucí

učitelé musí mít přehled o současném vývoji, možnostech a výhodách, které tyto metody přinášejí, aby je dokázali zařadit do výuky vhodným způsobem. V tomto směru by tato práce mohla být přínosem, protože přináší ucelený náhled na celou problematiku a shrnuje téma v přehledné formě. Práce by proto mohla být podkladem při tvorbě přednášek nebo cvičení, zaměřených na výuku týkající se bezpečné elektronické komunikace.

Protože v zahraničí působí velké množství certifikačních autorit, bylo by určitě velmi zajímavé a přínosné rozšířit výzkum i tímto směrem. Tyto autority pravděpodobně nenabízí kvalifikované certifikáty, odpovídající českým právním normám ale samozřejmě se nabízí využití komerčních certifikátů. Zajímavé by bylo nejen cenové srovnání ale především srovnání technických parametrů a nabízených služeb.

Dalším směr možného výzkumu představují komerční softwarové produkty pro správu certifikačních autorit. Pro tuto práci se mi nepodařilo získat testovací verzi žádného produktu, protože je společnosti ke studijním účelům nenabízí. Jihočeská univerzita však určitě disponuje možnostmi, jak tyto produkty pro testovací účely získat. Přínosem by pak bylo srovnání těchto drahých komerčních produktů s běžně dostupnými softwarovými nástroji, které v této práci byly prakticky odzkoušeny.

Tématem PKI se zabývá mnoho literatury, žádná však neřeší problematiku samotných certifikačních autorit. Tato práce shrnuje technické možnosti a nabídku služeb všech českých certifikačních autorit oprávněných k vydávání kvalifikovaných digitálních certifikátů. Proto může být přínosem pro uživatele, kteří hledají potřebné informace nebo pro volbu vhodné certifikační autority nebo její alternativy.

Téma digitálních certifikátů je natolik rozsáhlé, že je velmi obtížné popsat všechny důležité informace v rozsahu diplomové práce. Pro komplexní zpracování všech detailů a podrobností by bylo nutné počítat s daleko rozsáhlejší publikací.

# Literatura a zdroje


Andrew, L. *Bezpečnost sítí na maximum*. Praha: Computer press, 2006. 280 s. ISBN 80-251-0805-8.

Algoritmy.net. *Algoritmus RSA.* [online]. Dostupné z WWW: <http://www.algoritmy.net/article/4033/RSA>.

Bíbr, I. *Ubuntu 10.04 CZ, Praktická příručka uživatele Linuxu*. Brno: Computer Press, 2010. 366 s. ISBN 978-80-251-3121-3.

Clever and smart. *Jak vybrat vhodnou autentizační metodu* [online]. Dostupné z WWW: <http://www.cleverandsmart.cz/autentizace-jak-vybrat-vhodnou-autentizacni-metodu/>.

Clever and smart. *Politika účtů a hesel* [online]. Dostupné z WWW: <http://www.cleverandsmart.cz/autentizace-politika-uctu-a-hesel>.

Česká pošta, s. p., *Certifikační politika PostSignum,* verze 2 [online]. Dostupné z WWW: <http://www.postsignum.cz>.

Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*, 2. aktualizované vydání. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6.

Dostálek, L., Kabelová, A. Velký *průvodce protokoly TCP/IP a systémem DNS*, 5. aktualizované vydání. Praha: Computer press, 2008. 488 s. EAN 9788025122365.

eIdentity, a.s., *Certifikační politika eIdentity*, verze 2.2 [online]. Dostupné z WWW: <http://www.eidentity.cz>.

Hernady, R. *Zavedení hash algoritmů SHA-2 v prostředí OS Microsoft Windows* [online]. [cit. 2011-1-28]. Dostupné z WWW: <http://www.lupa.cz/clanky/zavedeni-hash-algoritmu-sha-2-v-prostredi-ms-win/>.

Kolektiv pracovníků Ústavu pro jazyk český AV ČR. *Pravidla českého pravopisu, školní vydání včetně Dodatků*, 2. vydání. Praha: Fortuna, 2003. ISBN 80-7168-913-0.

Lorenc, V., Matyáš, V. *Autentizační HW a možná vylepšení.* Zpravodaj ÚVT MU, 2007. ISSN 1212-0901.

Ministerstvo vnitra. *Portál Veřejné správy České republiky* [online]. Dostupné z WWW: <http://portal.gov.cz>.

National Institute of Standarts and Technology. *FIPS Publications* [online]. Dostupné z WWW: <http://csrc.nist.gov/publications/PubsFIPS.html>.

Nápravník, J. *Jsou čipové karty bezpečné?* [online]. Dostupné z WWW: <http://www.lupa.cz/clanky/jsou-cipove-karty-bezpecne/>.

Popelka, A. *Metody autentizace sběrové centrály a koncových zařízení* [online]. Dostupné z WWW: <http://www.ais-brno.cz/vyvoj/zprava_09.pdf?lang=cz>.

První certifikační autorita, a.s., *Certifikační politika*, verze 3.1 [online]. Dostupné z WWW: <http://www.ica.cz>.

Rahmel, D. *Joomla! Podrobný průvodce tvorbou a správou webů*. Brno: Computer Press, 2010. 382 s. ISBN 978-80-251-2714-8.

Stanek, W. *Microsoft Windows Server 2008, Kapesní rádce administrátora.* Brno: Computer Press, 2008. 704 s. ISBN 978-80-251-1936-5.

Svoboda, J. *Seminář PKI* [online]. Dostupné z WWW: <http://www.cesnet.cz/akce/20031204/karty.pdf>.

Vysoké učení technické v Brně, Fakulta informačních technologií. *STRaDe* [online]. Dostupné z WWW: <http://strade.fit.vutbr.cz>.

## Použité zkratky

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ASN.1 | Jazyk pro popis dat v digitálním certifikátu |
| CA | Certifikační autorita |
| CCD | Charge-Coupled Device |
| CRL | Certificate Revocation List |
| CRMF | Certificate Request Message Format |
| DES | Data Encryption Standard |
| DN | Distinguished name (jedinečné jméno) |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| FIPS | Federal Information Processing Standards |
| FTP | File transfer protocol |
| HTTP(S) | Hypertext Transfer Protocol (Secure) |
| IMAP | *Internet Message Access Protocol* |
| JČU | Jihočeská univerzita |
| MD5 | Message – Digest algorithm (hašovací funkce) |
| MD5 | Message-Digest algorithm |
| NIST | National Institute of Standarts and Technology |
| OCSP | On-line Certificate Status Protocol |
| PKCS | Public Key Cryptographic Standards |
| POP3 | Post Office Protocol |
| RA | Registrační autorita |
| ROM | Read Only Memory |
| RSA | Rivest, Shamir, Adleman |
| SHA | Secure Hash Algorithm (hašovací funkce) |
| SHA | Secure Hash Algorithm |
| SMTP | Simple Mail Transfer Protocol |

| | |
|---|---|
| SSL | Secure Sockets Layer |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport Layer Security |
| USB | Universal Serial Bus |
| X.509 | Definice formátu digitálního certifikátu |