Porovnání certifikačních autorit Thawte a Prvej slovenskej certifikacnej autority (PSCA)

Comparison CA Thawte and Prva slovenska certifikacna autorita (PSCA)

Bc. Peter TOMAŠČÍK

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Peter TOMAŠČÍK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Porovnání certifikačních autorit Thawte a Prvej slovenskej certifikacnej autority (PSCA)**

Zásady pro vypracování:

1. **Proveďte průzkum informačních zdrojů k danému tématu a proveďte jeho literární rešerši.**
2. **Popište současný stav a proveďte analýzu využití konkrétních technologií.**
3. **Porovnejte technologie Thawte a PSCA a navrhněte formou projektu vhodnou implementaci.**
4. **Realizujte zvolené řešení a toto diskutujte.**
5. **Vyslovte závěry týkající se implementace a zadání práce.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **POŽÁR, Josef. Informační bezpečnost. 2005. 311 s. ISBN 8086898385.**
2. **NORTHCUTT, Stephen, et al. Bezpečnost sítí na maximum : Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. [20–?]. 592 s. ISBN 8025106977.**
3. **DOSEDĚL , Tomáš. Počítačová bezpečnost a ochrana dat. 2004. 200 s. ISBN 8025101061.**
4. **BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 2008. 2008 s. ISBN 9788072634651.**
5. **BITTO, Ondřej. 333 tipů a triků pro Internet. 2007. 120 s. ISBN 9788025115862.**
6. **DOSTÁLEK , L., VOHNOUTOVÁ , M. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. [200–]. 350 s. ISBN 8025108287.**
7. **DOSEDĚL, Tomáš . 21 základních pravidel počítačové bezpečnosti. 2005. 52 s. ISBN 8025105741 .**
8. **ROSEBROCK, Eric, FILSON , Eric . Linux, Apache, MySQL a PHP : Linux, Apache, MySQL a PHP. 2005. 344 s. ISBN 8024712601 .**

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

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

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

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Porovnanie certifikačných autorít Thawte a PSCA. Ponuka a typy certifikátov, spôsob objednávania a ergonómia prace s rozhraním na vystavenie certifikátov. Práca a inštalácia testovacích certifikátov. Validácia certifikátov a ich použitie na Slovensku.

Kľúčové slova:

PSCA, Thawte, certifikát, elektronický podpis, certifikačná autorita, webserver certifikát, zákon o elektronickom podpise.

ABSTRACT

The Thawte and the PSCA certification authorities comparison. Options and the types of certificates, ordering methods and ergonomics of work with interface to issue certificates. Test certificates service and installation. Validation of certificates and their use in Slovakia.

Keywords:

PSCA, Thawte, the certificate, electronic signature, certification authority, a web server certificate, the Law on Electronic Signatures,

Ďakujem vedúcemu práce, doc. Mgr. Romanovi Jaškovi, Ph.D. , za jeho cenné rady a vedenie, bez ktorých by práca nikdy nezískala tento obsah ani formu.

Ďakujem svojej manželke a dcére za ich lásku, podporu a trpezlivosť počas celého štúdia.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

1 ÚVOD

Vďaka rozvoju informačných technológií sa používanie elektronických dokumentov stalo každodennou súčasťou života väčšiny obyvateľov vyspelých krajín. Dokumenty v elektronickej forme postupne nahrádzajú papierové dokumenty.

Inak tomu nie je ani na Slovensku a je pravdepodobné, že tento trend bude i naďalej stále silnieť. Skutočnosť, že používanie elektronických dokumentov sa rozšírilo do všetkých oblastí súkromného a verejného života, so sebou priniesla aj nové požiadavky na bezpečnosť informácií uložených v digitálnej forme.

V mnohých prípadoch totiž nestačí dokument len vytvoriť, je potrebné ho aj podpísať. Týmto autor dokumentu adresátovi okrem iného zaručuje, že dokument skutočné vytvoril on, a že s obsahom dokumentu súhlasí. Dokumenty v papierovej forme podpisujeme vlastnoručným podpisom. Aby sme mohli spoľahlivo používať elektronické dokumenty, bolo potrebné nájsť spôsob, akým by sa dali elektronické dokumenty podpisovať a vytvoriť mechanizmus, ktorý by bol analógiou k vlastnoručnému podpisu, t.j. poskytoval rovnaké bezpečnostné záruky ako vlastnoručný podpis. Túto funkciu vo svete digitálnych (elektronických) dokumentov plní elektronický podpis založený na digitálnom podpise – digitálnom certifikáte.

Na overovanie distribúciu a kontrolu platnosti digitálnych certifikátov slúžia organizácie s názvom certifikačná autorita. V súčasnosti je na trhu niekoľko zavedených a etablovaných certifikačných autorít. Jedná sa o spoločnosti pôsobiace na globálnom alebo lokálnom trhu, spĺňajúce legislatívne normy daného trhu. Táto práca pojednáva o dvoch takýchto registračných autoritách. Sú to druhá najväčšia registračná autorita na svete Thawte a slovenská certifikačná autorita PSCA.

1.1 Ciele diplomovej práce

Cieľom mojej diplomovej práce je v prvom rade ponúknuť čitateľovi základný prehľad v oblasti informačnej bezpečnosti a kryptológie, oboznámiť ho s infraštruktúrou verejného kľúča, ozrejmiť funkciu certifikátov verejných kľúčov a úlohu certifikačných autorít. Najdôležitejším cieľom je ale porovnať dve certifikačné autority pôsobiace na Slovensku a to Prvú slovenskú certifikačnú autoritu PSCA a komerčne najúspešnejšiu certifikačnú

autoritu na Slovensku Thawte. Analyzovať ponúkané druhy certifikátov ako aj porovnať ich použitie na Slovensku.

Popritom je cieľom mojej diplomovej práce aj ozrejmiť spôsob práce s testovacím webserver certifikátom oboch certifikačných autorít a ukázať, ako sa má certifikát vytvárať a inštalovať v prostredí Windows.

1.2 Štruktúra diplomovej práce

Diplomová práca je určená predovšetkým pre administrátorov web serverov, webmásterov, programátorov aplikácií na prácu s elektronickými podpismi, ale aj používateľov týchto aplikácií.

Delí sa na kapitoly. V úvodnej kapitole sa čitateľ dostáva do problému, a dozvedá, o čom diplomová práca je. Vzhľadom na široké spektrum potenciálnych čitateľov, diplomová práca ďalej obsahuje kapitolu o informačnej bezpečnosti a kryptológii, v ktorej sú spomenuté aspoň základné informácie a definície pojmov z oblasti týchto vedných disciplín. Táto kapitola je určená predovšetkým pre používateľov, ktorí nemajú potrebné informatické vzdelanie, pre pochopenie základných pojmov.

Potom nasleduje kapitola o infraštruktúre verejného kľúča, v ktorej sú informácie o certifikátoch, certifikačných autoritách, ich úlohách, vzájomných vzťahoch a štruktúre. Je určená najmä pre používateľov a programátorov, aby sa oboznámili s realizáciou PKI.

Najdôležitejšia je kapitola o certifikačných autoritách PSCA a THAWTE, v ktorej sa nachádzajú analýzy jednotlivých certifikačných autoritách a certifikátoch ktorá ponúkajú. Je určená pre všetkých, ktorí majú záujem dozvedieť sa o možnostiach jednotlivých certifikačných autoritách a možnostiach ich použitia v praxi, od odborníkov po laikov.

Každá kapitola sa podľa významového obsahu jednotlivých častí môže deliť na podkapitoly. Podľa úrovne vedomostí môže čitateľ kapitoly, ktorých obsah je pre neho známy preskočiť. V prípade potreby v nich nájde presné definície pojmov, pre prípad, že by mu bol niektorý pojem neznámy, alebo by sa len potreboval uistiť, v akom význame sa pojem v práci používa.

V závere diplomovej práce sú zhrnuté výsledky, nájdeme tu zoznam použitých skratiek, zoznam použitej literatúry a obsah CD s prílohami.

I. TEORETICKÁ ČASŤ

2 ZÁKLADNÉ POJMY

Diplomová práca pojednáva o jednom z prostriedkov na zaistenie bezpečnosti elektronických dokumentov, o elektronickom podpise, webových certifikátoch a možnostiach certifikačnej autority PSCA a THAWTE. Elektronický podpis je informácia pripojená k elektronickému dokumentu, ktorá má niekoľko dôležitých funkcií. Slúži predovšetkým na zabezpečenie integrity a autentickosti ním podpísaných elektronických dokumentov. Overovanie elektronického podpisu vytvoreného neznámym podpisovateľom si vyžaduje poznanie verejného kľúča, ktorý tvorí pár so súkromným kľúčom použitým pri vytváraní elektronického podpisu, identifikáciu držiteľa súkromného kľúča.

Obe funkcie plní certifikát verejného kľúča, ktorý pre držiteľa súkromného kľúča vydala dôveryhodná tretia strana, tzv. certifikačná autorita (CA). Certifikačná autorita overila totožnosť držiteľa súkromného kľúča, overila, či predložený verejný kľúč, na ktorý má vydať certifikát tvorí pár so súkromným kľúčom podpisovateľa, ktorý žiada o vydanie osvedčenia. Verejný kľúč a meno držiteľa certifikátu (držiteľa súkromného kľúča) je zapísané v certifikáte, ktorý certifikačná autorita vydala a podpísala svojim elektronickým podpisom.

Overovateľ elektronického podpisu overí elektronický podpis vydavateľa certifikátu, zistí, či je certifikát platný a ak áno, pomocou verejného kľúča z certifikátu overí elektronický podpis. Meno uvedené v certifikáte je potom meno človeka, ktorý elektronický podpis vytvoril.

Celá táto procedúra má niekoľko nedostatkov. Skôr, ako overovateľ môže použiť verejný kľuč z certifikátu na overenie elektronického podpisu, potrebuje overiť elektronický podpis na certifikáte. Na to potrebuje poznať verejný kľuč certifikačnej autority, ktorá certifikát vydala. Ak to nie je certifikačná autorita, ktorej verejný kľuč overovateľ pozná (napríklad certifikačná autorita, ktorá mu vydala certifikát), podpis na certifikáte overuje na základe certifikátu verejného kľúča, ktorý certifikačnej autorite vydala iná certifikačná autorita. Tento proces nie je nekonečný a pravidlá upravujúce používanie elektronických podpisov vylučujú cykly. V hierarchickej infraštruktúre verejného kľúča (PKI - public key infrastructure) sa overovateľ po niekoľkých krokoch dostane k najvyššej CA, tzv. koreňovej CA, ktorej verejný kľuč poznajú (teda mali by poznať) všetci používatelia elektronických podpisov z domény danej koreňovej CA.[1]

Ale je tu ďalší problém. Z bezpečnostných dôvodov, je obmedzená životnosť certifikátu a certifikát sa môže kedykoľvek počas svojej životnosti zrušiť. Certifikát ktorý bol zrušený, nemožno použiť na overenie elektronického podpisu. Certifikačná autorita je povinná pravidelne vydávať zoznamy zrušených certifikátov (každých 24 hodín). Každý takýto zoznam zrušených certifikátov je podpísaný elektronickým podpisom, overený a platia rovnaké pravidlá ako u bežných elektronických podpisov. Okrem toho, aby sme si mohli byť istí vystaveným elektronickým podpisom, a kedy prišlo udalosti (doručenie elektronického dokumentu, vytvorenie elektronického podpisu, download, zrušenie zoznam, atď) je možne vytaviť a vydať akukoľvek časovú pečiatku, čo je v podstate elektronický podpis na hash (digitálny odtlačok).[2]

3 ZÁKLADY INFORMAČNEJ BEZPEČNOSTI A KRYPTOLÓGIE

Informačná bezpečnosť je vedná disciplína, ktorej hlavnou úlohou je najmä ochrana informácií a informačných systémov pred hrozbami počas celého ich životného cyklu. Pre dosiahnutie svojich cieľov využíva informačná bezpečnosť aj poznatky iných technických, ale aj humanitných vedných odborov, pričom najužšie prepojená je práve s kryptológiou.[4]

Kryptológia je vedná oblasť, ktorá sa zaoberá konštrukciou a analýzou kryptosystémov. Spočiatku sa kryptológia upriamovala na zabezpečenie dôvernosti údajov, teda na šifrovanie. Neskôr sa začala zaoberať aj ostatnými požiadavkami na integritu údajov, autentickosť, nepopierateľnosť konania, či časovú súslednosť. [3]

3.1 Informačná bezpečnosť

Moderná spoločnosť postupne prechádza pri spracovávaní údajov k automatizácii. Výhodou automatizovaného spracovania informácií je predovšetkým možnosť spracovať veľké množstvá informácií. K tomu je potrebné využívať informačné systémy založené na informačných a komunikačných technológiách (IKT). Takýto systém sa skladá z hardvéru, kam patria nielen počítače, ale aj ostatné zariadenia, či káble, zo softvéru – operačných systémov a aplikácií, a z dát - informácií, ktoré systém spravuje. Jeho prevádzka je závislá od ďalších faktorov, akými sú hlavne fyzická organizácia systému, rozmiestnenie hardvéru, spôsob softvérového riešenia systému a v neposlednom rade aj technické a legislatívne normy, pravidlá, zvyklosti a skúsenosti.[1]

Súhrn takýchto faktorov, ktoré nejakým spôsobom ovplyvňujú chod a funkčnosť systému, nazývame bezpečnostné okolie systému. Patria sem všetky entity nachádzajúce sa mimo systému. Väčšinou sa zaujímame iba o také okolie, s ktorým systém vzájomne posobí.. Pomyselnú deliacu čiaru medzi systémom a jeho okolím budeme nazývať hranica IKT systému. IKT systémy je potrebné podrobne popísať, aby bolo možné zabezpečiť ich spoľahlivosť, ochranu a bezpečnosť. IKT systém popisujeme na rôznych úrovniach abstrakcie, aby sme sa vyhli zbytočné zložitým popisom, ktoré sú nie vždy žiadané. IKT systémy sa popisujú na základe medzinárodných štandardov. [4]

3.1.1 Informačný a komunikačný systém

Informačný a komunikačný systém definujeme ako systém technických a programových prostriedkov, ktorých úlohou je zber, prenos, spracovanie, ukladanie a uchovanie informácií. Je zriadený pre dosahovanie určených cieľov a plnenie definovaných úloh. IKT systém tvorí logický celok, ktorý obsahuje samostatné časti, nazývané položky - assets. Položkami môžu byt aj nemateriálne entity, údaje, znalosti, dobré meno organizácie, čí schopnosť poskytovať služby. Hrozba je akákoľvek udalosť, ktorej následkom je odchýlka od pravidiel, upravujúcich činnosť IKT systémov. Ak takáto udalosť nastane, hovoríme, že hrozba bola naplnená, prišlo k bezpečnostnému incidentu. O naplnenie hrozby, prípadne jej využitie, sa môžu pokúšať aj konkrétne osoby, v takomto prípade ide o útok, osoby označujeme za útočníkov. Okrem incidentov zapríčinených vedomým konaním ľudí, môže nastať situácia, kedy dôjde k naplneniu hrozby v dôsledku neúmyselného konania, prípadne v dôsledku technickej poruchy. Osoba, zariadenie alebo skutočnosť, ktorá zapríčinila naplnenie hrozby sa označuje pojmom nositeľ hrozby. Výsledky uskutočnenia hrozby nazývame dopady alebo dôsledky.[5]

Aby mohli nastať bezpečnostné incidenty, je potrebné, aby mal systém tzv. slabé miesta - zraniteľnosti. Sú to vlastnosti, nedostatky alebo riešenia systému, ktoré umožňujú hrozbu realizovať. Každý bezpečnostný incident nastáva s určitou pravdepodobnosťou a má pre systém nejaké dôsledky. Oba tieto faktory sa súhrnne označujú ako bezpečnostné riziko. Riziko je strednou hodnotou dôsledkov naplnenia hrozby, narastá s rastúcou pravdepodobnosťou naplnenia hrozby ako aj s rastúcim rozsahom dôsledkov pri naplnení hrozby.

Pri popise každého IKT systému je dôležitá analýza rizík - odhad pravdepodobnosti výskytu bezpečnostných incidentov a analýza dopadu a dôsledkov týchto incidentov na systém. Rovnako dôležité je aj definovať bezpečnostné opatrenia, teda pravidlá a prostriedky na elimináciu rizík a zníženie pravdepodobnosti naplnenia hrozieb. Podľa rizika možno hrozby rozdeliť do troch základných skupín - kritické, stredne závažné a nepodstatné. Podľa charakteru hrozby sa potom navrhujú, realizujú a kontrolujú konkrétne bezpečnostné opatrenia.[4]

3.1.2 Ciele informačnej bezpečnosti

Úlohou informačnej bezpečnosti je však nielen ochrana systému, ale aj ochrana informácií, ktoré systém spracováva a uchováva. Základné ciele informačnej bezpečnosti sú integrita údajov, dôvernosť údajov, dostupnosť, autentickosť, nepopierateľnosť konania a časová súslednosť. Integrita údajov zaručuje, že údaje sa počas ich prenosu nezmenia, či už úmyselným konaním tretej osoby, alebo v dôsledku zníženej kvality prenosového kanála, či iných faktorov. Rovnako u uložených či zálohovaných údajoch treba zamedziť neautorizovaným zmenám obsahu. Aby bolo možné zaručiť integritu údajov, je potrebné, v čo najväčšej miere zabrániť zmenám prenášaných údajov. Vo všeobecnosti nie je možné na 100% zamedziť poškodeniu, či zmene údajov dôsledkom technických chýb alebo nepriaznivých vplyvov prostredia. Do istej miery možno chyby vzniknuté vplyvom prostredia eliminovať použitím samo opravných kódov, ktoré sú schopné detekovať a opraviť chyby malého rozsahu. Pre zaistenie integrity údajov je rovnako potrebná schopnosť všetkých komunikujúcich strán identifikovať prípadné zmeny v prenášaných údajoch. Takúto schopnosť dosahujeme pomocou hašovacích funkcií, hašovacích funkcií s tajným kľúčom a elektronických podpisov.[6]

IKT systémy veľakrát pracujú s údajmi, ktoré sú určené len pre istú skupinu ľudí. Je dôležité, aby prístup k takýmto informáciám mali len oprávnené osoby. Hovoríme, že tieto informácie sú dôverné. Zamedziť prístupu neoprávnených osôb k údajom a tým ich kompromitácii, teda zabezpečiť dôvernosť údajov, možno metódou riadenia prístupu. Prístup k údajom je povolený len oprávneným osobám. Spoľahlivejšia metóda je šifrovanie. Zamedzuje útočníkom prístup k údajom aj v prípade neoprávneného odpočúvania komunikačného kanála, čo prvá metóda zabezpečiť nedokáže.

Dostupnosť informácií znamená, že informácie sú oprávneným osobám k dispozícii vtedy, keď ich potrebujú, v požadovanom rozsahu a na určenom mieste. Dostupnosť údajov nie je možné zabezpečiť za každých okolností. Dôsledkom úmyselných útokov, vplyvov prostredia, či technických porúch môžu nastať situácie, kedy sa údaje stanú dočasne nedostupnými. V niektorých prípadoch, ako sú napríklad trvalé poškodenia pevných diskov, sa informácie môžu stať nedostupnými natrvalo. Keď sa hovorí o dostupnosti, vždy je potrebné určiť maximálny čas, počas ktorého sa vzniknuté príčiny nedostupnosti údajov odstránia a obnoví sa oprávneným osobám prístup k informáciám.

Dostupnosť je väčšinou zabezpečovaná použitím záložných zdrojov, zálohovaním, archivovaním alebo zrkadlením údajov na diskových poliach. Pod autentickosťou rozumieme schopnosť spoľahlivo určiť pôvod informácií, overiť identitu osoby, ktorá dokument vytvorila, a pritom zaručiť, že dokument nebol pozmenený, a to dokonca ani samotným autorom dokumentu.

Prostriedkom na zabezpečenie autentickosti údajov je elektronický podpis. Závisí totiž od obsahu dokumentu, čím je zabezpečené, že informácia sa nezmení, a na jeho vytvorenie je potrebná znalosť súkromného kľúča autora, čím je zabezpečená identifikácia autora dokumentu. Nepopierateľnosť konania zaručuje, že osoba zúčastnená na komunikácii, prípadne modifikácii údajov, nie je schopná poprieť vykonanie daných akcií. Inými slovami, v prípade potreby je možné dokázať, že konkrétnu akciu vykonala konkrétna osoba. Napríklad takto nie je možné odmietnuť vykonanú objednávku tovaru, alebo chybu pri editácii a zmene údajov, či už úmyselnú alebo neúmyselnú.

Časová súslednosť umožňuje odhaliť existenciu údajov v čase a zistiť postupnosť vykonávania akcií, určiť ich vzájomnú súslednosť. Najjednoduchším riešením je pridať k informácii údaj o aktuálnom čase. Treba však ošetriť prípadnú entropiu jednotlivých subjektov pracujúcich s informáciami.[4]

3.1.3 Bezpečnostné funkcie a požiadavky

Spomenuté ciele dosahujeme pomocou bezpečnostných funkcií. Pravdaže, nie vždy vyžadujeme všetky ciele naraz. Funkčné bezpečnostné požiadavky určujú, ktoré bezpečnostné funkcie má IKT systém poskytovať. Realizácia funkcií poskytovaných systémom nemusí byt dostatočná, prípadne môže byt defektná. Dôveryhodné systémy musia spĺňať popri funkcionálnych bezpečnostných požiadavkách aj požiadavky na bezpečnostné záruky. Ich úlohou je poskytnúť dôveru, že bezpečnostné funkcie sú dostatočné a správne implementované. [7]

3.2 Kryptológia

Pri komunikácii dvoch jednotlivcov, si títo medzi sebou posielajú informácie väčšinou zapísané v podobe textu. Takto posielaný text, ktorého obsahom je daná informácia, nazývame správa alebo údaj. Matematicky je správa postupnosť slov nad abecedou. Takáto správa sa posiela od jedného spoluúčastníka komunikácie k druhému pomocou

prenosového kanála. Takto prenášanú správu môže zachytiť protivník odpočúvajúci komunikáciu. Aby sa predišlo zneužitiu alebo modifikácii informácie uloženej v správe týmto útočníkom, je potrebné, aby sa správa neposielala po prenosovom kanáli v otvorenom tvare, ale aby bola šifrovaná.[7]

Kryptografia sa zaoberá matematickým aspektom bezpečnosti informačných systémov, najmä otázkami ako sú dôvernosť a integrita dát, autentizácia a nepopierateľnosť doručenia a pod. V zásade hlavnú časť kryptografie tvorí symetrické a asymetrické šifrovanie a jednosmerné hash funkcie. Kryptografia využíva tieto metódy šifrovania, aby ukryla citlivé údaje a informácie pred nepovoleným prístupom.

Šifrovanie je proces, v ktorom daná kryptografická metóda premení otvorený text (teda originálny tvar správy) pomocou kryptografického algoritmu a šifrovacieho kľúča do šifrovaného textu (ten potom zvyčajne vyzerá ako náhodný zhluk znakov). Tento text nie je možné dešifrovať bez adekvátneho kľúča.

3.2.1 Šifrovanie

Šifrovanie je metóda transformácie otvoreného textu na šifrový text pomocou vhodne zvoleného šifrovacieho algoritmu tak, aby bol zachovaný obsah (informácia), ale zmenená formu zápisu (text správy). Takto útočník nie je schopný získať zo zachytenej správy informáciu. Avšak toto musí byt umožnené adresátovi správy, ktorý dokáže bezchybne dešifrovať prichádzajúci šifrový text späť na odosielateľom odoslaný otvorený text. Aby sme želaný efekt dosiahli, požívame pri šifrovaní kľúče. Kľuč je popri správe jedným zo vstupov šifrovacieho algoritmu a pomocou neho algoritmus spracuje správu. Rovnako je znalosť kľúča potrebná aj pri dešifrovaní zašifrovanej správy. Kryptológia sa delí na dve časti - kryptografiu a kryptoanalýzu.[7] Obidve časti môžeme prezentovať ako samostatné vedné disciplíny. Zatiaľ čo kryptografia sa zaoberá hlavne tvorbou šifier, návrhom šifrovacích algoritmov a bezpečnostných protokolov, kryptoanalýza skúma možné hrozby a možnosti útokov na tieto štruktúry, ale aj spôsoby, ako dešifrovať zašifrovaný text.

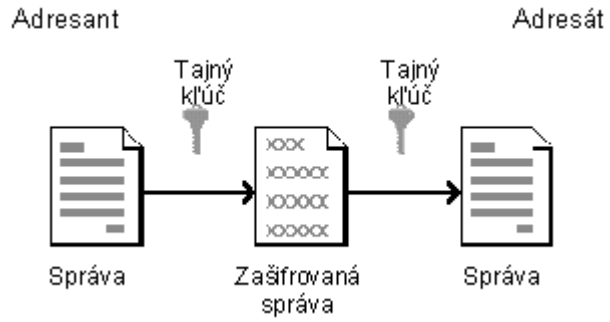
Šifrovacie algoritmy môžeme zaradiť do dvoch základných skupín. Jednou sú algoritmy symetrické, na druhej strane ide o algoritmy asymetrické. Rozdiel medzi týmito dvoma typmi je v použití šifrovacích kľúčov.[4]

3.2.2 Symetrické šifrovanie

Symetrické, tiež konvenčné šifrovanie je založené na princípe jedného kľúča, ktorým možno správu ako zašifrovať, tak aj odšifrovať. Príkladom symetrického kľúča je DES (Data Encryption Standard) vyvinutý v 70. rokoch v USA a americkou vládou tiež hojne používaný. Symetrické kódy majú ako hlavnú výhodu rýchlosť algoritmu. Na druhú stranu je nutné aby sa príjemca aj odosielateľ dohodli na jednom kľúči, ktorý budú poznať len oni dvaja. Problémom je teda distribúcia kľúča - ako dostať kľúč k príjemcovi bez toho by sa ho chopil niekto nepovolaný?

Symetrické šifrovanie je postup, ktorým jednoznačne zašifrujeme pomocou kľúča čistý text na zašifrovaný text, pričom z tohto zašifrovaného textu dostaneme pôvodný text len v prípade, že poznáme pri šifrovaní použitý kľúč. Princíp symetrického šifrovania teda spočíva v tom, že odosielateľ aj príjemca správy zdieľajú tajný kľuč, ktorým odosielateľ správu zašifruje a ktorým príjemca túto správu aj dešifruje.

Pri symetrickom šifrovaní sa na šifrovanie a rovnako aj na dešifrovanie použije ten istý kľuč. Z tohto dôvodu je nevyhnutnosťou, aby bol kľuč tajný, a aby ho poznali len oprávnené osoby, teda osoby, ktoré medzi sebou komunikujú. Predstavme si ale, že chceme zabezpečiť komunikáciu viac ako dvoch účastníkov, pričom vyžadujeme, aby každá jedna dvojica bola schopná súkromnej komunikácie.



Obrázok 1 Šifrovanie symetrickým kľúčom [13]

V takom prípade by sme museli mať samostatný kľuč pre každú z dvojíc. Pre komunikáciu n účastníkov by sme teda potrebovali n rôznych kľúčov, pričom každý účastník by musel disponovať (n-1) rôznymi kľúčmi - pre každú osobu, s ktorou by chcel komunikovať, by musel použiť iný kľuč. Takéto riešenie je neprehľadné, zložité na realizáciu a vedie k chybám.

Veľmi jednoduchú a známu aplikácií symetrického kľúča je tzv Ceasarova šifra. Jej princíp je v tom, že je vykonané abecedný posunutie po písmenách a kľúčom je číslo, o koľko sa písmeno posunie.

3.2.3 Asymetrické šifrovanie

Problém so symetrickým šifrovaním je v prenose kľúča. Kľúč K sa totiž musí preniesť cez nejaké médium. To bola v minulosti jedna z najväčších priorít medzinárodnej špionáže. Už vôbec nebolo možné kľúč preniesť cez elektronický kanál, ktorý je veľmi ľahko odpočúvateľný. Fyzický prenos je na druhej strane veľmi pomalý. Asymetrické šifrovanie tento problém rieši veľmi efektívne. Asymetrické šifrovanie je séria postupov, pri ktorých jednoznačne premeníme text T1 na text T2 pomocou kľúča Kn (n=1,2). Skladá sa z dvoch častí. Prvá časť (šifrovanie - encryption) premení text M na text T pričom použije kľúč K1 (väčšinou označovaný ako verejný kľúč - public key). Druhá časť (dešifrovanie - decryption) premení text T na text M, pričom sa použije kľúč K2 (väčšinou označovaný ako súkromný kľúč - private key). V zásade platí, že z K1 sa žiadnym matematickým postupom nedá získať K2. Súkromný kľúč K2 je kľúč, ktorý vlastní len človek, ktorému je správa určená. K1 je verejný kľúč, ktorý môže vlastniť ktokoľvek (daná osoba ho teda môže poskytovať na stiahnutie na internete). Text M zašifrovaný pomocou kľúča K1 sa teda dá dešifrovať len za pomoci kľúča K2, ktorý má len človek, ktorému je správa určená (z toho vyplýva, že text T na text M nemôže dešifrovať ani ten, kto ho zašifroval, pretože nemá súkromný kľúč K2, potrebný na túto operáciu). V skratke:

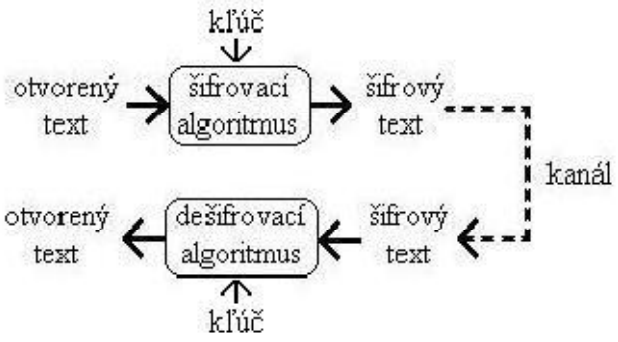
E(M, K1) = T

D(T, K2) = M

K2 != f(K1)

Posledný riadok teda hovorí, že neexistuje funkcia f, ktorá ako argument dostane K1 a vráti hodnotu K2. (5)

Šifrovací kľuč nazývaný aj verejný, je známy a nie je potrebné jeho utajenie. Ktokoľvek je schopný zašifrovať ľubovoľnú správu, ktorú potom odošle príjemcovi. Avšak dešifrovaní kľuč, nazývaný aj súkromný, je tajný a pozná ho len adresát správy. Samozrejme, tento tajný kľuč nesmie byt známy útočníkovi, aby nebolo možné prípadné dešifrovanie zachytených správ. Celá komunikácia je zjednodušene zobrazená na obrázku:



Obrázok 2 Asymetrické šiforvanie [14]

3.2.4 Manažment kryptografických kľúčov

Kľúče sú dôležitou zložkou pre zachovanie bezpečnosti šifrovacích systémov a ostatných kryptografických prostriedkov, ktoré kľúče využívajú. Bezpečnosť celého systému je priamo závislá od bezpečnosti kľúčov. Kľúče musia byt chránené pred modifikáciou a prezradením. Je dôležité zabezpečiť ich vhodné spravovanie, utajenie a riadenie prístupu počas celého životného cyklu od ich vygenerovania, pri ich distribúcii, počas ich využívania a samozrejme aj po tom, ako sa prestanú používať, je potrebné zabezpečiť ich ochranu, archiváciu, alebo prípadnú likvidáciu. Manažment kľúčov definuje protokoly a procedúry na realizáciu všetkých spomínaných akcií.

3.2.5 Hašovacie funkcie

Pri práci s elektronickými dokumentmi dochádza často k situácii, kedy je možné pre urýchlenie a zjednodušenie ich spracovania použiť namiesto pôvodného dokumentu len jeho kratšiu reprezentáciu. Takejto reprezentácii dokumentu, ktorá je obvykle podstatne kratšia ako originál, hovoríme haš alebo digitálny odtlačok. Funkciu h : X ! Y , použitú na vytvorenie odtlačku, nazývame kryptografická hašovacia funkcia. Množina odtlačkov Y je konečna, od množiny vzorov X to nepožadujeme. Hodnota x 2 X je potom pôvodný dokument a hodnota h(x) je jeho digitálny odtlačok.

Hašovacie funkcie musia mat niektoré základné vlastnosti, aby mohli byť bezpečne použité v schémach digitálnych podpisov, pri kontrole integrity, alebo v kryptografických protokoloch. Najdôležitejšou vlastnosťou hašovacích funkcií je jednosmernosť. Hovoríme, že hašovacia funkcia je jednosmerná, ak pre daný odtlačok y = h(x) nie je možné efektívne

nájsť vzor x. [3] Druhou dôležitou vlastnosťou je odolnosť voči kolíziám. Kolízia nastáva vtedy, ak majú dva rôzne dokumenty rovnaký odtlačok. Vtedy by mohlo dôjsť k zneužitiu tohto faktu nahradením jedného dokumentu druhým, pričom odtlačok by ostal rovnaký.

V súčasnosti sa používajú nové hašovacie funkcie SHA-256, SHA-384 a SHA-512 (SHA - Secure Hash Algorithm), ktoré sú súčasťou štandardu SHS (Secure Hash Standard). Čísla 256, 384 a 512 určujú dĺžku vypočítaného digitálneho odtlačku v bitoch. Súčasťou štandardu je aj staršia hašovacia funkcia SHA-1. Medzi často používané hašovacie funkcie patrí aj funkcia MD5.[4]

4 ZÁKLADY PKI

Základom PKI je bezpochyby kryptografia (šifrovanie), a to hlavne asymetrické kryptografické metódy. Hlavným prínosom asymetrickej kryptografie je použitie dvoch kľúčov namiesto jedného. Jeden z kľúčov môžem ľubovoľne zverejniť, druhý zostáva tajný. Takáto asymetria sa s výhodou využíva najmä pri rozsiahlych systémoch obsahujúcich tisícky participantov. Aj pri použití asymetrickej kryptografie však zostáva jeden zásadný problém: autenticita kľúča. Ako môže môj obchodný partner na druhej strane sveta s určitosťou vedieť, že verejný kľúč, ktorý práve dostal je naozaj môj? Ako môže vedieť, že kľúč pomocou ktorého bol vytvorený podpis na správe je platný? Na vyriešenie tohto problému bolo navrhnutých niekoľko riešení, časom sa však ukázalo, že infraštruktúra dôveryhodných tretích strán - certifikačných autorít (CA) je asi najvhodnejšia pre požiadavky dnešných distribuovaných informačných systémov. Certifikačná autorita vydáva Certifikáty verejného kľúča (PKC, Public Key Certificate), ktoré slúžia ako potvrdenie identity osoby, ktorej bol certifikát vydaný. Všeobecne uznávaným štandardom v tejto oblasti je odporučenie ITU-T X.509, ktoré definuje kostru pre budovanie bezpečnostnej infraštruktúry. [8]

4.1 Elektronický podpis

Podľa zákona č. 215/2002 Zbierky zákonov o elektronickom podpise a o zmene a doplnení niektorých zákonov zo dňa 15. marca 2002 : Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,

b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitím na jej vyhotovenie[9].

Z takto formulovanej definície vyplýva, že nie je možné elektronický podpis jedného dokumentu pripojiť k inému dokumentu a získať tak korektne podpísaný dokument, a že nie je možné pozmeniť obsah podpísaného dokumentu a zachovať korektnosť

elektronického podpisu. Ak chceme, aby nebolo možné poprieť autorstvo vlastného elektronického podpisu, musíme použiť zaručený elektronický podpis.[4]

”Zaručený elektronický podpis je elektronický podpis, ktorý musí spĺňať podmienky podľa § 3:

a) je vyhotovený pomocou skromného kľúča, ktorý je určený na vyhotovenie zaručeného elektronického podpisu,

b) možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie elektronického podpisu podľa § 2 písm. h),

c) spôsob jeho vyhotovovania umožňuje spoľahlivo určiť, ktorá fyzická osoba zaručený elektronický podpis vyhotovila,

d) na verejný kľuč patriaci k súkromnému kľúču použitému na vyhotovení zaručeného elektronického podpisu je vydaný kvalifikovaný certifikát”[9].

Elektronický podpis teda nie je len digitálny obrázok vlastnoručného podpisu, ako si mnoho ľudí myslí. Elektronický podpis je zväčša založený na digitálnom podpise, teda na kryptografickom mechanizme, ktorý je prostriedkom na realizáciu niektorých bezpečnostných funkcií, hlavne integrity a autentickosti.

Príjemca správy dokáže prostredníctvom zaručeného elektronického podpisu overiť, kto správu podpísal, a že informácia nebola po podpísaní modifikovaná.

Na druhej strane odosielateľ nemôže poprieť podpísanie správy. Elektronický podpis je informácia v elektronickej podobe. Aby nebolo možné elektronický podpis jednoducho pripojiť k ľubovoľnému dokumentu, aj k takému, ktorý podpisovateľ nepodpísal, je potrebné, aby elektronický podpis nebol závislý len na identite podpisujúceho, ale aj na dokumente, ktorý podpisuje.

Elektronický podpis má za úlohu v prípade potreby nahradiť vlastnoručný podpis. Medzi týmito dvoma typmi podpisov ale existujú dva dôležité rozdiely, a to, že elektronický podpis nie je súčasťou podpisovaného dokumentu, ako je to pri vlastnoručnom podpise, ale je jeho prídavnou informáciou, a že elektronický podpis je možné kopírovať bez toho, aby sa akokoľvek zmenil, čo samozrejme pri vlastnoručnom podpise možné nie je. Aby nemohla byť táto skutočnosť zneužitá pripojením kópie elektronického podpisu k inému dokumentu, je potrebné, aby bol elektronický podpis viazaný na konkrétny dokument.

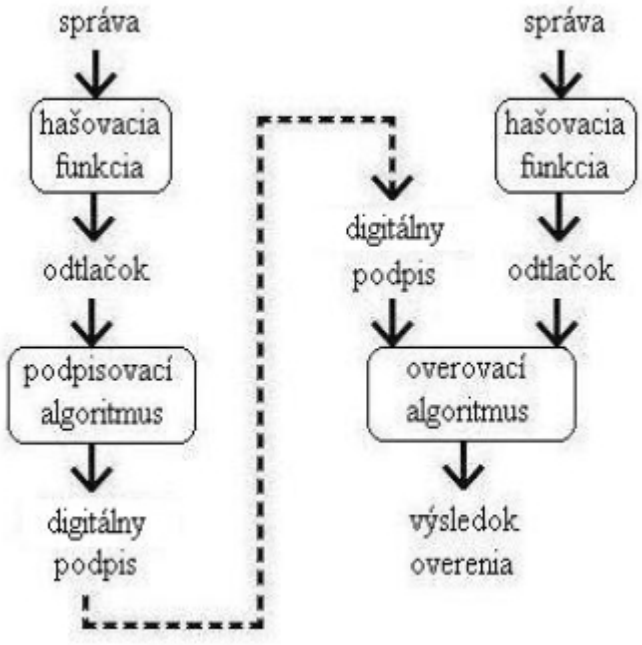
Rovnako dôležité je zabezpečiť, aby nemohol byť elektronický podpis s dokumentom skopírovaný a použitý viackrát, napríklad príkaz na prevod peňazí v banke musí obsahovať aj dodatočnú informáciu, aby bola operácia vykonaná len raz.[4]

4.1.1 Schémy digitálnych podpisov

Základom elektronických podpisov sú digitálne podpisy, teda výstupy podpisovacieho algoritmu. Digitálny podpis je dokument, alebo haš dokumentu zašifrovaný pomocou súkromného kľúča podpisovateľa. Spôsoby vytvárania a overovania digitálnych podpisov sú definované v schémach digitálnych podpisov.

Obsahujú popis algoritmu na podpisovanie a popis overovacieho algoritmu. Schémy digitálnych podpisov sú realizované v praxi pomocou systémov s verejnými kľúčmi a s použitím hašovacích funkcií. Namiesto celého dokumentu sa podpisuje len jeho digitálny odtlačok. Hašovacie funkcie používame hlavne z dôvodu zníženia časovej zložitosti asymetrických systémov, vyhotovenie a podpísanie digitálneho odtlačku je podstatne rýchlejšie ako podpisovanie celého dokumentu. Druhým pozitívom pri použití hašovacích funkcií je ochrana informácií pred niektorými typmi útokov vďaka vlastnostiam, ktoré hašovacie funkcie majú - jednosmernosť a odolnosť voči kolíziám.

Na obrázku je znázornené, akým spôsobom sú vytvárané a overované digitálne podpisy :



Obrázok 3 Schéma vytvárania a overovania digitálneho podpisu. [15]

4.2 Právna úprava elektronického podpisu

Vytvorenie elektronického podpisu bolo veľkým plusom pre elektronickú komunikáciu. Používatelia verejných sietí, najmä internetu, sa viac nemuseli obávať, či správa, ktorú obdržali, nebola počas prenosu poškodená, zmenená alebo inak úmyselne ale aj neúmyselne znehodnotená. Z právneho hľadiska len definovanie formátu elektronického podpisu nestačilo. Myšlienku elektronického podpisu bolo treba doviesť do reálnej podoby, a tým aj právne podchytiť a zakomponovať elektronický podpis, spôsob jeho vytvárania a overovania, jeho funkcie a vlastnosti, ako aj jeho právnu silu do zákona. Právnu formu elektronického podpisu na Slovensku stanovuje Zákon o elektronickom podpise a o zmene a doplnení niektorých zákonov č. 215/2002 Zb. [9] schválený NR SR 15. marca 2002. Účinnosť nadobudol 1. mája 2002, s výnimkou niektorých paragrafov, nadobúdajúcich účinnosť 1. septembra 2002.

Zákon č. 215/2002 Zb. o elektronickom podpise rozoznáva dva druhy elektronických podpisov - obyčajný elektronický podpis a zaručený elektronický podpis. Úlohou obyčajného elektronického podpisu je preukázať, že dokument bol podpísaný osobou, ktorá vlastní súkromný kľuč, teda že ide skutočne o osobu, o ktorej predpokladáme, že tento dokument podpísala. Zároveň poskytuje možnosť overenia, či počas prenosu nedošlo

k modifikácii tohto dokumentu. Zaručený elektronický podpis, ktorý musí spĺňať kritériá dané v § 4 zákona č. 215/2002 Zb. [9]zaručuje popri integrite a autentickosti údajov aj nepopierateľnosť konania podpisovateľa. V styku so štátnymi úradmi sa musí používať tento druh elektronického podpisu. Podstatou zaručeného elektronický podpisu je skutočnosť, že je vytváraný pomocou bezpečného zariadenia na vyhotovenie elektronického podpisu a na verejný kľuč je vydaný kvalifikovaný certifikát. Ak však určitá právna norma vyžaduje na právne úkony notárske osvedčenie podpisu, musí byt takto osvedčený i zaručený elektronický podpis[9].

Dňa 15. marca 2002 bol Národnou radou Slovenskej republiky prijatý zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých paragrafov. Zákon upravuje vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním elektronického podpisu, práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom. Zákon nadobudol účinnosť v plnom rozsahu dňa 1. septembra 2002. Zákon vychádza zo Smernice Európskej únie č. 1999/93/EC z decembra 1999.

Národný bezpečnostný úrad je ústredným orgánom štátnej správy pre elektronický podpis.

Vykonávacie právne predpisy k zákonu č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov účinné od 8. apríla 2009:

Vyhláška Národného bezpečnostného úradu č. 131/2009 Z.z., o formáte, obsahu a správe certifikátov a kvalifikovaných certifikátov a formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o certifikátoch a kvalifikovaných certifikátoch)

Vyhláška Národného bezpečnostného úradu č. 132/2009 Z.z., o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov

Vyhláška Národného bezpečnostného úradu č. 133/2009 Z.z., o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností

Vyhláška Národného bezpečnostného úradu č. 134/2009 Z.z., ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (o produktoch elektronického podpisu)

Vyhláška Národného bezpečnostného úradu č. 135/2009 Z.z., o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, podmienkach platnosti pre zaručený elektronický podpis, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky)

Vyhláška Národného bezpečnostného úradu č. 136/2009 Z.z., o spôsobe a postupe používania elektronického podpisu v obchodnom styku a administratívnom styku [18]

4.3 Certifikáty a infraštruktúra verejného kľúča

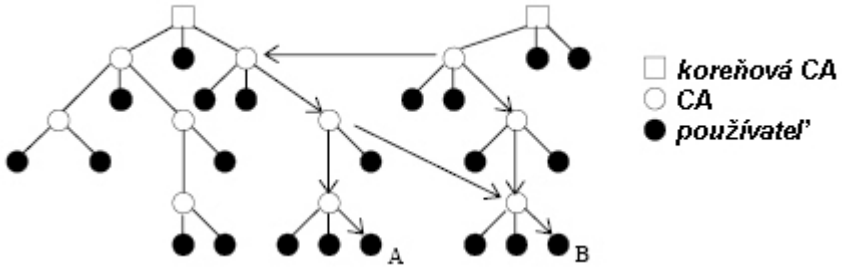
Vďaka asymetrickým kryptosystémom je možné bezpečne oddeliť súkromný a verejný kľuč a zabezpečiť publikovanie verejného kľúča. Problém je ale v tom, ako sa osoba, ktorá chce overiť nejaký podpis, dostane k verejnému kľúču pre tento podpis. Utajenie kľúča nie je potrebné, avšak musíme zabezpečiť, aby kľuč nemohol niekto modifikovať pred alebo počas prenosu k overovateľovi. Potenciálny útočník by mohol overovateľovi preposlať namiesto verejného kľúča podpisovateľa svoj verejný kľuč a týmto kľúčom podpísanú upravenú správu namiesto pôvodnej správy bez toho, aby túto skutočnosť overovateľ odhalil, keďže overenie podpisu v takomto prípade prebehne bez problémov. V súčasnosti sa na distribúciu a prenos kľúčov od podpisovateľa k overovateľovi využíva metóda dôveryhodnej tretej strany - Trusted Third Party (TTP). TTP poskytuje overovateľovi službu, ktorá mu potvrdí, že daný verejný kľuč skutočne patrí podpisovateľovi. Dôležité je, že dôveryhodnej tretej strane veria obaja účastníci, teda podpisovateľ aj overovateľ.[4]

4.3.1 Certifikát verejného kľúča

Momentálne najrozšírenejšou schémou, ktorá implementuje metódu využitia TTP, je použitie certifikátov. Certifikát verejného kľúča je elektronický dokument, ktorý viaže verejný kľuč k identite jeho držiteľa. Podľa § 6 zákona č. 215/2002 Zb.[9], certifikát verejného kľúča je potvrdenie, že kľuč z certifikátu patrí danej osobe.

4.3.2 Certifikačná autorita

Certifikačná autorita je dôveryhodná tretia strana, ktorá je zodpovedná za vydávanie, správu a rušenie certifikátov verejného kľúča. Certifikačné autority sú zoradené do štruktúr. Niekedy sa môžu využívať aj štruktúry typu všeobecných orientovaných grafov, väčšinou sú však využívané hierarchické štruktúry tak, ako je zobrazené na obrázku :



Obrázok 4 Hierarchická štruktúra certifikačných autorít[15]

Certifikačná autorita, ktorá inej certifikačnej autorite, prípadne používateľovi, vydala a podpísala certifikát, sa nachádza na vyššej úrovni ako táto certifikačná autorita či používateľ. Na vrchole každej hierarchickej štruktúry stojí koreňová certifikačná autorita. Na Slovensku zastáva miesto koreňovej certifikačnej autority Národný bezpečnostný úrad (NBÚ)[10].

Elektronický certifikát nám zaručí, že správa po ceste nebola zmenená a že ju podpísala osoba, ktorá „patrí“ k elektronickému podpisu. Zostáva však ešte uistiť sa, že máme správnu informáciu o fyzickej osobe, na ktorú sa dáta pre overovanie elektronického podpisu vzťahujú – teda kto vlastne správu elektronicky podpísal. Na to potrebujeme, aby niekto dostatočne dôveryhodný bol schopný potvrdiť, komu tento podpis patrí. Túto funkciu preberá práve certifikačná autorita. Je to fyzická alebo právnická osoba a vystupuje pri vzájomnej komunikácii dvoch subjektov ako tretí nezávislý dôveryhodný subjekt, ktorý prostredníctvom ním vydaného certifikátu jednoznačne identifikuje subjekt s jeho digitálnym podpisom. Plní teda funkciu „elektronického notára“.

Podľa § 10 zákona č. 215/2002 Zb.[9] vykonáva NBÚ na Slovensku okrem iného aj dohľad nad dodržiavaním zákona o elektronickom podpise, udeľuje a odníma certifikačným autoritám akreditáciu, vydáva osvedčenia o akreditácii a eviduje certifikačné autority pôsobiace v Slovenskej Republike. Každá certifikačná autorita poskytuje certifikačné služby, spravuje certifikáty a vykonáva certifikačnú činnosť. Certifikačnou

službou sa rozumie najmä vydávanie certifikátov, zrušovanie platnosti certifikátov, poskytovanie zoznamu zrušených certifikátov, potvrdzovanie existencie a platnosti certifikátov, vyhľadávanie a poskytovanie vydaných certifikátov. Okrem poskytovania týchto služieb sa pod certifikačnou činnosťou rozumie aj prijímanie žiadostí o vydanie certifikátu, vedenie evidencie, či prevádzka potrebných Technických zariadení.

Medzi služby poskytované certifikačnou autoritou patrí aj registrácia používateľov. Používatelia sa musia predtým, ako im bude vydaný certifikát, registrovať u certifikačnej autority. Po overení identity užívateľa, mu certifikačná autorita pridelí jednoznačné meno, pod ktorým bude môcť vytvárať elektronické podpisy. V prípade, že používateľ z ľubovoľného dôvodu nechce podpisovať dokumenty svojím menom, môže požiadať o pridelenie pseudonymu, ktorý bude používať pri podpisovaní namiesto svojho mena.

Ešte predtým ako je možné vydať nejaký certifikát je potrebné vygenerovať kľúče, konkrétne je potrebné vygenerovať pár - súkromný kľuč a verejný kľuč. Žiadny konkrétny pár nesmie byt vygenerovaný viac ako jedenkrát. Samozrejme, je potrebné zamedziť neautorizovanému prístupu k páru kľúčov.

Párové údaje sú generované na základe vybranej metódy generovania kľúčov, ktorá zodpovedá príslušnému štandardu pre elektronické podpisy. Pár kľúčov musí byt vytvorený vo vhodnom bezpečnom prostredí, teda na zariadení, ktoré splna požiadavky na vyhotovovanie zaručených elektronických podpisov podľa zákona č. 215/2002 Zb. (1) a bolo pre tento účel certifikované NBÚ. Toto zariadenie je počas generovania kľúčov zásadne pod výhradnou kontrolou používateľa. Vygenerovaný súkromný kľuč v ňom zostáva uložený i počas práce s ním, pričom je garantované, že súkromný kľuč nikdy zariadenie neopustí. Takýmto zariadením môže byt špeciálna čipová karta, alebo USB token.

Ak už je pár kľúčov vygenerovaný, certifikačná autorita overí potrebné náležitosti žiadateľa o vydanie certifikátu (doklady, vlastníctvo súkromného kľúča patriaceho k predloženému verejnému kľúču) a následne vydá žiadateľovi certifikát verejného kľúča. Každý certifikát vydaný používateľovi musí obsahovať jeho identifikáciu, jeho verejný kľuč a dobu platnosti certifikátu.

Tieto informácie podpíše certifikačná autorita svojím elektronickým podpisom. Tým berie na seba zodpovednosť za obsah vydaného certifikátu. Vydaný certifikát verejného kľúča je zvyčajne uložený na čipovej karte spolu so súkromným kľúčom používateľa. Prístup k

informáciám na čipovej karte je zabezpečený väčšinou pomocou hesla alebo PIN kódu, no môže byt zabezpečený aj biometrickou identifikačnou metódou, napríklad pomocou geometrie odtlačkov prstov, dúhovky, či sietnice.

Povinnosťou každej certifikačnej autority je vytvoriť podmienky, ktoré umožnia overovateľovi overiť platnosť certifikátu, ktorý certifikačná autorita vydala. Zrušené certifikáty sú uvádzané na zozname zrušených certifikátov - Certificate revocation list (CRL), ktorý obsahuje aj informáciu o čase, kedy bol ten ktorý certifikát zrušený. Certifikačná autorita musí pravidelne vydávať zoznam ňou zrušených certifikátov. Certifikačná politika danej certifikačnej autority určuje, ako často bude CRL vydávaný. Tieto zoznamy zrušených certifikátov musia byt prístupné komukoľvek a kedykoľvek. Spôsob zverejňovania CRL je definovaný certifikačnou politikou danej certifikačnej autority.

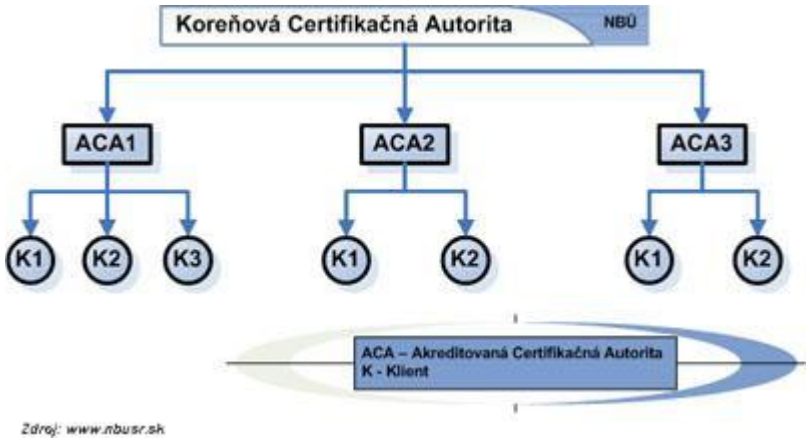
V niektorých prípadoch je potrebné pripojiť k podpisovanému dokumentu aj časovú pečiatku - informáciu o aktuálnom čase, kedy bol dokument podpísaný.

Túto informáciu je možné v prípade potreby overiť, teda určiť čas, kedy bol dokument podpísaný. Keďže nastavenie aktuálneho času môže mat každý používateľ vo svojom systéme rôzne, je potrebné zabezpečiť synchronizáciu medzi jednotlivými používateľmi. Z tohto dôvodu sa vydávanie časových pečiatok presunulo do kompetencie certifikačných autorít, ktoré zaručujú jednotnosť časových údajov pre všetkých používateľov.

4.3.3 Infraštruktúra verejného kľúča

PKI je štruktúra, ktorá má stromový charakter. Koreňom celého stromu je koreňová certifikačná autorita (KCA). U nás túto úlohu zastáva Národný bezpečnostný úrad. Táto hierarchická štruktúra zaručuje, že všetky certifikáty na nižšej úrovni (K1, K2,... a ACA1, ACA2,...) sú pravé vtedy, ak používateľ uzná pravosť KCA.

Ak je touto autoritou štát, pravosť je nespochybniteľná. Avšak nič nebráni uznať pravosť aj inej CA. Je to vždy otázka zmluvných vzťahov medzi používateľmi. Treba však brať do úvahy prípady, kedy sám štát vstupuje do takýchto vzťahov a ten často implicitne uznáva iba jedinú garantovanú autoritu (NBÚ SR) - viac nabudúce. Samozrejme uznáva v istých prípadoch aj iné, ale vždy si ponecháva právomoc vykonávať kontrolu ich činnosti.



Obrázok 5 Infraštruktúra KCA[11]

Strom na predchádzajúcom obrázku vzniká veľmi jednoducho. Každý certifikát je vytvorený podpísaním verejného kľúča majiteľa certifikátu pomocou súkromného kľúča nadradenej certifikačnej autority.

KCA má vytvorený svoj vlastný koreňový certifikát. Tento je odlišný od ostatných, ktoré sú jeho nasledovníci, v tom, že aj položka vydavateľa aj držiteľa sú rovnaké, teda je self-signed (podpísaný sám sebou). Presvedčiť sa o tom dá konkrétne na certifikátoch NBÚ. Na uvedenej stránke je vidieť všetky certifikáty vydané slovenským NBÚ.

Ako je možné vidieť, sú tam dva koreňové certifikáty. To znamená, že sú vytvorené dva certifikačné stromy. Aby bolo možné tieto stromy „prepojiť", v každom z nich sa nachádza tzv. krížový certifikát**.** Jednou z možností by bolo vytvoriť spoločnú KCA, ale to často nie je vôbec možné, preto sa používa práve technika krížových certifikátov.

Na predchádzajúcom obrázku je v strome B certifikačná autorita, ktorá vydá certifikát na verejný kľúč inej certifikačnej autority a tým sa akoby celý podstrom stromu A zaintegruje do stromu B. Je to možné aj naopak (podstrom stromu B sa zaintegruje do A.) V prípade NBÚ existujú dva krížové certifikáty. Krížový certifikát patriaci do stromu KCA1 je verejný kľúč z koreňového certifikátu stromu KCA2 podpísaný súkromným kľúčom KCA1. Podobný krížový certifikát je aj v strome KCA2, čím sú oba stromy vzájomne prepojené.[11]

4.4 Formáty elektronických podpisov

V praxi sa ukázalo, že jediný formát zaručeného elektronického podpisu je nedostacujúci na velké množstvo rôznorodých právnych účelov. Zaručený elektronický podpis má preto

viacero rôznych formátov, ktorých použitie závisí od toho, na aký účel elektronický podpis slúži. Jednotlivé formáty vymedzuje Vyhláška Národného bezpečnostného úradu č. 537/2002 Zb. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky (2) a presne špecifikuje dokument Formáty zaručených elektronických podpisov (8) vydaný NBÚ. Zaručený elektronický podpis musí byt kompatibilný v rámci celej SR a EÚ tak, aby uznával rovnaké právne požiadavky na podpis vo vzťahu k údajom v elektronickej forme rovnako ako vlastnoručný podpis vo vzťahu k papierovým dokumentom a aby bol prijateľný ako dôkaz pri súdnych sporoch. Formáty zaručených elektronických podpisov sú :

a) bez časovej pečiatky
b) s časovou pečiatkou
c) s úplnou informáciou pre overenie platnosti
d) archívny
e) kombinácie formátov podľa písmen a) až d).

Zaručený elektronický podpis bez časovej pečiatky je najjednoduchším formátom zaručených elektronických podpisov. Obsahuje identifikátor podpisovej politiky použitej pri podpisovaní a overovaní podpisu, podpisové údaje, ktoré podpisujúci do podpisu zahrnul (napríklad miesto a čas vyhotovenia podpisu, meno podpisujúcej osoby) a samotný digitálny podpis vytvorený na základe digitálneho odtlačku dokumentu, identifikátora podpisovej politiky a údajov zahrnutých do podpisu.

Zaručený elektronický podpis s časovou pečiatkou má formu zaručeného elektronického podpisu, ku ktorému je pripojená časová pečiatka vyhotovená na základe daného zaručeného elektronického podpisu.

Zaručený elektronický podpis s úplnou informáciou pre overenie platnosti má formu zaručeného elektronického podpisu s časovou pečiatkou, ku ktorému sú pripojené úplné informácie o všetkých kvalifikovaných certifikátoch verejného kľúča potrebných na overenie platnosti podpisu, ako aj úplné informácie o zoznamoch zrušených kvalifikovaných certifikátov, alebo informácie o stave kvalifikovaných certifikátov potrebných na overenie platnosti podpisu.

Archívny zaručený elektronický podpis má formu zaručeného elektronického podpisu s časovou pečiatkou, ku ktorému sú pripojené všetky údaje potrebné na overenie archívneho zaručeného elektronického podpisu. Na tieto údaje je vyhotovená časová pečiatka, ktorá je k nim pripojená.[12]

4.5 Štandardy pre elektronické podpisy

Štandardy pokrývajúce šifrovací systém RSA, Diffieho-Hellmanov protokol na výmenu kľúčov, certifikáty verejných kľúčov, algoritmy na šifrovanie, dešifrovanie, podpisovanie a na tvorbu digitálnych odtlačkov, ktoré v roku 1993 vydali RSA Laboratories (dnes už súčasťou súkromnej firmy RSA Security) sa označujú za štandard PKCS - Public Key Cryptography Standards.[13]

4.5.1 Čo je to SSL

SSL (Secure Sockets Layer) je nekomerčný otvorený protokol a v súčasnej dobe jedna z najviac používaných metód pre zabezpečenie dátových prenosov v rámci internetu medzi serverom s webovou prezentáciou a prehliadačom (používateľom).

SSL je protokol, ktorý zaisťuje šifrovanie prenášaných dát a autentizáciu servera pomocou digitálnych certifikátov. To, že sme pripojení na webové stránky zabezpečené pomocou SSL, spoznáme podľa adresy stránky, ktorá obsahuje naviac písmeno "s", napr https://www.paypal.com/ alebo podľa upozornenia prehliadača. Výhodou SSL protokolu je aj to, že webmaster pre využitie tohto zabezpečenia musí iba zabezpečiť presmerovanie na adresu s HTTPS protokolom.

Princíp funkcie SSL certifikátov je založený na asymetrickom šifrovaní, keď každá z komunikujúcich strán má dva šifrovacie kľúče - verejný a súkromný. Verejný kľúč je možné zverejniť a ak týmto verejným kľúčom dôjde na zašifrovanie dát, je zabezpečené, že tieto dáta bude môcť rozšifrovať iba majiteľ použitého verejného kľúča svojim súkromným kľúčom. SSL certifikáty by mal používať každý majiteľ webovej prezentácie, ktorý akýmkoľvek spôsobom zhromažďuje od svojich používateľov dôverné údaje vo formulároch alebo ponúka napríklad prihlasovanie na stránky pomocou hesiel. U intranetových portálov a hlavne elektronických obchodoch by malo byť používanie SSL zabezpečenia samozrejmosťou.

4.5.2 Význam certifikačnej autority

Alfou a omegou elektronickej komunikácie je bezpečnosť. Kritickým bodom je problém pravosti verejného kľúča.

Je ten, kto podpísal, skutočne tým, kto podpisoval? Je to, čo vidíme podpísané, skutočne tým, čo sa podpisovalo? Nepodstrčil nám niekto svoj verejný kľúč, aby sa mohol vydávať za niekoho iného?

Tento problém za nás rieši dôveryhodná tretia strana – certifikačná autorita.

Certifikačnú autoritu môžeme prirovnať k notárovi, ktorý potvrdzuje totožnosť. Vydaný certifikát tak možno chápať ako elektronický preukaz totožnosti. Pred vytvorením elektronického podpisu tak musíme najskôr navštíviť certifikačnú autoritu alebo kontaktné pracoviská (registračné autority) a požiadať o vydanie certifikátu. Pri vydaní certifikátu dochádza k fyzickému overeniu totožnosti. Certifikačná autorita svojim elektronickým podpisom potvrdí certifikát, ktorý obsahuje verejný kľúč a osobné údaje jeho držiteľa.

4.5.3 Možnosti využitia elektronických podpisov

Zákon spolu s naň nadväzujúcimi vyhláškami vytvorili právny rámec, ktorý upravuje použitie elektronického podpisu v styku s verejnou mocou, v administratívnom a v obchodnom styku. Zákon tu už rozoznáva elektronický podpis a zaručený elektronický podpis. Zaručený elektronický podpis je spájaný s kvalifikovaným certifikátom, ktorý používateľom vydáva akreditovaná certifikačná autorita.

V zmysle platnej legislatívy je možné v obchodnom styku používať elektronický podpis, v styku s verejnou mocou zaručený elektronický podpis.

Implementácia technológie elektronického podpisu do prostredia spoločnosti môže byť prínosná nielen pre zvýšenie bezpečnosti internej komunikácie, ale aj pre zvýšenie bezpečnosti elektronickej komunikácie s obchodnými partnermi.

Samotný elektronický podpis môže byť využitý pri:

- podpisovaní e-mailových správ v rámci spoločnosti, ale aj správ smerujúcich von z organizácie – jednoznačná identifikácia podpisujúcej osoby na strane prijímateľa podpísanej správy,

- bezpečnom doručovaní a poskytovaní dôverných informácií elektronickou poštou – šifrovanými e-mailovými správami (napr. zasielanie výplatných pások, citlivej dokumentácie, zmlúv, dôležitých finančných ukazovateľov),
- bezpečnom prihlasovaní sa do systému certifikátom – náhrada za prihlásenie pomocou mena a hesla,
- bezpečnej komunikácii s webovými stránkami – certifikát pre server umožní návštevníkom webových stránok využívať bezpečný protokol HTTPS, ktorým sa výrazne zvyšuje dôveryhodnosť servera a bezpečnosť komunikácie,
- EDI komunikácii – zavedení elektronickej výmeny štandardných dokumentov medzi dvoma nezávislými subjektmi a tým nahradenie papierovej dokumentácie elektronickými.

4.5.4 Prínos elektronizácie pre spoločnosť

Výhody elektronizácie procesov v rámci spoločnosti a zároveň výmeny informácií, citlivých dát a údajov elektronickou formou sú jednoznačné:

- Ochrana proti úniku dôverných informácií,
- určenie zodpovednosti za nesprávne dodanie údajov (napr. odosielateľ dodá nesprávny údaj a tvrdí, že chyba vznikla na strane príjemcu),
- zabránenie vzniku chýb pri prenose/prepise dokumentov,
- bezpečné doručovanie a poskytovanie dôverných informácií elektronickou poštou prostredníctvom šifrovaných e-mailových správ,
- zvýšenie celkovej bezpečnosti,
- zníženie nákladov pri nahradení papierovej komunikácie elektronickou,
- úspora času pri elektronickej komunikácii.

II. PRAKTICKÁ ČASŤ

5 SSL CERTIFIKÁTY THAWTE

THAWTE je jednou z najznámejších najuznávanejších certifikačných autorít SSL na svete. Zároveň jedným z priekopníkov digitálnych certifikátov. V súčasnej dobe je 100% vlastníkom spoločnosť VeriSign, ktorá zaujíma vedúce postavenie v bezpečnosti IT.

Certifikát THAWTE, je istotou, že pre návštevníci na pri prístupe na zabezpečené stránky z rôznych prehliadačov nebudú obťažovaný akýmikoľvek hlásením o "nedôveryhodnosti" certifikátu, ktoré sa zobrazuje pri certifikátoch neznámych autorít, keďže certifikáty THAWTE patria k takzvaným Trusted Certifikačným autoritám. Kvalita certifikátov THAWTE je už všeobecne známa a klienti pristupujúci na takto zabezpečené stránky majú väčšiu dôveru k poskytovateľovi stránok.

SSL certifikáty by mali používať všetci majitelia webových prezentácií, ktorí akýmkoľvek spôsobom zhromažďujú od svojich používateľov dôverné údaje vo formulároch alebo ponúkajú napríklad prihlasovanie na stránky pomoci hesiel. Minimálne prevádzkovateľom elektronických predajní by mal byť certifikát SSL samozrejmosťou.

5.1 Certifikáty

Spoločnosť THAWTE ponúka ako SSL, tak aj Code Signing certifikáty umožňujúce k aplikácii distribuované cez internet priradiť digitálny podpis. V mojej práci som sa zameral na certifikáty ktoré sú porovnateľné s certifikátmi vydávanými PSCA na Slovensku. To znamená serverové certifikáty. Všetky typy certifikátov THAWTE sú už štandardne predinštalované vo všetkých bežných systémoch a webových prehliadačoch. Koncový používateľ nevykonáva žiadnu dodatočnú inštaláciu a certifikáty sú dôveryhodné.

5.2 THAWTE SSL 123

THAWTE SSL 123 "Low authenticated" certifikát obsahujúci informácie len o doméne, bez akýchkoľvek ďalších údajov. Má zjednodušenú overovaciu procedúru, kedy na základe údajov z registra domén (napr. pre SK domény SK-NIC) je poslaný vlastníkovi domény e-mail s odkazom pre overenie vlastníctva domény. Tento certifikát je možné získať v priebehu niekoľkých minút.

Rozdiel medzi THAWTE Web Server Certifikát a THAWTE SSL 123 je v tom, že SSL 123 poskytuje informácie len o doméne, na rozdiel od štandardného, ktorý obsahuje ďalšie

informácie. SSL 123 sa hodí skôr pre extranetové aplikácie alebo pre www stránky, kde poskytovateľ nepovažuje za nutné uvádzať v certifikáte svoje informácie, ktoré zvyšujú dôveru klientov. [14]

5.2.1 Charakteristika certifikátu

Šifrovanie: Až 256-bit

Kompatibilita prehliadačov: Vysoká - zoznam prehliadačov a verzií

Zobrazenie v detaile certifikáte: Iba overené doménové meno

THAWTE pečať: ÁNO (THAWTE Trusted Site Seal)

Root CA: ÁNO

Obnova certifikátu (reissues): ÁNO

Možnosť zrušenia certifikátu: ÁNO

Podpora IDN domén: ÁNO

Ako náhle je certifikát na stránky nainštalovaný, zobrazí sa v prehliadači WWW stránok symbol zámku.

5.2.2 Postup vystavenia certifikátu THAWTE SSL 123

Po objednaní certifikátu SSL 123, jeho úhrade je certifikát generovaný na základe verejného kľúča - TXT request je zo strany THAWTE budu dožiadane informácie potrebné na vygenerovanie certifikátu SSL 123. Verejný kľúč (TXT request)

Zabezpečenie certifikátov je postavené na synchrónnym šifrovaní pomocou dvoch kľúčov (privátny a verejný). Verejný kľúč je možné zverejniť a ak týmto kľúčom ktokoľvek zašifruje nejakú správu (odosielané dáta), je zabezpečené, že ju bude môcť rozšifrovať len majiteľ použitého verejného kľúča svojim súkromným kľúčom.

5.2.3 Verejný kľúč pre SSL certifikáty

Verejný kľúč (TXT request), nazývaný Certificate Signing Request (CSR), je generovaný na serveri, kde je hostovaná (umiestnená) doména na ktorej bude SSL certifikát funkčný. Tento TXT request vygeneruje administrátor servera alebo poskytovateľ webhostingu.

Pre vygenerovanie verejného kľúča je nutné poznať nasledujúce informácie:

Popis

Common Name (CN) - Presný názov domény

Organization Name - Meno firmy - majiteľa domény

Organizational unit – Organizačná jednotka

Country Code - Kód krajiny

State or Province - Štát

Locality - Mesto

Key Size - Bitová hĺbka

Priklad:

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIDYDCCAskCAQAwgYQxFTATBgNVBAMTDHpvbmVyLXNlcnZlcjEXMBUGA1
UECxMOTmVqYWthIHBvYm9ja2ExHTAbBgNVBAoTFFRlc3RvdmFjaSBjZXJ0aWZp
a2F0MRMwEQYDVQQHEwpCcmF0aXNsYXZhMREwDwYDVQQIEwhTbG92YXRp
YTELMAkGA1UEBhMCU0swgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAL
03uc/vLIsAi/UIryfeS2vG3zU2mx/xBp1HrbVovkYN1TouNdvz83tK7Ocg3SuOfriKjWNk
d5T/gzx6r85XBIUhg2kFTKPN29RbMwAMOL5JV9gGX0lxhjrdp8eZsCpw+sqn0fSy7A2
6WyBmIV4yZOq6DxnonxN9QISa4saykdsdAgMBAAGgggGZMBoGCisGAQQBgjcNAg
MxDBYKNS4wLjIxOTUuMjB7BgorBgEEAYI3AgEOMW0wazAOBgNVHQ8BAf8EB
AMCBPAwRAYJKoZIhvcNAQkPBDcwNTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhv
cNAwQCAgCAMAcGBSsOAwIHMAoGCCqGSIb3DQMHMBMGA1UdJQQMMAoGC
CsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloATQBpAGMAcgBv
AHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcg
B5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDgYk
AJ1L9qpiQmoL5dNlVLkM2P6UFcMYME1cUMidPEUHEGfxOB1eTGXu8rhguJfDScUi
y9h1SOkHO8CnjCQFoYPhb/iRhaCbbu1UsNfoJG1imCP07Lr8k8gOW76zuvn+zfU5AbS
QjJf/SbXyLZO9TDbe4Y2aklRo2aeZBVm2GXz3ezjYAAAAAAAAAADANBgkqhkiG9
w0BAQUFAAOBgQADdfu6UtUIjy/9ijsPOU4Jx0oKII9fPuWSggCYNZdU1lCwjbj3nSqZ
oAIysM6b8r2ouPqT8jjNdM2/AY5laPVxbsW9e3wetNaBx973OOdHxwo8uPQcBKngRx
WEBlp/QGGbB2EvA/GYmPKrqUOIAtPazAy8yv6CPSU0deKVcXJ9fg==

-----END NEW CERTIFICATE REQUEST-----

Je rozdiel, ak je názov domény uvedený s "www" (napr. www.nazov-domeny.sk) alebo bez "www" (napr. nazov-domeny.sk). Pri prístupe na iný názov ako je v osvedčení, je zobrazované chybové hlásenie o certifikáte pre inú doménu. Je preto dôležité zvoliť správny názov, ktorý zodpovedá webovým stránkam. Vo Verejnom kľúči sa nepoužíva diakritika.

Meno firmy (majiteľa domény) musí byť identické s menom vedenom v obchodnom registri a musia sa zhodovať s informáciami uvedenými u držiteľa domény.

Na kontaktný email (osoba pre autorizáciu) uvedený v objednávke dorazí emailová správa o vykonanej žiadosti:

Od:isp_enrollmentprocess@thawte.com
Předmet: thawte SSL123 Certificate Order Confirmation

5.2.4 Overenie certifikátu

Na kontaktnú emailovú adresu majiteľa domény (na ktorú sa certifikát zriaďuje) bude zaslaná emailová správa pre jeho schválenie. Používaný emailový kontakt u domény je možné si overiť u správcu domén, napr http://www.sk-nic.sk/ pre domény SK.

Emailovú správu získame v nasledujúcej forme:

Od:isp_enrollmentprocess@thawte.com
Predmet: thawte SSL123 Certificate Approval

Aby bol certifikát čo najskôr vystavený, je potrebné prejsť na odkaz pre potvrdenie v emailovej správe a na stránkach THAWTE vystavenie certifikátu potvrdiť - tlačidlo "I approvata". Následne bude certifikát SSL 123 do cca. 30 minút vygenerovaný.

Zobrazenie stránky pre potvrdenie overenie osvedčenia:

Obrázok 6 Stránka na generovanie certifikátu

Hňeď ako je THAWTE SSL 123 certifikát vygenerovaný, je zaslaný v štandardnom formáte na technický kontakt uvedený v objednávke. Certifikát Vám je možné na požiadanie kedykoľvek predoslať.

Ak nie je kontaktný email majiteľa danej domény funkčný, je možné po dohode zaslať email na schválenie na jednu z nasledujúcich emailových schránok:

admin@nazov-domeny.sk

administrator@nazov-domeny.sk

hostmaster@nazov-domeny.sk

root@nazov-domeny.sk

ssladmin@nazov-domeny.sk

sysadmin@nazov-domeny.sk

webmaster@nazov-domeny.sk

info@nazov-domeny.sk

is@nazov-domeny.sk

it@nazov-domeny.sk

mis@nazov-domeny.sk

ssladministrator@nazov-domeny.sk

sslwebmaster@nazov-domeny.sk

postmaster@nazov-domeny.sk

5.3 THAWTE SSL Web Server

Najpoužívanejší certifikát THAWTE Overujú sa podrobnosti o doménovom mene, e-mailu, názvu organizácie, organizačnej jednotke a prebieha verbálne overenie.

Certifikát umožňuje šifrovanie s kľúčom o sile 40/56/128/256 bitov podľa podporovaného prehliadača a nastavenie webového servera.

5.3.1 Charakteristika certifikátu

Šifrovanie: Až 256-bit

Kompatibilita prehliadačov: Vysoká

Zobrazenie v detaile certifikátu: Overené doménové meno a organizácie

THAWTE pečať: ÁNO (THAWTE Trusted Site Seal)

Root CA: ÁNO

Obnova certifikátu (reissues): ÁNO

Možnosť zrušenia certifikátu: ÁNO

Podpora IDN domén: ÁNO

Zobrazenie certifikátu

Hneď ako je certifikát na stránky nainštalovaný, zobrazí sa v prehliadači WWW stránok symbol zámku

5.3.2 Postup vystavenia THAWTE SSL Web Server

Vykonanie po objednaní certifikátu je zhodné ako pri THAWTE 123

5.3.3 Overenie certifikátu

Po vykonaní žiadosti SSL Web Server certifikátu bude spoločnosť THAWTE overovať všetky uvedené informácie o spoločnosti alebo objednávateľovi, ktorý bude daný certifikát používať. Všetky informácie sú overované z oficiálnych registrov, zoznamov, internetových stránok a podobne.

Základné overenie trvá cca. 2-3 pracovné dni. Ak nie je možné niektoré dokumenty voľne dohľadať, bude objednávateľ kontaktovaný (osoba pre autorizáciu i technický kontakt) pre doloženie potrebného dokumentu. Ak nebude o certifikát žiadať spoločnosť alebo objednávateľ, ktorý je aj majiteľom domény na ktorej sa certifikát vystavuje, bude THAWTE vyžadovať podpísať dokument "Authorization LETTER" majiteľom domény.

Informácie o vlastníkovi domény je možné si overiť u správcu domén, napr http://www.sk-nic.sk/ pre domény SK. Všetka emailová komunikácia prebieha v anglickom jazyku. Ako náhle prebehne základné overenie, THAWTE vykonáva finálne verbálnej (telefonické) overenie autorizačné osoby. Uvedené telefónne číslo v objednávke musí byť voľne dohľadatelné - zlaté stránky, telefónne zoznamy, webová prezentácia danej spoločnosti, atď. Ak nie je možné dané telefónne číslo overiť, bude THAWTE vyžadovať zaslanie telefónneho účtu, kde bude figurovať daná spoločnosť alebo meno autorizačnej osoby.

Následné verbálne (telefonické) overenie autorizačnej osoby prebieha štandardne v anglickom jazyku a trvá cca. jednu minútu.

Kompletná procedúra overenia SSL Web Server certifikátu trvá cca. 3-5 pracovných dní. Ak nebude možné niektoré dokumenty dohľadať / doložiť, overenie môže trvať aj niekoľko týždňov.

5.3.4 Zaslanie certifikátu

Akonáhle je THAWTE SSL Web Server certifikát overený je počas cca. 30-tich minút vygenerovaný a zaslaný v štandardnom formáte na technický kontakt uvedený v objednávke. Certifikát je možné kedykoľvek preposlať.

5.4 SSL Web Server EV

Umožňuje zobraziť v nových prehliadačoch informáciu, ktorá zreteľne identifikuje organizáciu stojacu za príslušnou webovou stránkou a lištu s URL zobrazuje v zelenej farbe.

Certifikáty EV SSL (EV = extended validation) umožňujú zobraziť v nových prehliadačoch informáciu, ktorá má zreteľne identifikovať organizáciu stojacu za príslušnou webovou stránkou. Napríklad ak pomocou MS prehliadača IE7 vstúpime na stránku zabezpečenú týmto certifikátom, potom lišta s URL bude mať zelenú farbu. Zároveň sa v zelenej farbe takisto zobrazí meno vlastníka certifikátu EV SSL. Dôležitou vlastnosťou nových EV SSL certifikátov sú však podstatne náročnejšie prístupy pri overovaní vlastníka vydávaného certifikátu.

5.4.1 Charakteristika certifikátu

Šifrovanie: Až 256-bit

Kompatibilita prehliadačov: Vysoká, Zelená lišta URL od IE 7 a FF 3.

Zobrazenie v detaile certifikátu: Overené doménové meno a organizácie

THAWTE pečať: ÁNO (THAWTE Trusted Site Seal)

Root CA: ÁNO

Obnova certifikátu (reissues): ÁNO

Možnosť zrušenia certifikátu: ÁNO

Podpora IDN domén: ÁNO

Zobrazenie certifikátu

Hneď ako je certifikát s EV na stránky nainštalovaný, zobrazí sa v prehliadači WWW stránok symbol zámku s názvom danej spoločnosti a celá URL lišta sa zafarbí do zelena.

5.4.2 Postup vydania THAWTE SSL Web Server EV

Po vykonaní objednávky je proces zhodný ako pri predchádzajúcich certifikátoch.

Na kontaktný email uvedený v objednávke dorazí emailová správa o vykonanej žiadosti:

Od: isp_enrollmentprocess@thawte.com

Predmet: THAWTE SSL Web Server EV Certificate Order Confirmation

5.4.3 Overenie certifikátu

Po vykonaní žiadosti SSL Web Server EV certifikátu spoločnosť THAWTE overuje všetky uvedené informácie o spoločnosti alebo objednávateľovi, ktorý bude daný certifikát používať. Všetky informácie sú overované z oficiálnych registrov, zoznamov, internetových stránok a podobne.

Základné overenie trvá cca. jeden týždeň. Ak nie je možné niektoré dokumenty voľne dohľadať, bude objednávateľ kontaktovaný (osoba pre autorizáciu i technický kontakt) pre doloženie potrebného dokumentu. Ak nebude o certifikát žiadať spoločnosť alebo objednávateľ, ktorý je aj majiteľom domény na ktoré sa certifikát vystavuje, bude THAWTE vyžadovať podpísať dokument "Authorization LETTER" majiteľom domény.

Informácie o vlastníkovi domény je možné si overiť u správcu domén, napr http://www.sk-nic.sk/ pre domény SK. Všetka emailová komunikácia prebieha v anglickom jazyku. Okamžite keď prebehne základné overenie, THAWTE vykonáva finálne verbálnej (telefonické) overenie autorizačnej osoby. Uvedené telefónne číslo v objednávke musí byť voľne vysledovania - zlaté stránky, telefónne zoznamy, webová prezentácia danej spoločnosti, atď Ak nie je možné dané telefónne číslo overiť, bude THAWTE vyžadovať zaslať dokument (scan) telefónneho účtu, kde bude figurovať daná spoločnosť alebo meno autorizačnej osoby.

Následné verbálne (telefonické) overenie autorizačný osoby prebieha štandardne v anglickom jazyku a trvá cca. jednu minútu.

Kompletná procedúra overenia SSL Web Server EV certifikátu trvá cca. 10-14 pracovných dní. Ak nebude možné niektoré dokumenty dohľadať / doložiť, overenie môže trvať aj niekoľko týždňov.

5.4.4 Zaslanie certifikátu

Po overení je THAWTE SSL Web Server EV certifikát počas cca. 30-tich minút vygenerovaný a zaslaný v štandardnom formáte na technický kontakt uvedený v objednávke.

5.5 SSL Wildcard

Obsahuje pred názvom domény * (hviezdičku). Nachádza využitie v rámci jednej domény na neobmedzenom množstve domén 3. úrovne.

Tento certifikát obsahuje pred názvom domény * (hviezdičku), napr *. Nazov-domeny.sk. Ide v podstate o SSL Web Server certifikát, ale zabezpečuje všetky domény 3. úrovne v rámci hlavnej domény.

5.5.1 Postup objednania a vystavenie certifikátu THAWTE SSL Wildcard

Charakteristika certifikátu

Šifrovanie: Až 256-bit

Kompatibilita prehliadačov: Vysoká

Zobrazenie v detaile certifikáte: Overené doménové meno a organizácia

THAWTE pečať: ÁNO (THAWTE Trusted Site Seal)

Root CA: ÁNO

Obnova certifikátu (reissues): ÁNO

Možnosť zrušenia certifikátu: ÁNO

Podpora IDN domén: ÁNO

Zobrazenie certifikátu

Akonáhle je certifikát na stránky nainštalovaný, zobrazí sa v prehliadači WWW stránok symbol zámku.

Po vykonaní objednávky je proces zhodný ako pri predchádzajúcich certifikátoch.

Na kontaktný email uvedený v objednávke dorazí emailová správa o vykonanej žiadosti:

Od: isp_enrollmentprocess@thawte.com

Predmet: THAWTE SSL Wildcard Certificate Order Confirmation

5.5.2 Overenie certifikátu

Po vykonaní žiadosti SSL Wildcard certifikátu spoločnosť THAWTE overuje všetky uvedené informácie o spoločnosti alebo objednávateľovi, ktorý bude daný certifikát

používať. Všetky informácie sú overované z oficiálnych registrov, zoznamov, internetových stránok a podobne.

Základné overenie trvá cca. 2-3 pracovné dni. Ak nie je možné niektoré dokumenty voľne dohľadať, bude objednávateľ kontaktovaný (osoba pre autorizáciu i technický kontakt) pre doloženie potrebného dokumentu. Ak nebude o certifikát žiadať spoločnosť alebo objednávateľ, ktorý je aj majiteľom domény na ktoré sa certifikát vystavuje, bude THAWTE vyžadovať podpísať dokument "Authorization LETTER" majiteľom domény.

Informácie o vlastníkovi domény je možné si overiť u správcu domén, napr http://www.sk-nic.sk/ pre domény SK. Všetka emailová komunikácia prebieha v anglickom jazyku.

Hneď po dokončení prebehne základné overenie, THAWTE vykonáva finálne verbálnej (telefonické) overenie autorizačnej osoby. Uvedené telefónne číslo v objednávke musí byť voľne dohľadateľná - zlaté stránky, telefónne zoznamy, webová prezentácia danej spoločnosti, atď. Ak nie je možné dané telefónne číslo overiť, bude THAWTE vyžadovať zaslať dokument (scan) telefónneho účtu, kde bude figurovať daná spoločnosť alebo meno autorizačnej osoby.

Následné verbálne (telefonické) overenie autorizačný osoby prebieha štandardne v anglickom jazyku a trvá cca. jednu minútu.

Kompletná procedúra overenia SSL Wildcard certifikátu trvá cca. 3-5 pracovných dní. Ak nebude možné niektoré dokumenty dohľadať / doložiť, overenie môže trvať aj niekoľko týždňov.

5.5.3 Zaslanie certifikátu

Akonáhle je THAWTE SSL Wildcard certifikát overený je počas cca. 30-tich minút vygenerovaný a zaslaný v štandardnom formáte na technický kontakt uvedený v objednávke.

5.6 THAWTE pečať

Ak je funkčný SSL certifikát THAWTE, môžeme si na svoje stránky umiestniť THAWTE pečať (Trusted Site Seal). THAWTE pečať je dynamický obrázok, zobrazujúci sa na Vašich zabezpečených stránkach. Návštevníci stránok tak hneď vidia, že stránky sú zabezpečené SSL certifikátom spoločnosti THAWTE. Informáciu o platnosti certifikátu je

možné kliknutím na pečať ihneď overiť. Pri vkladaní obrázku si môžete vybrať jeden z troch grafických variantov.

Obrázok 7 Typy pečatí Thawte

Na stránkach THAWTE do formulára zadajte presný názov Vašej domény, pre ktorú bol certifikát vystavený a pokračujte ďalej na presný výber zobrazenia THAWTE pečate na Vašich stránkach.

6 PSCA

PSCA je jednou s prvých CA na Slovensku ktorá poskytuje certifikáty či už ako Akreditovaná alebo Neakreditovaná certifikačná autorita. Akreditáciu certifikačnej autority zabezpečuje zo zákona [9] Národný bezpečnostný úrad

PSCA poskytuje prostredníctvom Akreditovanej Certifikačnej Autority (ACA PSCA) kvalifikované certifikáty, ktoré sú určené výlučne na vytváranie a overovanie zaručeného elektronického podpisu použitím bezpečného zariadenia na vyhotovovanie ZEP a programovej aplikácie pre vyhotovovanie a overovanie ZEP, ktoré boli certifikované Národným bezpečnostným úradom v zmysle ustanovení zákona č. 215/2002 Z. z. o elektronickom podpise .

Certifikačná autorita Prvá Slovenská Certifikačná Autorita (CA PSCA) je neakreditovanou certifikačnou autoritou**.**

Rozdiel medzi týmito dvomi certifikačnými autoritami je hlavne v splnení všetkých bodov zákona č. 215/2002 Z. z. [9] o elektronickom podpise a akreditácii Národným bezpečnostným úradom.

6.1 Akreditovaná Certifikačná Autorita (ACA PSCA)

Akreditovaná Certifikačná Autorita (ACA PSCA**)** poskytuje kvalifikované certifikáty, ktoré sú určené výlučne na vytváranie a overovanie zaručeného elektronického podpisu (ZEP) použitím bezpečného zariadenia na vyhotovovanie ZEP a programovej aplikácie pre vyhotovovanie a overovanie ZEP, ktoré boli certifikované Národným bezpečnostným úradom v zmysle ustanovení zákona č. 215/2002 Z. z. o elektronickom podpise. Zaručený elektronický podpis (ZEP) je jediný elektronický podpis, ktorý je možné v súlade s § 5 zákona č. 215/2002 Z. z. o elektronickom podpise použiť v styku s verejnou mocou. Overovateľ overuje elektronický podpis prostriedkami na overovanie elektronického podpisu využitím podpísaného elektronického dokumentu a verejného kľúča patriaceho udávanému podpisovateľovi. Pri overovaní elektronického podpisu overovateľ môže požadovať overenie pravosti verejného kľúča, to znamená, že verejný kľúč patrí podpisovateľovi. Na tento účel môže použiť certifikát verejného kľúča podpisovateľa. Certifikát verejného kľúča je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný. Bezpečné zariadenie na vyhotovenie elektronického podpisu je prostriedok na vyhotovenie

elektronického podpisu, ktorý spĺňa požiadavky zákona č. 215/2002 Z.z, a ktoré slúži na vyhotovovanie zaručených elektronických podpisov.

V zmysle § 14 ods.2 zákona č. 215/2002 Z. z. o elektronickom podpise akreditovaná certifikačná autorita je povinná mať vypracované bezpečnostné pravidlá a pravidlá na výkon certifikačných činností podľa pravidiel ustanovených všeobecne záväzným právnym predpisom (Vyhláška NBÚ č.541/2002 Z.z.). V zmysle § 14 ods.3 zákona č. 215/2002 Z. z. o elektronickom podpise akreditovaná certifikačná autorita je povinná poskytnúť žiadateľovi o vydanie kvalifikovaného certifikátu informáciu o podmienkach používania certifikátov, o obmedzení ich používania a metódach riešenia sporov a takéto informácie poskytovať aj na požiadanie inej fyzickej osoby alebo právnickej osoby, ktorá preukáže o ne oprávnený záujem. [15]

6.2 Certifikačná Autorita (CA PSCA)

V tejto práci sa zaoberám porovnaním CA Thawte a PSCA. Z vyššie uvedeného je jasné, že ACA ktorá vydáva certifikáty spĺňajúce literu zákona vydáva v zjednodušení len kvalifikovane osobne certifikáty na zaručený elektronicky podpis, preto, napriek tomu že je vlastne v pomeroch slovenská dôveryhodnejšou autoritou ako CA PSCA, nie je pre splnenie zadania našej prace vhodná. Je neporovnateľná s CA Thawte a to hlavne s dôvodu absencie serverových certifikátov, ktoré sú primárnym zameraním CA Thawte.

Zameriame sa teda na CA PSCA ktorá aj napriek tomu že nie je priamo akreditovaná NBU, spĺňa zákonné normy a v neposlednom rade vydáva serverové certifikáty.

6.2.1 Kvalifikovaný certifikát (KC)

Kvalifikovaný certifikát je certifikát fyzickej osoby, certifikát akreditovanej certifikačnej autority, krížový certifikát akreditovanej certifikačnej autority a certifikát úradu, ktorý spĺňa podmienky podľa odsekov 2 až 5 a § 6. (Zákon č. 215/2002 o elektronickom podpise a o zmene a doplnení niektorých zákonov)

Kvalifikovaný certifikát - vydáva PSCA v rámci poskytovania služieb akreditovanej certifikačnej autority v súlade so zákonom č. 215/2002 Z. z. o elektronickom podpise a súvisiacimi vyhláškami NBÚ podľa štandardu X.509 verzia 3.

Platnosť vydaného KC je jeden rok, ak sa zmluvne nedohodne kratšia doba. V zmysle platnej legislatívy subjektom KC môže byť len fyzická osoba.

6.2.2 Elektronický certifikát CA PSCA pre server

Elektronický certifikát CA PSCA pre server je určený pre bezpečnú komunikáciu serverov. Môže byť vydaný pre fyzické alebo právnické osoby na základe riadne vyplnenej žiadosti. Doba platnosti certifikátu pre server je 1 rok.

6.2.3 Certifikačný poriadok PSCA

Je poriadok, ktorý uplatňuje akreditovaná certifikačná autorita Prvá Slovenská Certifikačná Autorita (ďalej len ACA PSCA) pri implementovaní infraštruktúry verejných kľúčov (ďalej len PKI) pozostávajúcej z produktov a služieb, ktoré poskytujú a spravujú kvalifikované certifikáty (ďalej len KC) podľa štandardu X.509 pre kryptografiu verejných kľúčov v súlade so zákonom 215/2002 Z.z o elektronickom podpise.

6.2.4 Procedúra registrácie

Pracovník registračnej autority (RA) overí totožnosť subjektu resp. žiadateľa o kvalifikovaný certifikát (KC), ktorý ho zastupuje, podľa ustanovení Certifikačného poriadku ACA PSCA časť 3.1.7 a 3.1.8. [16]

V prípade úspešného overenia totožnosti pracovník RA vypíše pre každú overenú fyzickú osobu dvojmo formulár "Súhlas so spracovaním osobných údajov", tento sám podpíše a dá ho podpísať žiadateľovi o KC resp. subjektu, ktorý ho zastupuje. Jeden vyplnený formulár zostáva na RA, jeden dostane žiadateľ.

Zákazník priamo na RA pod dohľadom pracovníka RA pomocou definovaného softvéru vygeneruje novú žiadosť o KC priamo v svojom tokene a uloží ju na disk.

Zákazník v súlade s údajmi, ktoré zadal do prehliadača pri generovaní žiadosti o KC, vyplní formulár "Žiadosť o vydanie KC" v dvoch exemplároch, ak tak neurobil ešte pred príchodom na RA. Formulár je k dispozícii na RA.

Pracovník RA preberie od zákazníka súbor so žiadosťou o KC a vyplnený formulár "Žiadosť o vydanie KC".

Pracovník RA skontroluje, či sa údaje na vyplnenom formulári "Žiadosť o vydanie KC" zhodujú s údajmi na žiadosti o KC v súbore a či sú vyplnené všetky povinné položky.

Všetky položky musia byť vyplnené bez diakritiky. Malé a veľké písmená sa rozlišujú.

Položky ST (stateOrProvinceName (názov kraja)), L (localityName ("Mesto")), O (organizationName ("Firma")), OU (organizationUnitName ("Útvar vo firme")) a Email adresa sú nepovinné**.**

Ostatné položky žiadosti o KC musia byť povinne vyplnené nasledovne

Tabuľka 1 Informácie potrebné k žiadosti certifikátu

Názov položky:	Spôsob vyplnenia položky:
C (countryName (Štát))	Dvojznaková skratka štátu (dvojmiestny kód podľa ISO 3166, SK pre Slovenskú republiku) definujúci štátnu príslušnosť subjektu KC
CN (commonName (Meno a priezvisko))	Meno a priezvisko alebo pseudonym subjektu KC, ak bol použitý pseudonym, musí byť za ním uvedený reťazec PSEUDONYM (spolu max. 64 znakov)
G (givenName ("dané mená"))	Všetky mená použité v položke CN okrem priezviska. Údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený
SN (Surname (Priezvisko))	Priezvisko z položky CN. Údaj je povinný, ak v položke CN nebol uvedený pseudonym ale v prípade použitia pseudonymu údaj nesmie byť uvedený

Prostredníctvom informačného systému ACA PSCA sa automatizovane overí, či pre verejný kľúč nachádzajúci sa v predloženej žiadosti o KC už nebol v minulosti vydaný KC. Ak bol, RA žiadosť o KC odmietne prijať z bezpečnostných dôvodov, lebo už raz certifikovaný verejný kľúč nemôže byť použitý v inom KC.

Zákazník a pracovník RA podpíšu dva exempláre zákazníkom vyplneného formulára "Žiadosť o vydanie KC". Jedna kópia zostáva zákazníkovi.

Ak žiadateľ predloží aj iné doklady (okrem osobných dokladov fyzických osôb, napr. výpis z obchodného registra alebo iný doklad o právnickej osobe, plná moc v prípade zastupovania iného subjektu), pracovník RA prevezme a uschová kópie (nemusia byť overené) všetkých predložených dokladov, porovná ich s originálmi a na každú kópiu napíše text "Potvrdzujem zhodu s originálom" a doplní dátum a svoj podpis.

Ak je v položke CN (commonName (Meno a priezvisko)) uvedený aj jeden alebo viacero titulov (napr. Ing., Mgr., CSc. a iné), použitie titulu v žiadosti o KC sa akceptuje, ak sa použité tituly nachádzajú v aspoň jednom z predložených osobných dokladov patriacich subjektu KC. V opačnom prípade je žiadateľ povinný RA preukázať oprávnenosť použitia každého uvedeného titulu predložením originálu alebo úradne overenej kópie diplomu alebo iného dokumentu, ktorý potvrdzuje, že daná osoba má právo používať daný titul.

RA odmietne žiadosť o KC, ktorá obsahuje uvedenie titulu, ktorý žiadateľ nevie dokladovať vyššie uvedeným spôsobom.

Pracovník RA predloží žiadateľovi o KC na podpis Zmluvu o vydaní a používaní KC ACA PSCA v dvoch exemplároch - jeden pre ACA PSCA a jeden pre zákazníka. Súhlas žiadateľa s textom tejto zmluvy je podmienkou na prijatie žiadosti o KC a vytvorenie KC.

Pracovník RA zinkasuje v hotovosti poplatky podľa "Cenníka služieb ACA PSCA" a dá zákazníkovi blok (daňový doklad). Zákazník bude môcť dostať svoj KC až po zaplatení zaň. Zákazník môže platiť aj faktúrou, ak to s ním bolo dohodnuté.

Pracovník RA vloží do aplikácie RA a informačného systému ACA PSCA žiadosť o KC zo súboru a ostatné požadované údaje.

V prípade, že z danej žiadosti o KC z nejakého dôvodu nie je možné urobiť KC, Operátor CA o tom upovedomí príslušnú RA vrátane uvedenia dôvodu, ktorá potom vyrozumie žiadateľa o KC. Žiadateľ o KC môže v takom prípade buď podať novú žiadosť o KC alebo mu budú vrátené zaplatené peniaze. Všetky doklady v tlačenej forme bude RA odosielať na CA stanoveným spôsobom v stanovených periódach.

Vytvorený KC bude uložený v tokene a odovzdaný žiadateľovi, alebo subjektu, ktorý ho zastupuje. Pri preberaní kvalifikovaného certifikátu (KC) žiadateľ podpíše Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát, ktoré tvorí prílohu Zmluvy o vydaní a používaní kvalifikovaného certifikátu PSCA. Toto potvrdenie sa vyhotoví v dvoch exemplároch - jeden pre žiadateľa a jeden pre RA.

Žiadateľ sa pri preberaní svojho KC môže dať zastupovať na RA inou fyzickou alebo právnickou osobou za rovnakých podmienok ako pri podávaní žiadosti o KC. [16]

6.3 Elektronický certifikát CA PSCA

Elektronický certifikát CA PSCA pre server je určený pre bezpečnú komunikáciu serverov. Môže byť vydaný pre fyzické alebo právnické osoby na základe riadne vyplnenej žiadosti. Doba platnosti certifikátu pre server je 1 rok.

Na získanie elektronického certifikátu pre server je potrebné vyplniť písomnú žiadosť o vydanie certifikátu a odovzdať registračnej autorite.

Elektronický certifikát CA PSCA pre server je určený pre bezpečnú komunikáciu serverov. Môže byť vydaný pre fyzické alebo právnické osoby na základe riadne vyplnenej žiadosti. Doba platnosti certifikátu pre server je 1 rok.

Na získanie elektronického certifikátu pre server je potrebné vyplniť písomnú žiadosť o vydanie certifikátu a odovzdať registračnej autorite.

6.3.1 Detailný postup na získanie certifikátu PSCA pre server

Rovnako ako pri osobnom certifikáte je postup ponechaný takmer bezo zmeny podľa návodu na www.psca.sk

Zákazník (žiadateľ o certifikát) vykoná nasledovné kroky ako prípravu na návštevu na RA:

oboznámi sa s týmto postupom, prípadne s princípmi a návodmi pre získanie certifikátu zákazník si pomocou svojho softvéru (typicky napr. Microsoft IIS alebo Apache/Openssl) vygeneruje novú žiadosť o certifikát pre server a skopíruje si ju na 3,5" disketu.

(Upozorňujeme, že žiadosť o certifikát resp. v nej sa nachádzajúci verejný kľúč, pre ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného certifikátu a bude na RA odmietnutá!) Žiadosť musí povinne obsahovať vhodne vyplnenú položku commonName (tzn. názov komponentu). Jednotlivé položky pritom vyplní tak, aby zadané hodnoty boli v súlade s Certifikačným poriadkom PSCA s dôrazom na jeho časť 3.1.2 a aby jednoznačne identifikovali dané zariadenie resp. softvér, ktorý bude používať daný certifikát pre server (typicky napr. uvedením údaja ako je úplné doménové meno, registrovaná IP adresa, výrobné číslo zariadenia, licenčné číslo a pod.). Pri zadávaní hodnôt do položiek žiadosti o certifikát by mal žiadateľ o certifikát mať na zreteli, že na RA bude musieť uspokojivým spôsobom preukázať oprávnenosť všetkých údajov, ktoré zadal do jednotlivých položiek žiadosti o certifikát. Použitie špeciálnych znakov (napr. čiarka, pomlčka, =, / a iné) treba obmedziť na minimálnu nutnú mieru,

odporúčame prípadne tieto znaky použiť až po dohode s PSCA, v opačnom prípade si PSCA vyhradzuje právo odmietnuť takúto žiadosť o certifikát.

Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.). V poli Firma sa nesmie použiť znak čiarka.

Pri príprave návštevy na RA treba mať na pamäti, že ak sa žiadateľ o certifikát mieni dať zastupovať na CMA iným subjektom (fyzickou alebo právnickou osobou), musí tento zastupujúci subjekt odovzdať na CMA vytlačenú žiadosť o certifikát, z ktorej sa má vytvoriť certifikát. Táto vytlačená žiadosť o certifikát musí obsahovať text „Potvrdzujem týmto, že pár kľúčov, zodpovedajúci tejto žiadosti o certifikát je môj" a úradne overený (notárom alebo matrikou) podpis zastupovaného žiadateľa o certifikát.

Zákazník v súlade s údajmi, ktoré zadal do prehliadača pri generovaní žiadosti o certifikát, vyplní formulár "Žiadosť o vydanie certifikátu" v troch exemplároch. Formulár si skopíruje z webu www.psca.sk (je k dispozícii aj na RA).

Zákazník si pripraví zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra (doporučujeme overiť platnosť dokladov) podľa ustanovení časti 3 Certifikačného poriadku PSCA.

Je potrebné, aby si zákazník pripravil kópie (nemusia byt overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré mieni predložiť na RA (napr. výpis z obchodného registra a iné doklady o právnickej osobe, plnomocenstvo, ak sa dá zastupovať na RA), aby ich mohol odovzdať na RA. Výpis z obchodného registra získaný z Internetu nie je postačujúci, nakoľko má len informatívny charakter a nie je použiteľný na právne úkony.

- odporúča sa, aby si zákazník na CMA ešte pred návštevou RA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o certifikát. Je tiež vhodné, aby si zákazník overil svoje poznatky a použitie certifikátov pomocou automaticky vytváraných bezplatných certifikátov PSCA.
- zákazník si dohodne termín návštevy RA (telefonicky, e-mailom) Zákazník v dohodnutom termíne príde na RA, pričom vezme so sebou a predloží:
- 3,5" disketu obsahujúcu žiadosť o certifikát v elektronickej forme

- zvolené doklady totožnosti resp. iné potrebné doklady, napr. výpis z obchodného registra, plná moc atď. podľa ustanovení časti 3 Certifikačného poriadku PSCA. Zákazník odovzdá na RA kópie (nemusia byt overené) všetkých dokladov (okrem osobných dokladov fyzických osôb), ktoré predkladá na RA pri registrácii (napr. výpis z obchodného registra a iné doklady o právnickej osobe, plnomocenstvo v prípade zastupovania iného subjektu).
- vyplnený formulár "Žiadosť o vydanie certifikátu" v troch exemplároch
- príslušnú peňažnú čiastku, ak nebola vopred dohodnutá iná forma platby za certifikát [18]

6.3.2 Postup pri registrácii zákazníka na RA

Pracovník RA overí totožnosť žiadateľa o certifikát resp. subjektu, ktorý ho zastupuje.

V prípade úspešného overenia totožnosti pracovník RA vypíše pre každú overenú fyzickú osobu dvojmo formulár „Vyhlásenie o identite", tento sám podpíše a dá ho podpísať žiadateľovi o certifikát resp. subjektu, ktorý ho zastupuje. Vyplnené formuláre zostávajú na RA.

Pracovník RA preberie od zákazníka disketu so žiadosťou o certifikát vygenerovanú softvérom zákazníka a vyplnený formulár "Žiadosť o vydanie certifikátu".

Žiadosť o certifikát prekopíruje z diskety na disk a vypíše ju na tlačiarni. Disketa je vrátená zákazníkovi. Na výpis sa doplní text „Potvrdzujem týmto, že pár kľúčov, zodpovedajúci tejto žiadosti o certifikát je môj" a dátum, čitateľne meno a priezvisko zákazníka a dá ho podpísať zákazníkovi a uschová ho.

Žiadateľ o certifikát musí žiadosť osobne podpísať pred pracovníkom RA, t.j. nie je prípustné, aby pracovník RA prevzal výpis žiadosti o certifikát, ktorý by prípadne priniesol zákazník so sebou, aby odpadla nutnosť overovať, či sa vypísaná žiadosť zhoduje so žiadosťou na diskete.

Ak je žiadateľ o certifikát zastupovaný na CMA iným subjektom (fyzickou alebo právnickou osobou), musí tento zastupujúci subjekt odovzdať na CMA vytlačenú žiadosť o certifikát, z ktorej sa má vytvoriť certifikát. Táto vytlačená žiadosť o certifikát musí obsahovať text „Potvrdzujem týmto, že pár kľúčov, zodpovedajúci tejto žiadosti o certifikát je môj" a úradne overený (notárom alebo matrikou) podpis zastupovaného žiadateľa o certifikát.

Za akékoľvek prípadné následky nezhody vytlačenej žiadosti so žiadosťou na diskete plne zodpovedá žiadateľ o certifikát a to aj v prípade, že by nezhoda nebola odhalená na RA.

Pracovník RA skontroluje, či sa údaje na "Žiadosti o vydanie certifikátu" zhodujú s údajmi na žiadosti o certifikát na diskete a či sú vyplnené všetky povinné položky.

Všetky položky musia byť vyplnené bez diakritiky. Malé a veľké písmená sa rozlišujú. Položky "Mesto:", "Firma:", "Útvar vo firme:" a „Email:" sú nepovinné.

Žiadosť musí povinne obsahovať vhodne vyplnenú položku commonName (tzn. názov komponentu). Jednotlivé položky pritom musia byť vyplnené tak, aby zadané hodnoty boli v súlade s Certifikačným poriadkom PSCA s dôrazom na jeho časť 3.1.2 a aby jednoznačne identifikovali dané zariadenie resp. softvér, ktorý bude používať daný certifikát pre server (typicky napr. uvedením údaja ako je úplné doménové meno, registrovaná IP adresa, výrobné číslo zariadenia, licenčné číslo a pod.).

Ak bolo použité doménové meno a pracovník RA má vážne podozrenie na neoprávnené použitie danej domény druhej úrovne žiadateľom o certifikát, má právo požadovať, aby žiadateľ dôveryhodným spôsobom dokladoval oprávnenosť použitia danej domény druhej úrovne, v opačnom prípade môže RA odmietnuť prijať danú žiadosť o certifikát.

Ak bola použitá registrovaná IP adresa, RA nepreveruje oprávnenosť jej použitia žiadateľom o certifikát.

Prostredníctvom informačného systému PSCA sa automatizovane overí, či pre verejný kľúč nachádzajúci sa v predloženej žiadosti o certifikát už nebol v minulosti vydaný certifikát. Ak bol, RA žiadosť o certifikát odmietne prijať z bezpečnostných dôvodov, lebo už raz certifikovaný verejný kľúč nemôže byť použitý v inom certifikáte.

Zákazník a pracovník RA podpíšu tri exempláre zákazníkom vyplneného formulára "Žiadosť o vydanie certifikátu". Jedna kópia zostáva zákazníkovi.

Upozornenie:

Údaje uvedené v položkách "Žiadosti o vydanie certifikátu" by sa mali zhodovať s hodnotami uvedenými v elektronickej forme žiadosti na zákazníkovej diskete.

Všetky dôsledky za prípadné chyby a odlišnosti nesie zákazník.

Rozdiely v hodnotách položiek medzi "Žiadosťou o vydanie certifikátu" a žiadosťou na zákazníkovej diskete môžu byť príčinou odmietnutia vydania certifikátu PSCA alebo oneskorenia jeho vydania.

Pri posudzovaní hodnôt všetkých položiek berie pracovník RA do úvahy zmysluplnosť týchto hodnôt - porušenie princípu zmysluplnosti môže byť dôvodom na odmietnutie vydania certifikátu.

Žiadateľ o certifikát musí na RA uspokojivým spôsobom preukázať všetky údaje, ktoré zadal do jednotlivých položiek žiadosti o certifikát.

Ak žiadateľ predloží aj iné doklady (okrem osobných dokladov fyzických osôb, napr. výpis z obchodného registra alebo iný doklad o právnickej osobe, plná moc v prípade zastupovania iného subjektu), pracovník RA prevezme a uschová kópie (nemusia byt overené) všetkých predložených dokladov, porovná ich s originálmi a na každú kópiu napíše text „Potvrdzujem zhodu s originálom" a doplní dátum a svoj podpis. Výpis z obchodného registra získaný z Internetu nie je postačujúci, nakoľko má len informatívny charakter a nie je použiteľný na právne úkony.

Pracovník RA overí, či by vydaním certifikátu nedošlo k duplicite certifikátov resp. či daný subjekt už nemá platný osobný certifikát - dôraz sa pritom kladie na hodnotu uvedenú v položke commonName. Nesplnenie podmienok uvedených vyššie je závažným dôvodom na odmietnutie prijatia žiadosti o certifikát.

Pracovník RA predloží žiadateľovi o certifikát na podpis Zmluvu o vydaní a používaní certifikátu PSCA v troch exemplároch - dva pre PSCA a jeden pre zákazníka.

Súhlas žiadateľa s textom tejto zmluvy je podmienkou na prijatie žiadosti o certifikát a vytvorenie certifikátu.

Pracovník RA zinkasuje v hotovosti poplatky podľa Cenníka služieb PSCA a dá zákazníkovi blok (daňový doklad). Zákazník bude môcť dostať svoj certifikát až po zaplatení zaň. Zákazník môže platiť aj faktúrou, ak to s ním bolo dohodnuté.

Pracovník RA vloží do informačného systému PSCA žiadosť o certifikát z diskety zákazníka (disketu predtým overí na výskyt vírusov) a ostatné požadované údaje vrátane údaja, či zákazník za certifikát zaplatil alebo nezaplatil.

V prípade, že z danej žiadosti o certifikát z nejakého dôvodu nie je možné urobiť certifikát, CA o tom upovedomí príslušnú RA vrátane uvedenia dôvodu, ktorá potom vyrozumie

žiadateľa o certifikát. Žiadateľ o certifikát môže v takom prípade buď podať novú žiadosť o certifikát alebo mu budú vrátené zaplatené peniaze. [18]

6.3.3 Prevzatie certifikátu pre server

Len čo CA vytvorí certifikát, RA vyzve žiadateľa o certifikát prostredníctvom email správy zaslanej na dohodnutú email adresu, aby sa dostavil na RA kvôli prevzatiu svojho certifikátu a podpísaniu potvrdenia o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát, ktoré tvorí prílohu zmluvy o vydaní a používaní certifikátu PSCA. Toto potvrdenie sa vyhotoví v troch exemplároch - jeden pre žiadateľa a dva zostanú na RA.

Žiadateľ o certifikát sa pri preberaní svojho certifikátu môže dať zastupovať na RA inou fyzickou alebo právnickou osobou za rovnakých podmienok ako pri podávaní žiadosti o certifikát.

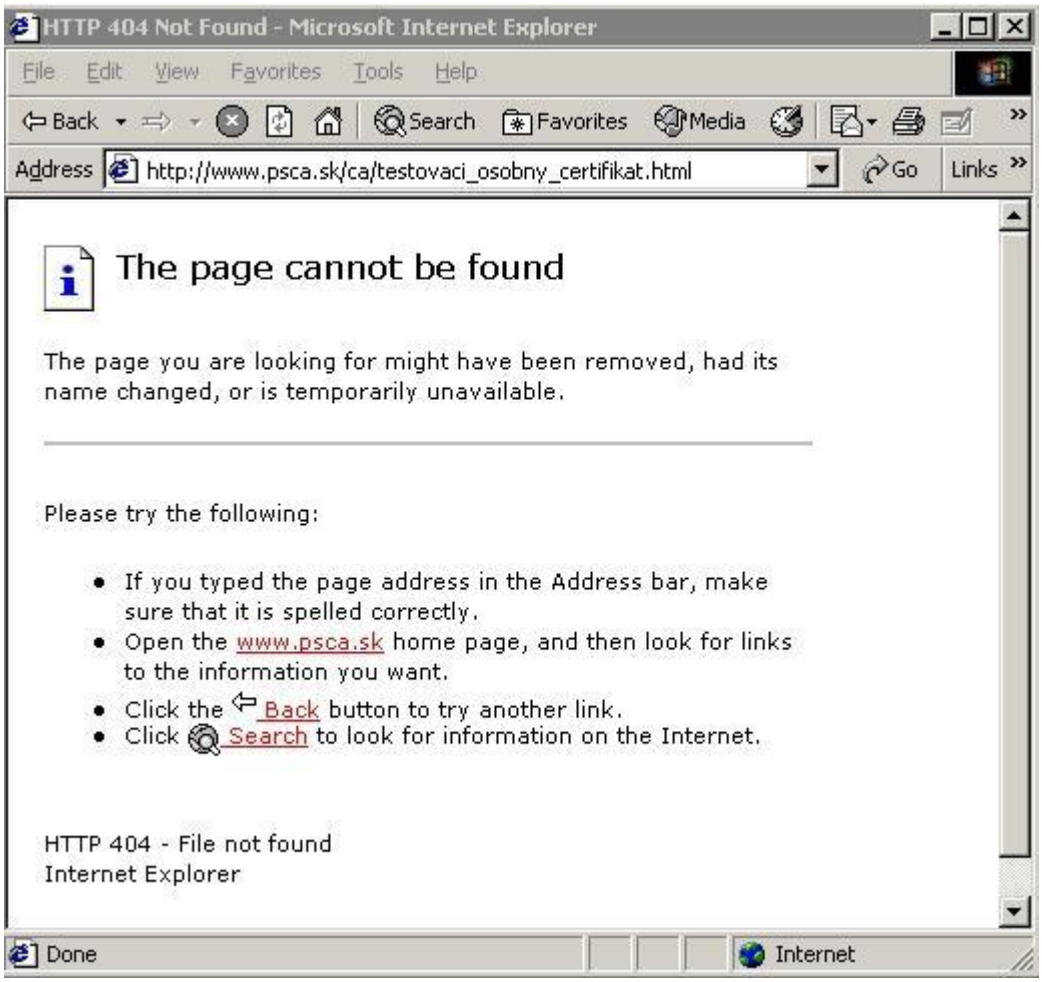
Vytvorený certifikát bude odovzdaný na 3,5" diskete majiteľovi certifikátu alebo subjektu, ktorý ho zastupuje, spolu s certifikátom CA PSCA a certifikačným poriadkom PSCA. [18]

7 INŠTALÁCIA TESTOVACIEHO CERTIFIKÁTU A JEHO POUŽITIE.

Po dohode s vedúcim práce som sa rozhodol ako súčasť práce vysvetliť a popísať inštaláciu testovacieho certifikátu ktorú ponúkajú obe certifikačné autority. Jedná sa o kroky, ktoré vedú k objednaniu, získaniu a inštalácie testovacieho certifikátu na testovacom serveri s OS Win 2000 server a IIS 6.

7.1 Testovací cert. PSCA

Začal som s CA PSCA, ktorá na svojich stránkach ponúka inštaláciu testovacieho osobného certifikátu. Nanešťastie moje snaženie bolo rýchlo ukončené, nakoľko ma na adrese žiadosti o vydanie testovacieho certifikátu čakalo chybové hlásenie o nedostupnosti.



Obrázok 8 Prístup k vytvoreniu testovacieho cert. Na www.psca.sk

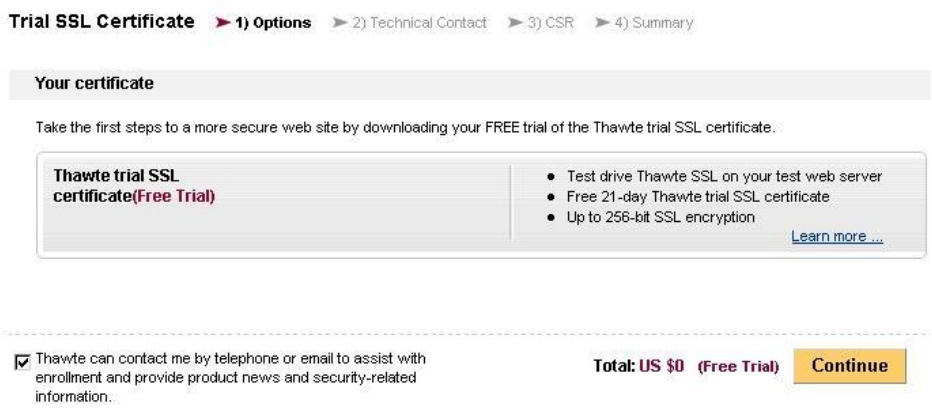
Takže týmto jednoduchým krokom bolo ukončené snaženie sa o vytvorenie testovacieho osobného certifikátu na www.psca.sk

7.2 Testovací cert. THAWTE

Webové rozhranie Thawte.com sa snaží čo najviac uľahčiť registráciu a vytvorenie certifikátu. To platí aj pre zriadenie testovacieho certifikátu, ktorý je inzerovaný hneď na hlavnej stránke.

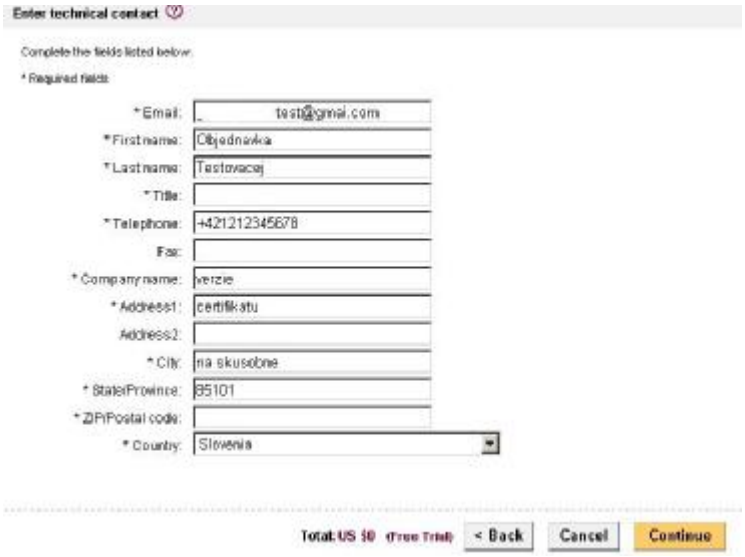
Obrázok 9 Odkaz na www.thawte .com na objednanie testovacieho cert.

Kliknutím na odkaz sa dostávame do rozhrania na objednanie 21 dňovej testovacej verzie SSL certifikátu.



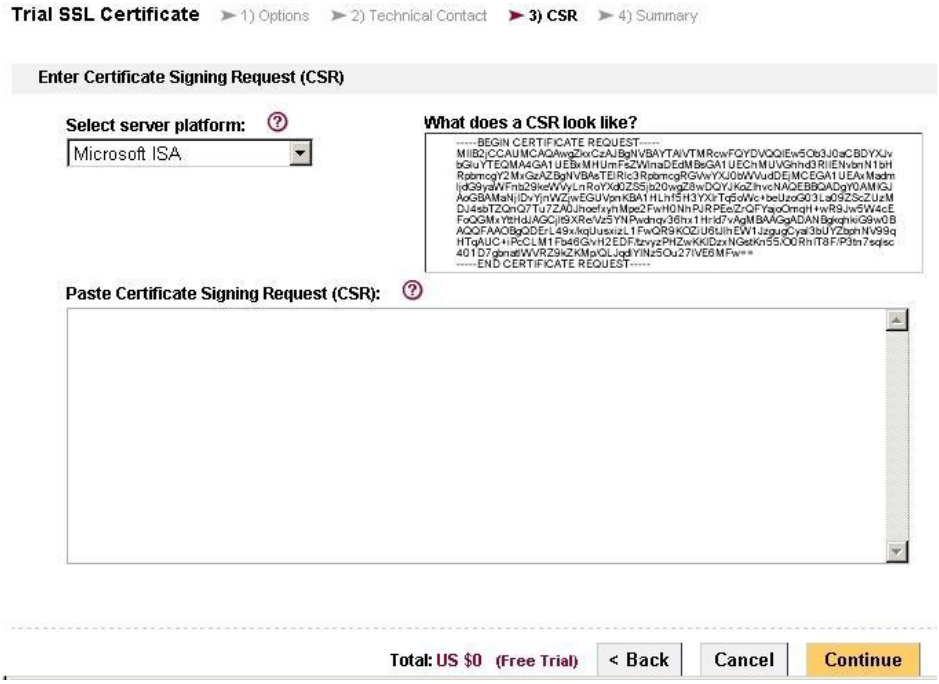
Obrázok 10 Objednávka testovacieho SSL.

Pokračovaním v objednávke sa dostávame do kontaktného formulára ktorý slúži na zadanie kontaktných údajov o vlastníkovi certifikátu.



Obrázok 11 Kontaktný formulár pri objednávke testovacieho SSL

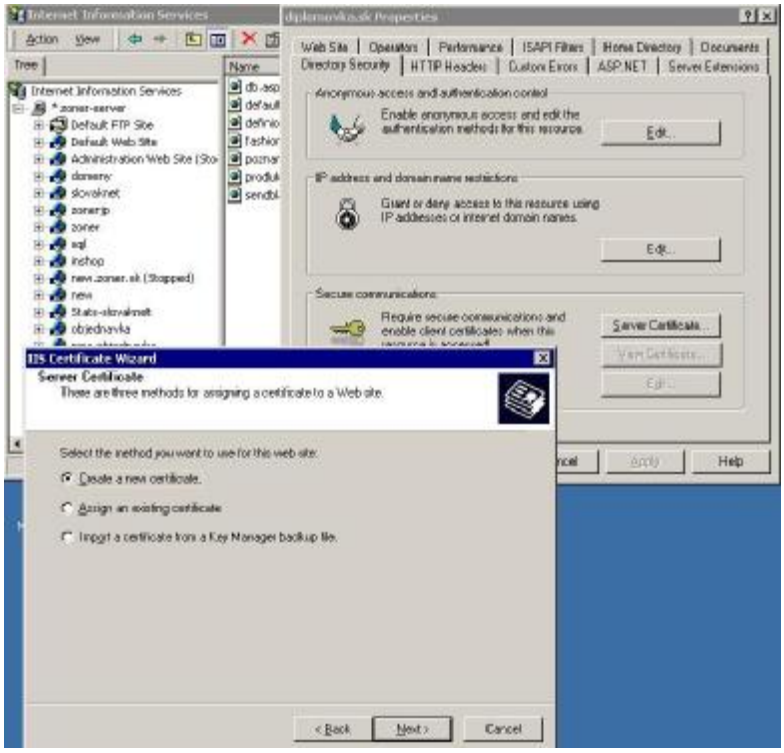
V ďalšom kroku musíme definovať pre akú platformu chceme generovať certifikát, a vložiť TXT request.



Obrázok 12 Definovanie platformy a vloženie requestu

Výhodou celej objednávky je že sa nám v ľavej časti zobrazuje nápoveda a tak v každom kroku vieme ako postupovať ďalej. Na obrázku to síce nie je vidieť, s dôvodu orezu, ale v helpe je odkaz na informácie ako generovať text request ktorý treba do formulára vložiť. Našou úlohou je teda vygenerovať request s IIS6 ktorá beží na mojom testovacom serveri (win2000). Postup je celkom intuitívny. Spustime si IIS konzolu v ktorej sme si vytvorili testovaciu doménu diplomova.sk Kliknutím pravým tlačidlom myši na properties sa nám

zobrazia karty nastavenia danej domény. V časti Directory Security/Secure communication klikneme na server certifikát a pokračujeme Wizardom na vytvorenie nového certifikátu ako je znázornene na obrázku.



Obrázok 13 Generovanie requestu

Po prejdení formulárom a nastavení všetkých náležitostí ako spoločnosť krajina a podobne je certifikát vygenerovaný na adrese c:\certreq.txt. Obsah súboru je nasledovný:

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIDYTCCAsoCAQAwgYUxFjAUBgNVBAMTDWRpcGxvbW92a2Euc2sxFzAVBgN
VBAsTDk5lamFrYSBwb2JvY2thMR0wGwYDVQQKExRUZXN0b3ZhY2kgY2VydGlm
aWthdDETMBEGA1UEBxMKQnJhdGlzbGF2YTERMA8GA1UECBMIU2xvdmF0aWE
xCzAJBgNVBAYTAlNLMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK
w2GDsYldXwnaQJELvYtAQrdMGC04ItegEXBDWtdbMxxbAGV6hDsXfvKtBfDmSH5
LFoXr1bCoyOiJNhDftwcNRe48QVD015xG3S9dPCjIRtmNQZGsoCNUy1Xg/l+kY/cQR
zpJ24Chs5nVU+nfhhmVsjJrI5jx7LJKcJqJaupeIwIDAQABoIIBmTAaBgorBgEEAYI3DQ
IDMQwWCjUuMC4yMTk1LjIwewYKKwYBBAGCNwIBDjFtMGswDgYDVR0PAQH/
BAQDAgTwMEQGCSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GC
CqGSIb3DQMEAgIAgDAHBgUrDgMCBzAKBggqhkiG9w0DBzATBgNVHSUEDDAK
BggrBgEFBQcDATCB/QYKKwYBBAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIA

bwBzAG8AZgB0ACAAUgBTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIAeQ
BwAHQAbwBnAHIAYQBwAGgAaQBjACAAUABvAG8AdgBpAGQAZQByA4GJAC
dS/aqYkJqC+XTZVS5DNj+lBXDGDBNXFDInTxFBxBn8TgdXkxl7vK4YLiXw0nFIsvY
dUjpBzvAp4wkBaGD4W/4kYWgm27tVLDX6CRtYpgj9Oy6/JPIDlu+s7r5/s31OQG0kIy
X/0m18i2TvUw23uGNmpJUaNmnmQVZthl893s42AAAAAAAAAAAwDQYJKoZIhvc
NAQEFBQADgYEAYwcqmi7X7qKL3QgkwVG9fJ30E1U5UpLLJ5D2wpY8mU2SuRBij
+qdlJv1juiS5zzETv+6xDx69QngUUolQR/Muko4z55uFlFYAC4RyygwFeW3TWxgtQ+Jp
W6mX98ka5pq1qdBr67d4cTQIB9lWGn3DYn63daqpltDjrQ1+H/1SFA=

-----END NEW CERTIFICATE REQUEST-----

Tieto informácie vložíme do objednávkového formulára Thawte, odsúhlasíme že súhlasíme s pravidlami vystavenia certifikátu a certifikát je doručený na našu kontaktnú emailovú adresu približne v tomto znení:

Hi Oslovnie,

Thank you for requesting our free trial SSL certificate.

Your order number: SKTESTX3
This certificate is valid for 21 days, and will give you anopportunity to experience the installation process as well asdetermine your required server configuration.

Your Thawte trial SSL certificate:

-----BEGIN CERTIFICATE-----

MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCBF8wggN
HoAMCAQICECZ7VsRL7gQ07OkYONfSVCcwDQYJKoZIhvcNAQEFBQAwga0xCzA
JBgNVBAYTAlVTMRUwEwYDVQQKEwx0aGF3dGUsIEluYy4xKDAmBgNVBAsTH
0NlcnRpZmljYXRpb24gU2VydmljZXMgRGl2aXNpb24xMDAuBgNVBAsTJ0ZvciBUZ
XN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2VzLjErMCkGA1UEAxMidGhhd3
RlIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgUm9vdCBDQTAeFw0xMDA0MTIwMDAwMD
BaFw0xMDA1MDMyMzU5NTlaMIG2MQswCQYDVQQGEwJTSzERMA8GA1UECB
MIU2xvdmF0aWExEzARBgNVBAcUCkJyYXRpc2xhdmExHTAbBgNVBAoUFFRlc3R
vdmFjaSBjZXJ0aWZpa2F0MRcwFQYDVQQLFA5OZWpha2EgcG9ib2NrYTEwMC4G
A1UECxQnRm9yIFRlc3QgUHVycG9zZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMRU
wEwYDVQQDFAxkaXBsb21vdmEuc2swggEiMA0GCSqGSIb3DQEBAQUAA4IBDwA

wggEKAoIBAQC2rg92HZtXyDYT9dvPZwBuy4C+gcDVRXHok8KIDH3Ldk99CSY3fp
epgsLy59r38OyNfKbIt0LSwN0rkOBSOWVMFEbnSsUGU1eM6qfBBY/EOZFkDor06W
JjrK0TRuBz/v+MGe4JWwP8yTV28Hrus6YucTBV9+8BIW7M7PoLqRFsM34Td2ynWh
cUqYysSFTdz4sAR/dA4968owK3IzWceXMpyciN6VMCLrkTqyY/w6Z9rQNq7NdN6M
OC+Srb/50VDFL9nJHZ030ejZkf+hSBx4fSnD9qB47MovsJIxEZm3RN2a0bjnOL0NhS8
DHxv6R3Vu53TlYpZ+cTiD6Cs/VC/M67AgMBAAGjcDBuMAwGA1UdEwEB/wQCM
AAwPwYDVR0fBDgwNjA0oDKgMIYuaHR0cDovL2NybC50aGF3dGUuY29tL3RoYX
d0ZVRyaWFsU1NMUm9vdENBLmNybDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIK
wYBBQUHAwIwDQYJKoZIhvcNAQEFBQADggEBAB8T+wltnXcUUqyl4qXfm1TryM
xfgPvjq+nnAEDvtwGvSCuswjwEuqUTY/uaa0r2Z37JuX3vpXTiE51VQnuPJjqgGduXuB
NnZvCDI97sp2j77mExp9Icq1E5SfNXAWKBpmc9YU6nRBpB7eLImmJonh/69Pf7Z8QD
JFRxHAi3UDrQZi45WPqp9gWiRSufWQc2MwcNRxSHlT+vhTUhtcBsKz49HtQfu6Zuz
q30RE7vXSfS9iPyV28AQuctG72dLKORE65LKbPyZvmEsnjHr/FLAlsQ2LdMIg92pEA
CsHxKOcuO7dP01F5krX4nKgCrMuTMtD8BQWS2ZHWUwCXPiow8NGsAADEAAA
AAAAAA

-----END CERTIFICATE-----

Thawte Test CA Root certificate:

For the trial SSL certificate to provide the same userexperience as a trusted certificate, the Thawte Test CA Rootcertificate must also be installed:

-----BEGIN CERTIFICATE----

MIIEVwYJKoZIhvcNAQcCoIIESDCCBEQCAQExADALBgkqhkiG9w0BBwGgggQsMI
IEKDCCAxCgAwIBAgIQP1MpAnGSsgnuvzehial42DANBgkqhkiG9w0BAQUFADCBr
TELMAkGA1UEBhMCVVMxFTATBgNVBAoTDHRoYXd0ZSwgSW5jLjEoMCYGA1
UECxMfQ2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjEwMC4GA1UECxMnR
m9yIFRlc3QgUHVycG9zZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMSswKQYDVQQ
DEyJ0aGF3dGUgVHJpYWwgU2VjdXJlIFNlcnZlciBSb290IENBMB4XDTA5MTAwOT
AwMDAwMFoXDTI5MTAwODIzNTk1OVowga0xCzAJBgNVBAYTAlVTMRUwEwY
DVQQKEwx0aGF3dGUsIEluYy4xKDAmBgNVBAsTH0NlcnRpZmljYXRpb24gU2Vyd
mljZXMgRGl2aXNpb24xMDAuBgNVBAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuIC

BObyBhc3N1cmFuY2VzLjErMCkGA1UEAxMidGhhd3RlIFRyaWFsIFNlY3VyZSBTZX
J2ZXIgUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA
ML5kYGJjOCgOr6QShUH2ruIqOdSYQJP+P/Rvm94Xkdn9X/ob8AfnLUaXAEByfLEaA
lzVKgt2dqlg6KzMWv1Gui2i9rdWXFdIJcfVruRC76RRup0SBW+KJAnwGTuv69fLtifb+
3fhPcioe5bT/0i6/A4NErip1QmYWlt0G2m+jpNg1/bvNtvZuA1was/cpKUKwIWsx0jWbN
hQjKKvEGuMzGnFImphg+Tu8LYVFevno9Z0+sk9OXugngBDykCPZeOFIvWl7VNasS
RuNUL6W3DqKlUQIiOYtHeLNur18z1sf2rq4iB5pAzySYqxyFNM1o8eoGFLXkt/kdZ74
uW64MzTCsCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf
8EBAMCAQYwHQYDVR0OBBYEFAVCaIYD6cllwSez2ZvUD/d/9QVAMA0GCSqGSI
b3DQEBBQUAA4IBAQC4PptVQCvjjNW1WG+cq8pbv+IwnH7TC11VG3SNKEOp/3DI
AR2yjPGUJy5+oDyeVxU9qWanO4uMNaXMiGPDVsULlZwVOQAF6pqWXeZcL4ErcC
8XzcrPufbKy2nP/8VUb7y7dA9YM6qc25j29J2YTw9FNgQDVOvkCK+8SpTLVImSGY
WE9/+qWXUff6cD9cw5nHPxnCo67ozmk+K8FVK1mvA22IrH0MGEdyXhxNwbxeL/oO
r7koALOv8lDR2IJqLZMwoMMG7dP64PAQwPtTPBJr03ysFL61qDrYVRSXcE8bM2ar5
KVXfIwxZuK5FOf8bMSp1DqKKLyOd9BFgQ0GxeXdXAMQA=
-----END CERTIFICATE-----

Installing your certificate

Installation instructions for a range of web server solutionsare available on our support site here:https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=SO7137

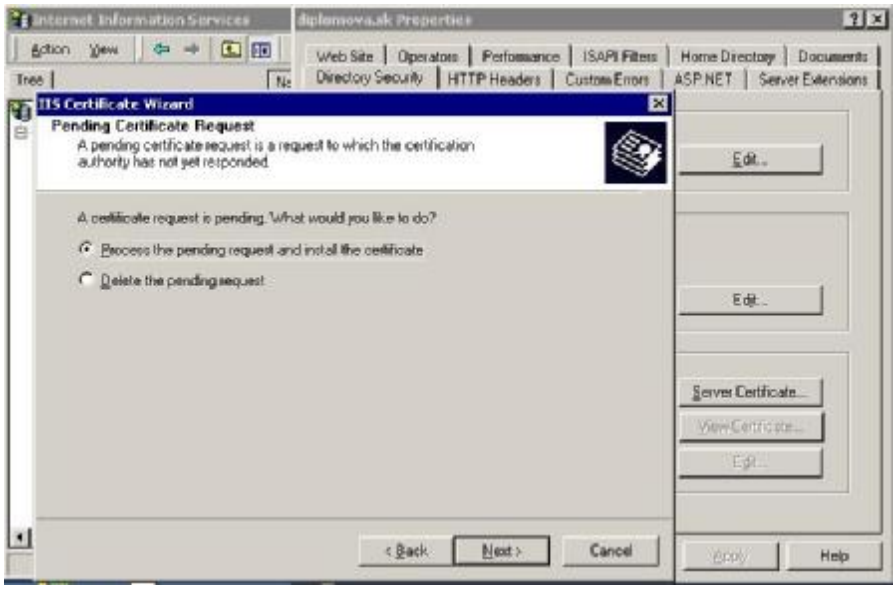
Remember, install your trial certificate on test or developmentservers only. The trial SSL certificate is intended for testingpurposes only.

Your Thawte advisor will be in touch during the nextfew days but if you need any immediate assistance pleasefeel free to contact us by calling, sending an e-mail or making use of our live chat facility below.

Thank you for your interest in thawte!

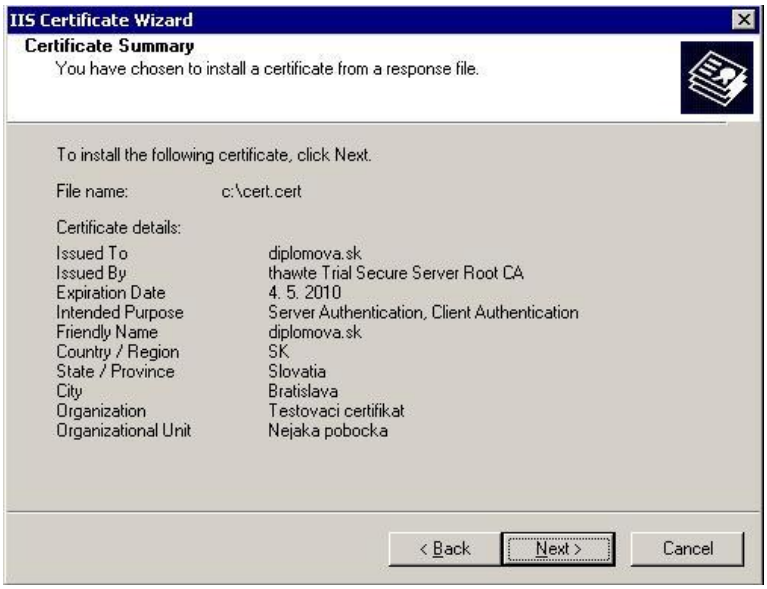
The Thawte Team

Samotná inštalácia certifikátu je jednoduchá. Stačí vytvoriť textový dokument s koncovkou .cert ktorého obsahom je zaslaný certifikát. Následne v IIS v properties domény na záložke Directory Security/Secure communication kliknúť na - server certificate spustí sa wizard na inštaláciu certifikátu.



Obrázok 14 Inštalácia certifikátu na IIS

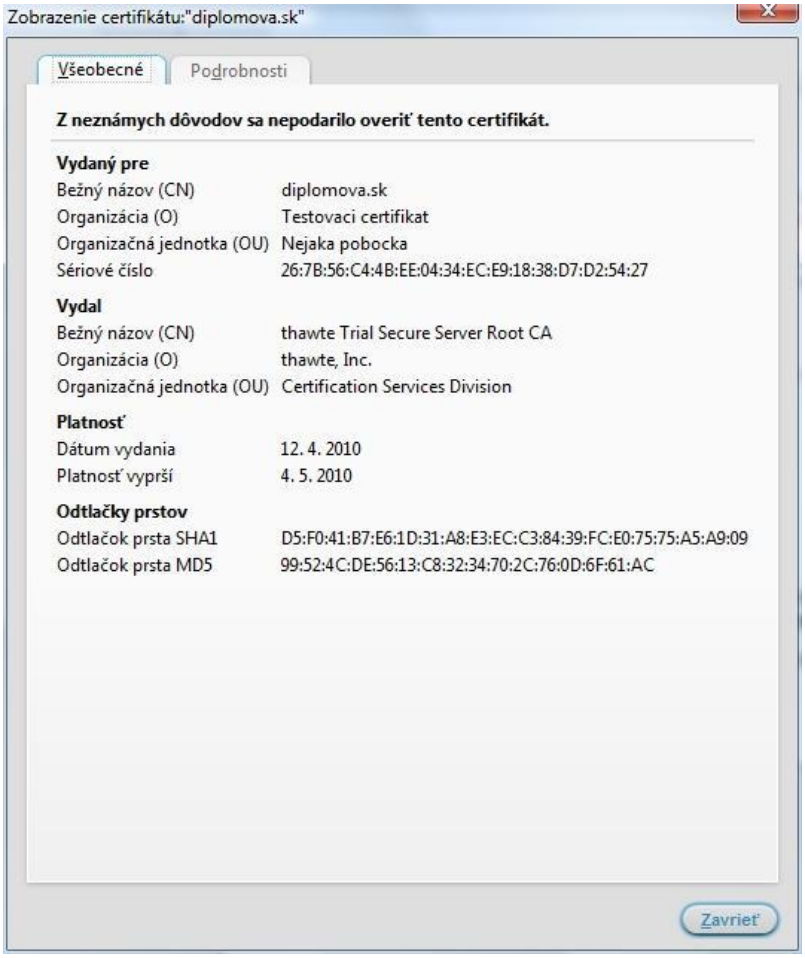
Zvolíme Process the pending and instal the certificate, nalistujeme svoj vytvorený .cert súbor a inštaláciu dokončíme. Zobrazia sa nám informácie o inštalovanom certifikáte.



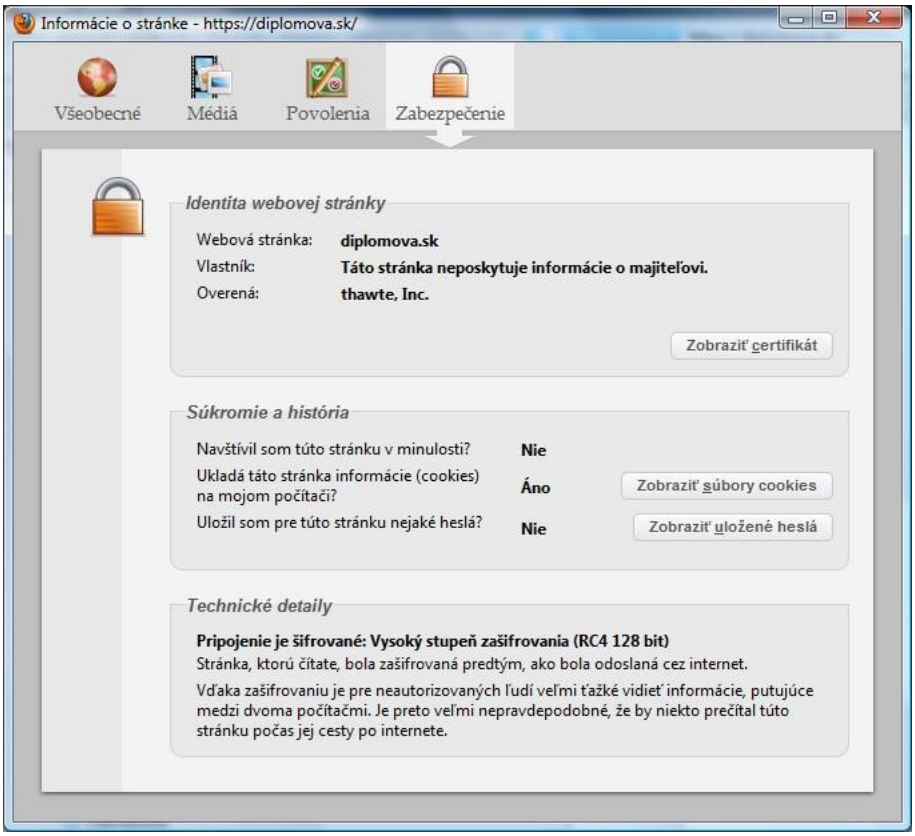
Obrázok 15 Informácie o inštalovanom certifikáte

Certifikát je úspešne nainštalovaný a môžeme ho používať. Chybové hlásenie Z neznámych dôvodov sa nepodarilo overiť tento certifikát je spôsobené tým, že doména diplomova.sk na ktorej sa testovací certifikát testoval nie je registrovaná a server na

ktorom bola inštalácia vytvorená je lokálny server za FW a nie je prístupný na porte 80 a 443.



Obrázok 16 Informácie o inštalovanom certifikáte



Obrázok 17 Informácie o certifikáte

8 POROVNANIE CA

Po popise jednotlivých CA, úspešnom vyskúšaní objednávky a inštalácie testovacieho certifikátu, pristúpime k samotnému porovnaniu jednotlivých certifikačných autorít.

.

8.1 Ponuka certifikátov

Thawte – Ponúka 5 Základných typov certifikatov

Tabuľka 2 Zoznam certifikátov THAWTE

	SSL123 Certificates	**SSL Web Server Certificates**	**SSL Web Server Certificates with EV**	**SGC SuperCerts**	**Wildcard SSL Certificates**
Green Address Bar			Identified by thawte		
Authentication Level	Domain validation ●○○	Full organization validation ●●○	Extended Validation (EV) ●●●	Full organization validation ●●○	Full organization validation ●●○
SSL encryption	128-bit to 256-bit in most browsers	128-bit to 256-bit in most browsers	128-bit to 256-bit in most browsers	128-bit to 256-bit in **99.9% of browsers**	128-bit to 256-bit in most browsers
Estimated issuance time	10 minutes	1-2 days	1-10 days	1-2 days	1-2 days
Thawte® Trusted Site Seal	Secured by thawte 2005-00-00	Secured by thawte 2005-00-00	Secured by thawte 2005-00-00	Secured by thawte 2005-00-00	Secured by thawte 2005-00-00
Recommended use	Secure intranets and internal servers	Secure log-ins for public and employee sites	Visually establish trust and security for all users	Enable strong encryption for the most site users	Secure multiple subdomains
Domains secured	Single	Single	Single	Single	Unlimited subdomains
Certificate Center Account setup	FREE	FREE	FREE	FREE	
Multilingual support	FREE	FREE	FREE	FREE	FREE

Free reissue	✓	✓	✓	✓	✓
Renewal reminders	✓	✓	✓	✓	✓
Over 99% browser compatibility	✓	✓	✓	✓	✓
EV Upgrader™			✓		
Root hierarchy	Thawte	Thawte	Thawte EV	Thawte	Thawte
OCSP and CRL Support	✓	✓	✓	✓	✓
Internationalized Domain Names	✓	✓	✓	✓	✓
Money back guarantee	✓	✓	✓	✓	✓

Zdroj http://www.thawte.com/ssl/index.html

CA PSCA – ponúka 2 typy certifikátov z toho 1 osobný ktorý je ako web server certifikát nepoužiteľný.

8.2 Ergonómia a objednávka

Thawte ponúka vysoký komfort on-line objednania a možnosti. Po vykonaní on-line objednávky a úhrady za certifikát, zaslaní vygenerovaného TXT requestu trvá zriadenie certifikátu len niekoľko dní, v prípade certifikátu 123 len pár minút.

Po vykonaní žiadosti SSL Wildcard certifikátu spoločnosť THAWTE overuje všetky uvedené informácie o spoločnosti alebo objednávateľovi, ktorý bude daný certifikát používať. Všetky informácie sú overované z oficiálnych registrov, zoznamov, internetových stránok a podobne.

Základné overenie trvá cca. 2-3 pracovné dni. Ak nie je možné niektoré dokumenty voľne dohľadať, bude objednávateľ kontaktovaný (osoba pre autorizáciu i technický kontakt) pre doloženie potrebného dokumentu. Ak nebude o certifikát žiadať spoločnosť alebo objednávateľ, ktorý je aj majiteľom domény na ktoré sa certifikát vystavuje, bude THAWTE vyžadovať podpísať dokument "Authorization LETTER" majiteľom domény.

Informácie o vlastníkovi domény je možné si overiť u správcu domén, napr http://www.sk-nic.sk/ pre domény SK. Všetka emailová komunikácia prebieha v anglickom jazyku.

Akonáhle prebehne základné overenie, THAWTE vykonáva finálne verbálnej (telefonické) overenie autorizačnej osoby. Uvedené telefónne číslo v objednávke musí byť voľne vysledovateľné - zlaté stránky, telefónne zoznamy, webová prezentácia danej spoločnosti, atď Ak nie je možné dané telefónne číslo overiť, bude THAWTE vyžadovať zaslať dokument (scan) telefónneho účtu, kde bude figurovať daná spoločnosť alebo meno autorizačnej osoby.

Následné verbálne (telefonické) overenie autorizačný osoby prebieha štandardne v anglickom jazyku a trvá cca. jednu minútu.

Práca s webovým rozhraním je komfortná a bezproblémová.

V prípade PSCA je však situácia odlišná. Webové rozhranie je neprehľadné, serverový certifikát nie je možné vôbec objednať. Je nutná osobná návšteva sídla PSCA. Pri osobnom certifikáte nie je možné generovať TXT request v inom prehiadači ako IE4-6 alebo Firefox. Systém v opačnom prípade končí rôznymi chybovými hláseniami.

Samotný TXT requst je nutne doručiť do PSCA na 3,5 diskete. Privátny kľúč získate až pri osobnej návšteve CA.

8.3 Testovací certifikát

Thawte umožňuje generovať testovací Trial SSL Certificate s 256 bitovym s platnosťou 21 dní pre otestovanie funkčnosti certifikátu. Objednávka vykonaná on-line, obratom je na kontaktný email zaslaný privat key, nainštalovaním ktorého je možné certifikát využívať.

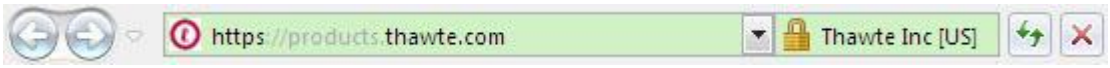
PSCA podľa svojej webovej prezentácie umožňuje objednať testovací osobný certifikát, žiaľ skutočnosť je iná. Prístup na http://www.psca.sk/ca/testovaci_osobny_certifikat.html končí chybou Not Found The requested URL /ca/testovaci_osobny_certifikat.html was not found on this server. Apache/1.3.33 Server at www.psca.sk Port 80

8.4 Validácia certifikátu.

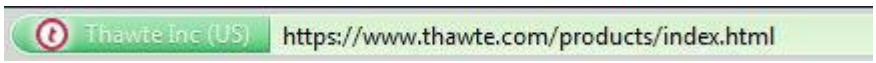
Thawte ponúka niekoľko typov validácie a rozšírenej validácie SSL certifikátu. Certifikát THAWTE, zaručuje že pri prístupe na zabezpečené stránky z rôznych prehliadačov nebudú obťažovaní akýmikoľvek hlásením o "nedôveryhodnosti" certifikátu, ktoré sa zobrazuje prevažne u certifikátov neznámych autorít. CA Thawte je zapísana do tzv. Trusted root

certifikátu. Naviac tradícia a kvalita certifikátov THAWTE je už všeobecne známa a klienti pristupujúci na takto zabezpečené stránky majú väčšiu dôveru k poskytovateľovi stránok. Používatelia nemusia inštalovať žiadne ďalšie certifikáty.

Medzi rozšírenú validáciu zaradíme EV validáciu SSL Webserver EV certifikátu, ktorá sa prejavuje hlave zozelenením adresného riadku v moderných prehliadačoch.



Obrázok 18 Zobrazenie rozšírenej validácie v IE7



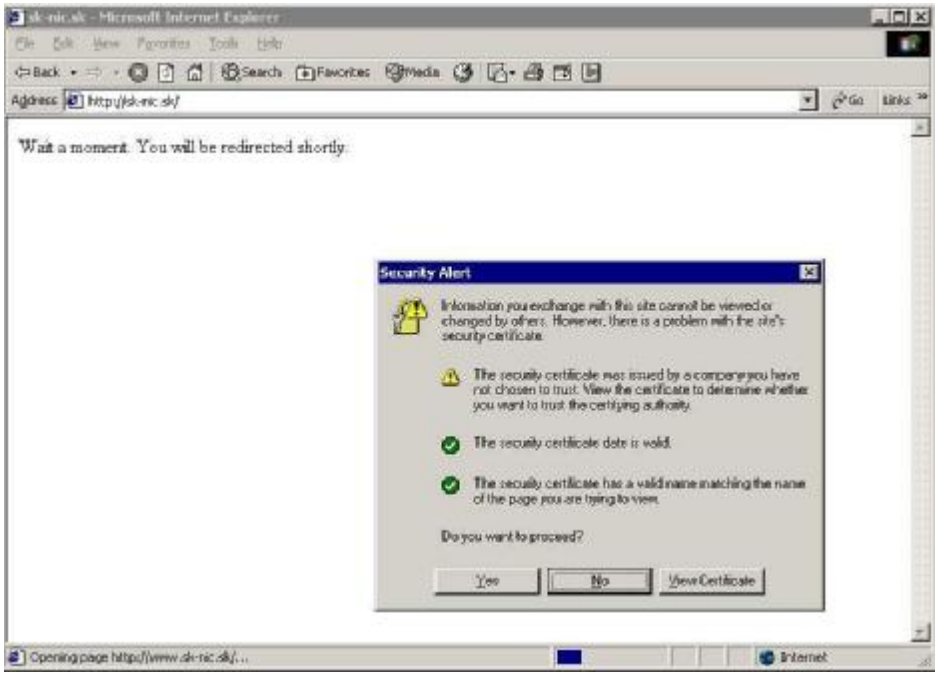
Obrázok 19 Zobrazenie rozšírenej validácie v FF 6.3

Posledným spôsobom rozšírenej validácie je pečať Thawte. Návštevník stránok tak hneď vidia, že stránky sú zabezpečené SSL certifikátom spoločnosti THAWTE. Informáciu o platnosti certifikátu je možné kliknutím na pečať ihneď overiť. Pri vkladaní obrázku si môžete vybrať jeden z troch grafických variantov.

Obrázok 20 Typy pečatí Thawte

Na stránkach THAWTE do formulára sa zadá presný názov domény, pre ktorú bol certifikát vystavený a pokračuje ďalej na presný výber zobrazenia THAWTE pečate na stránkach.

PSCA neumožňuje žiadnu rozšírenú validáciu. Samotná CA PSCA nie je ani Trusted root, takže návštevníci webu s nenainštalovaným certifikátom PSCA sú upozorňovaný na nedôveryhodný certifikát.



Obrázok 21 Chybové hlásenie o nedôveryhodnom certifikáte

Obrázok 22 Informácie o certifikáte na www.sk-nic.sk

Hlásenie o nedôveryhodnom certifikáte je možné odstrániť nainštalovaním rootoveho certifikátu CA PSCA zo stránok http://www.psca.sk/ca/certifikaty_psca.html

8.5 Zhrnutie

Takže ak si zhrnieme informácie a CA PSCA a postup zriadenia certifikátu. Úmyselne som nechával postupy ako citácie priamo z dokumentácie www.psca.sk. Podľa informácii riaditeľa PSCA pána Ing. Krauspeho je celý systém PSCA ktorý je postavený na upravenom OpenSSL 9 [http://www.slproweb.com/products/Win32OpenSSL.html], a správa aj podľa toho. Vo veku internetu a digitálnych médií stále pracuje manuálne. To znamená že procesy zriadenia nie sú automatizované, ale princíp je veľmi jednoduchý, ba povedal by som až prostý.

Prenosy dát na 3,5 disketach, generovanie certifikátu manuálne, nutná osobná návšteva CA, namiesto automatického webového rozhrania.

Ešte väčšie sklamanie zažijeme napríklad pri pokuse o generovanie testovacieho certifikátu na http://www.psca.sk/ca/testovaci_osobny_certifikat.html - stránka neexistuje. Prístup na stránku končí chybou 404. Not Found The requested URL /ca/testovaci_osobny_certifikat.html was not found on this server. Apache/1.3.33 Server at www.psca.sk Port 80

Celá technológia webového rozhrania je prispôsobená dátumu registrácie CA. Takže keď sa rozhodne registrovať si certifikát bežný jedinec zo súčasnosti narazí na neprekonateľný problém. Napríklad nejde generovať žiadosť na vystavenie osobného certifikátu v IE7 a vyššom. Web síce hrdo hlasí že pre Microsoft Internet Explorer verzie 4.0 a vyššej, ale je naozaj použiteľný len do verzie 6, pretože vo vyššej verzii nie je možné vybrať typ kľúča a generovanie končí chybou VBScriptu. Pri prehliadači Chrome síce formulár vypísať ide, systém predpokladá že ide o prehliadač na jadre mozzilla, napriek tomu končí odoslanie formulára CGI error: unrecognized format. Našťastie vo Firefoxe všetko ide bez problémov.

Web server certifikát dokonca ani nie je možné získať priamo na webe, v návode na získanie certifikátu majú jednoduchú vetu: V prípade, že máte záujem o certifikát CA PSCA pre server, kontaktujte niektorú z našich registračných autorít.

Po získaní certifikátu naráža používateľ na ďalší problém. PSCA je síce certifikovaná autorita ktorá je schválená NBU, ale prax ukazuje že sa jedná o spôsob veľmi nepraktický.

A to je neustále obťažovanie návštevníka stránky hlásením o nedôveryhodnom certifikáte. PSCA sa totiž nenachádza v tzv. Trusted Root CA, takže jej root certifikáty nie sú predinštalované v bežných prehliadačoch. To má za následok že bežný návštevník stránky s certifikátom od PSCA získa namiesto pocitu bezpečia a ochrany hlásenie a nedôveryhodnom certifikáte.

Na rozdiel od PSCA Thawte ukazuje ako má vyzerať práca s certifikátmi. Všetko je jednoduché, prehľadné, čokoľvek čo je potrebné si viete naklikať cez web. Stačí vyplniť on-line objednávku, uhradíte platbu a pokiaľ spĺňame všetky podmienky registrácie získame pola typu certifikát do niekoľkých minút či dni, bez nutnosti niekam chodiť, a nosiť tam disketu.

Prečo teda používať CA PSCA aj so všetkými tými chybami. Odpoveď je jednoduchá. Legislatíva na Slovensku. Zákon totiž jasne definuje že na komunikáciu s verejným sektorom je nutné používať len certifikačnú autoritu ktorá je akreditovaná Národným bezpečnostným úradom a to práve PSCA na rozdiel od Thawte je.

V stručnosti sa dá povedať že pokiaľ je nutná komunikácie na oficiálnej úrovni so štátnymi inštitúciami, je nutné siahnuť po Prvej Slovenskej Certifikačnej Autorite. Pokiaľ však treba vystupovať na internete ako dôveryhodný subjekt, je Thawte správna voľba.

ZÁVER

Komplexnosť diplomovej práce spočíva v podaní teoretických základov, ktorým sa venuje teoretická časť, teda technologické aspekty, základný legislatívny rámec a typy elektronických podpisov, tak praktických informácií týkajúcich sa využitia elektronického podpisu v praxi a porovnania certifikačných autorít.

Pri analýze informácií o certifikačných autoritách, ich možnostiach a zameraniu som uviedol a popísal jednotlivé produkty, ako aj spôsob vytvárania a práce s certifikátmi, ako aj podmienky nutné na ich získanie.

V kapitole porovnanie CA som porovnal tieto CA a upozornil na komplikácie pri vytváraní a prace s certifikátom, spomenul výhody a nevýhody ako aj použitie jednotlivých CA, či už s praktického alebo legislatívneho pohľadu.

V práci s dôvodu obsiahlosti témy boli len okrajovo spomenuté informácie o smerovaní legislatívy na Slovensku. Samotná technická a legislatívna implementácia by si zaslúžila samostatnú diplomovú prácu, nakoľko stav na Slovensku je v rámci integrácie do EU s môjho pohľadu nedostatočný.

Hlavný prínoso práce spočíva v podaní uceleného prehľadu o elektronickom podpise a porovnaní certifikačnej autority PSCA a Thawte, ako aj názorné vysvetlenie inštalácie testovacieho certifikátu oboch CA, nakoľko takéto porovnanie neexistuje. Svoje ciele naplnila len čiastočne. Zlé a nefunkčné rozhranie www.psca.sk neumožnilo generovanie testovacieho certifikátu, takže nebolo možné vykonať jeho inštaláciu. Ostatné ciele naplnené boli.

Práca obsahovo aj formálne napĺňa svoje zadanie a dáva čitateľovi informácie o možnostiach certifikačných autorít, ako aj informácie o využití inštalácie certifikátu v prostredí Windows.

Konečné rozhodnutie, ktorú certifikačnú autoritu si vybrať záleží na preferenciách každého jednotlivca. Ja osobne by som odporučil pre komunikáciu, ktorá nezahŕňa komunikáciu so štátnou správou, certifikačnú autoritu Thawte.

ZÁVER V ANGLIČTINE

The complexity of my diploma thesis lies on to give theoretical foundations, discussed in the theoretical part, (as technological aspects, the basic Legislative framework and types of electronic signature) and the practical information (as exploitation of electronic signatures in practice and certification authorities comparison).

In analysis of information's about certification authorities, its options and focus I mentioned and described individual products, as well as a way of creating and working with certificates and the conditions necessary for obtaining it.

In comparison, I compared the CA and highlighted the difficulties in creating works with a certificate, mentioned advantages and disadvantages as well as the usage of a single CA with both practical and legislative terms.

I mentioned the legislation in Slovakia only marginally because of the extensiveness of theory. The technical and legislative implementation itself would merit a separate thesis, as the situation in Slovakia is within integration into EU in my view inadequate.

The main contribution of my thesis lies in administration of comprehensive overview of electronic signature and comparison of the CA and the Thawte PSCA and an illustrative explanation of the installation test certificate of each CA, as such comparison don't exist. Its aims were only partially filled. Poor and broken interface www.psca.sk not allowed to generate a test certificate, so the installation was not possible. Other objectives were met.

Contents and formal part of the work fulfills its assignment and gives readers information about options of the certification authorities as well as information about usage of certificate installation in Windows settings.

A final decision by the certifying authority to choose depends on preferences each individual. I personally would recommend for the communication, which does not communication with government, certification authority Thawte.

ZOZNAM POUŽITEJ LITERATÚRY

[1] BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 2008. 2008 s. ISBN 9788072634651.

[2] LOCKHART, Andrew . Bezpečnost sítí na maximum : Bezpečnost sítí na maximum Andrew Lockhart, 100 tipů a opatření pro okamžité zvýšení bezpečnosti vašeho severu a sítě. 2005. 268 s. ISBN 8025108058.

[3] Information Technology - Security Techniques - Guide for the production

of protection profiles and security targets, ISO/IEC, 2000.

[4] ZAHOREC, Tomáš. Vytváranie a overovanie archívnych elektronických podpisov. www.uniba.sk

[4] DOSEDĚL , Tomáš. Počítačová bezpečnosť a ochrana dat. 2004. 200 s. ISBN 8025101061.

[5] KOLEKTIV AUTOROV. et al. Bezpečnost počítačových sítí : Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. 2005. 592 s. ISBN 8025106977.

[6] POŽÁR, Josef. Informační bezpečnost. 2005. 311 s. ISBN 8086898385.

[7] STANEK, M. Základy kryptológie. www.dcs.fmph.uniba.sk/~stanek/crypto/

[8] Čo prinesie PKI. http://www.mil.sk/index.php?ID=8783&day=2010-08-01

[9] Zákon 215/2002 Zb. o elektronickom podpise a o zmene a doplnení

niektorých zákonov. www.zbierka.sk, 2002.

[10] Vyhláška Národného bezpečnostného úradu č. 538/2002 Zb. o kvalifikovaných

certifikátoch. www.zbierka.sk, 2002.

[11] TnUAD, FSEV. Elektronický podpis. www.tnuni.sk.

[12] Formáty zaručených elektronických podpisov. www.nbusr.sk 2004.

[13] Public Key Infrastructure Study. NIST, The MITRE Corporation, 1994.

[14] www.thawte.com

[15] www.psca.sk

[16] Návod pre získanie certifikátu PSCA, http://www.psca.sk/ca/postup_ziskania.html

[17] Vyhláška Národného bezpečnostného úradu c. 537/2002 Zb. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky. www.zbierka.sk,

[18] www.nbu.sk

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ABA - American Bar Association

AES - Advanced Encryption Standard

BSI - Bundesamt für Sicherheit in der Informationstechnik

CA - Certifikacná autorita

DES - Data Encryption Standard

DSA - Digital Signature Algorithm

DSS - Digital Signature Standard

EESSI - European Electronic Signature Standardisation Initiative

ETSI - European Telecommunications Standards Institute

ESI - Electronic Signatures and Infrastructures

EÚ - Európska únia

FIPS - Federal Information Processing Standards

IEC - International Electrotechnical Commission

IKT - Informačné a komunikačné technológie

ISO - International Organization for Standardisation

KC – Kvalifikovaný certifikát

MD5 - Message Digest 5

NBÚ - Národný bezpečnostný úrad

NIST - National Institute of Standards and Technology

NR SR - Národná rada Slovenskej republiky

OCSP - Online Certificate Status Provider

PAG - PKI Assessmet Guidelines

PKI - Public Key Infrastructure

PKCS - Public Key Cryptography Standards

PUB – Publication

RA – Registračná autorita

RSA - Rivest, Shamir, Adleman

SHA - Secure Hash Algorithm

SHS - Secure Hash Standard

SR - Slovenská republika

TOE - Target of Evaluation

TTP - Trusted Third Party

Zb. - Zbierka zákonov

X.509 - Štandardizovaný formát pre certifikáty

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

CD