Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Důvěryhodnost serverových certifikátů

Jiří Šrámek

© 2021 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jiří Šrámek

Systémové inženýrství a informatika
Informatika

Název práce

Důvěryhodnost serverových certifikátů

Název anglicky

Trustworthiness of server certificates

Cíle práce

Cílem bakalářské práce je vymezit problematiku důvěryhodnosti serverových certifikátů. V praktické části práce je cílem implementace zabezpečení serveru prostřednictvím důvěryhodného certifikátu se zaměřením na ekonomiku provozu takového řešení.

Metodika

Analýza současného stavu serverových certifikátů pro https se zaměřením na problematiku self-signed certifikátů a důvěryhodnosti certifikačních autorit pro koncové uživatele. Autor realizuje porovnání vybraných certifikačních autorit pomocí komparativní metody, zejména pak porovnání jejich důvěryhodnosti. Na základě teoretických poznatků a výsledků praktické části bude formulován závěr bakalářské práce.

Doporučený rozsah práce

40-50

Klíčová slova

Certifikát, zabezpečení, certifikační autorita, server, https, ssl, operační systém

---

Doporučené zdroje informací

DOSTÁLEK, Libor a Marta VOHNOUTOVÁ. Velký průvodce infrastrukturou PKI [online]. 2., aktualiz. vyd. Brno: Computer Press, 2015. ISBN 978-80-251-2619-6.

KOMAR, Brian. Windows Server® 2008 PKI and Certificate Security. Washington: Microsoft Press, 2008. ISBN 9780735625167.

LHOTKA, L. *Server v Internetu.* České Budějovice: Kopp, 1996. ISBN 80-85828-65-0.

PETERKA, J. *Báječný svět elektronického podpisu.* Praha: CZ.NIC, 2011. ISBN 978-80-904248-3-8.

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 29. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 07. 11. 2020

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci " Důvěryhodnost serverových certifikátů " jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 03. 2021 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Tomáši Okounovi za odborné vedení této práce a veškerý věnovaný čas. Dále bych rád poděkoval Ing. Martinovi Havránkovi, Ph.D. za odborné konzultace.

Důvěryhodnost serverových certifikátů

Abstrakt

Tato bakalářská práce se zabývá problematikou digitálních certifikátů, zejména pak těmi serverovými, jejich využitím a důvěryhodností. První kapitola teoretické části popisuje jednotlivé metody šifrování a kryptografie, které jsou základem pro pochopení problematiky certifikátů. Dále jsou podrobně rozebrány digitální certifikáty se zaměřením na jejich důvěryhodnost. V neposlední řadě teoretická část vysvětluje pojem certifikační autorita, následně protokoly SSL/TLS a HTTPS a jejich provázání s certifikáty.

V praktické části jsou vypracovány dvě porovnání. První porovnání se týká nejvyužívanějších českých certifikačních autorit. U druhého jsou porovnány největší světové certifikační autority. Po analýze webových stránek a certifikačních politik zvolených autorit jsou výsledky zapsány do tabulek a následné porovnání je prezentováno pomocí grafu. Na závěr jsou shrnuty výsledky porovnání a je doporučena nejvhodnější volba certifikační autority.

Klíčová slova: certifikát, zabezpečení, certifikační autorita, server, https, ssl, operační systém

Trustworthiness of server certificates

Abstract

This bachelor thesis deals with the issue of digital certificates, especially server certificates, their utilization and trustworthiness. The first chapter of the theoretical part describes the various methods of encryption and cryptography, which are the basis for understanding the issue of certificates. Furthermore, digital certificates are analysed in detail with focus on their trustworthiness. Last but not least, the theoretical part explains the concept of certification authority, followed by SSL/TLS and HTTPS protocols and their connection with certificates.

In the practical part, two comparisons are made. The first comparison includes the most used Czech certification authorities. The second compares the world's largest certification authorities. After analysing the websites and certification policies of the selected authorities, the results are written into tables and the subsequent comparison is presented as a graph. In conclusion, the results of the comparison are summarized, and the most suitable choice of certification authority is recommended.

Keywords: certificate, security, certification authority, server, https, ssl, operating system

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V současné době je zabezpečená komunikace na internetu základ. Internet je sám o sobě opravdu málo bezpečné místo pro přenášená data, ale naštěstí umožňuje samotným uživatelům toto prostředí zabezpečit pomocí aplikací a aplikačních protokolů.

Všechno se pomalu, ale jistě přesouvá do online prostředí, ať už je to bankovnictví, úřady nebo obchody. Krom toho je nespočet webových stránek, kde uživatel musí zadávat své osobní údaje a hesla. V takovémto případě je potřeba zabezpečeného přenosu dat mezi klientem a serverem. Obzvláště s přibývajícím počtem hackerů nebo osob, které se chtějí vydávat za někoho kým ve skutečnosti nejsou a získat či upravit přenášená data v jejich prospěch.

Vezmeme-li si například internetové bankovnictví, mít jistotu, že nikdo nepřijde na náš PIN kód či klientské číslo, je v dnešní době samozřejmost, a to zejména díky šifrované komunikaci. Jako potvrzení toho, že je komunikace se serverem šifrovaná, jsou serverové certifikáty a je zaštiťující certifikační autority. Jedním z nejpodstatnějších kritérií u certifikačních autorit a jimi vydanými certifikáty je jejich důvěryhodnost, která nám dodává jistotu, že se naše citlivé údaje nedostanou do nepovolaných rukou.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem bakalářské práce je vymezit problematiku důvěryhodnosti serverových certifikátů. V praktické části práce je cílem implementace zabezpečení serveru prostřednictvím důvěryhodného certifikátu se zaměřením na ekonomiku provozu takového řešení.

2.2 Metodika

Analýza současného stavu serverových certifikátů pro https se zaměřením na problematiku self-signed certifikátů a důvěryhodnosti certifikačních autorit pro koncové uživatele. Autor realizuje porovnání vybraných certifikačních autorit pomocí komparativní metody, zejména pak porovnání jejich důvěryhodnosti. Na základě teoretických poznatků a výsledků praktické části bude formulován závěr bakalářské práce.

3 Teoretická část

3.1 Základy šifrování a kryptografie

Šifrování je, zjednodušeně řečeno, způsob, jak převést čitelný text zprávy na text jiný, bez dalších informací nečitelný. Tato další informace nutná pro rozluštění (dekódování, dešifrování) původního textu zprávy, se obvykle označuje jako (dešifrovací) klíč. Při kódování zprávy se obvykle používá (šifrovací) klíč, který nemusí být nutně totožný s dešifrovacím klíčem. Tento postup se dá znázornit následujícím schématem:

šifrování: **e (**text, šifrovací klíč**)** = šifra
dešifrování: **d (**šifra, dešifrovací klíč**)** = text

Pointa je samozřejmě v tom, že text na prvním řádku tabulky je totožný s textem na druhém řádku (šifra samozřejmě také); funkce **e** a **d** zde představují kódovací, respektive dekódovací algoritmy. Věda, která se zabývá různými šifrovacími schématy, se nazývá kryptografie a je založena na mnoha hlubokých poznatcích z matematiky a informatiky (23).

Kryptografie primárně vznikla k ochraně zpráv během jejich přenosu, a tak až donedávna byly její doménou přenosové systémy. Praxe však ukázala, že pomocí kryptograficky chráněných zpráv lze velmi efektivně zajistit vysokou úroveň bezpečnosti mnoha dalších systémů, jako například systémů řízení přístupu, systémů elektronických plateb apod. S aplikacemi kryptografie proto přicházíme do styku každodenně, avšak všeobecné povědomí o tom, jak fungují, je nízká. Je to dáno zejména tím, že uvedené aplikace jsou poměrně složité.

Autor zprávy (tzv. původce) svoji zprávu předává vhodným přenosovým systémem (typicky přes počítačovou síť) zamýšlenému příjemci (tzv. adresátovi). Z kryptografického hlediska mají běžně používané přenosové systémy charakter tzv. veřejného přenosového kanálu, což znamená, že ke kanálu mají kromě původce a adresáta přístup i jiné (tzv. neoprávněné) osoby. Některé z těchto osob usilují o čtení, resp. pozměňování přenášených zpráv, a tak je nazveme útočníky. Kryptografické techniky umožňují původci a adresátovi zajistit ochranu přenášených zpráv před uvedenými hrozbami. V případě utajování obsahu zpráv nejsou útočníci schopni zjistit, jaké zprávy jsou v přenosovém kanálu

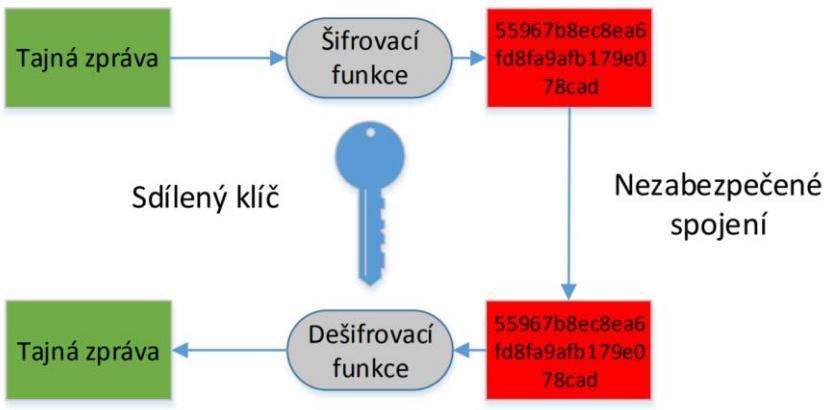
předávány (tzv. důvěrnost zpráv). A v případě prokazování původu zpráv si je adresát schopen ověřit, zda přijatá zpráva skutečně pochází od udávaného původce, tj. zda tato zpráva nebyla během přenosu případným útočníkem nějakým způsobem pozměněna, či dokonce nebyla celá podvržena (tzv. autentičnost zpráv). Zabezpečená komunikace mezi původcem a adresátem je definována kryptografickým protokolem. Základ kryptografického protokolu tvoří datové jednotky, což jsou bloky bitů, které si mezi sebou původce s adresátem vyměňují. Každý typ datové jednotky má svoji určenou strukturu a svůj význam (1).

Rozlišujeme dva typy šifrovacích metod: symetrické a asymetrické.

3.1.1 Symetrické šifrování

Symetrické šifrování používá stejný klíč jak pro šifrování, tak pro dešifrování. Algoritmy spojené se symetrickým šifrováním jsou schopné šifrovat velké množství dat za krátký čas díky použití jednoho klíče a faktu, že algoritmy symetrického šifrování jsou o dost jednodušší v porovnání s algoritmy asymetrického šifrování.

Když jsou data šifrována pomocí symetrického algoritmu, systém generuje náhodný symetrický klíč. Délka klíče, obvykle vyjádřena v počtu bitů, je vymezena algoritmem a aplikací využívající symetrický algoritmus. Jakmile je symetrický klíč vygenerován, je využit k šifrování dat prostého textu do zašifrovaného stavu, označovaného jako šifrovaný text. Šifrovaný text je poté odeslán nebo zpřístupněn příjemci dat. Symetrický klíč musí být bezpečně zaslán příjemci předtím, než příjemce může dešifrovat šifrovaný text. Zaslání symetrického klíče je největší bezpečnostní riziko při používání symetrických šifrovacích algoritmů. Pokud je symetrický klíč zachycen, útočníci mohou dešifrovat všechna data šifrovaná tímto klíčem (10).

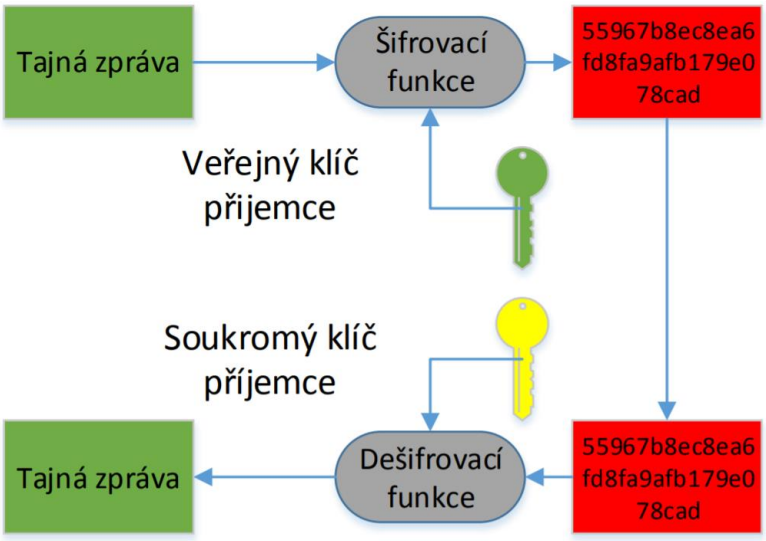


Obrázek 1 - Princip symetrického šifrování

3.1.2 Asymetrické šifrování

Asymetrické šifrování zvyšuje zabezpečení šifrovacího procesu za použití dvou oddělených, ale matematicky souvisejících klíčů známých jako veřejný a soukromý klíč. Šifrovací proces je více zabezpečený, protože soukromý klíč je vlastněn pouze uživatelem nebo počítačem, který generuje dvojici klíčů. Veřejný klíč lze zaslat jakékoli osobě, která si přeje poslat zašifrovaná data držiteli soukromého klíče.

Použití dvou klíčů asymetrického šifrování, jeden klíč pro šifrování a související klíč pro dešifrování a komplexnost asymetrického šifrovacího algoritmu dělá šifrovací proces o dost pomalejší. Studie ukázaly, že symetrické šifrování je při nejmenším stokrát rychlejší než asymetrické šifrování při použití softwarové kryptografie. Když jsou data šifrována pomocí asymetrického šifrování, použitá dvojice klíčů je vlastněna příjemcem dat. Využití této dvojice klíčů zajišťuje, že jen příjemce má přístup k potřebnému soukromému klíči k dešifrování dat, což omezuje šifrování dat na příjemce (10).



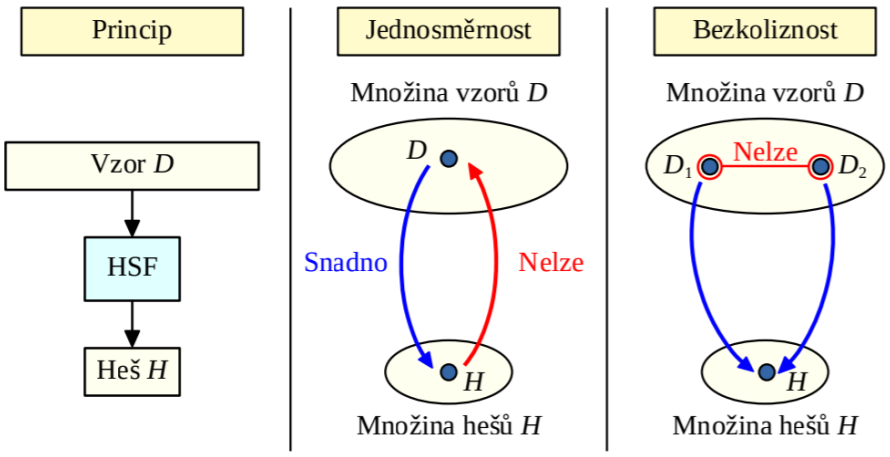
Obrázek 2 - Princip asymetrického šifrování

Pokud jsme dotyčnému předali náš veřejný klíč sami, hezky „z ruky do ruky“, pak není co řešit. Ale mnohem častější je situace, kdy jsme svůj veřejný klíč vyvěsili na nějakém veřejném místě v online světě (na nějaké veřejné nástěnce). Nebo – a to je zcela běžná praxe – jsme svůj veřejný klíč přiložili přímo k podepsanému dokumentu. Jak se potom může příjemce spolehnout na to, že skutečně jde o náš veřejný klíč?

Řešení naštěstí není principiálně složité: stačí najít někoho třetího – nějakou dostatečně důvěryhodnou autoritu – která potvrdí, komu veřejný klíč patří. A aby to nemusela deklarovat pokaždé znovu, vystaví na to jakési opakovaně využitelné potvrzení, které také sama podepíše (opatří vlastním elektronickým podpisem, přesněji: značkou). Tomuto potvrzení se říká certifikát (13).

3.1.3 Hashovací funkce

Hashovací funkce HSF je kryptografická funkce, která číselnému argumentu D (neboli vzoru) o prakticky libovolné délce (jednotky bitů až triliony triliónů bitů) přiřazuje tzv. hash H, což je číselná hodnota o pevně stanovené délce (typicky o délce 256 až 512 bitů). Formálně budeme tuto funkci zapisovat: **H = HSF(D)**.



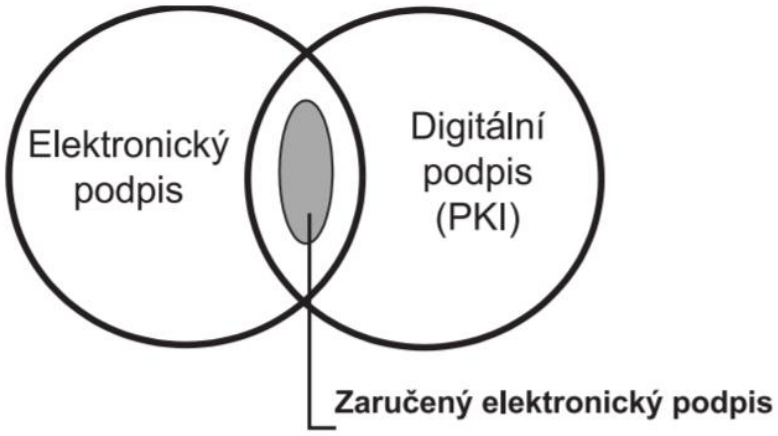
Obrázek 3 - Hashovací funkce a její vlastnosti (1)

Od hashovací funkce se vyžadují dvě specifické vlastnosti, které se nazývají jednosměrnost a bezkoliznost. Jednosměrnost znamená, že určení hodnoty hashe H je pro zadaný vzor D výpočetně snadné, avšak určení hodnoty vzoru D ze znalosti jeho hashe H je prakticky nemožné. Bezkolizností se rozumí, že je prakticky nemožné nalézt nějakou dvojici různých vzorů D1 a D2 takovou, aby jejich hashe byly stejné. V této souvislosti je zapotřebí si uvědomit, že počet číselných posloupností libovolné délky (tj. počet vzorů) je vždy větší, než počet posloupností jediné možné délky (tj. hashů). Z toho pak plyne, že mnoho vzorů musí mít stejný hash (tzv. kolize). Požaduje se však, aby nalezení kolize bylo prakticky nemožné (1).

3.2 Elektronický a digitální podpis

Pod pojmem elektronický podpis budeme chápat veškeré elektronicky vytvořené důkazy o tom, že dokument byl vytvořený konkrétní osobou nebo konkrétním systémem. Jedná se tedy o důkaz autenticity dokumentu.

Digitálním podpisem budeme rozumět podpis vytvořený na základě asymetrické kryptografie. Jelikož digitální podpis může sloužit jako důkaz pravosti dokumentu („nepopíratelnosti“), za jistých podmínek jej můžeme využít jako plnohodnotnou náhradu rukou psaného podpisu. Takový podpis pak označujeme jako zaručený elektronický podpis. Podmínky, za kterých vytváříme zaručený elektronický podpis, jsou dány nejenom kryptografickými parametry a organizačními opatřeními spojenými s bezpečnou generací a správou párů klíčů, ale zejména legislativními podmínkami státu, ve kterém chceme příslušný zaručený podpis uplatnit (5).



Obrázek 4 - Zaručený elektronický podpis (5)

3.3 Certifikáty

Jedná se o nástroj, který potvrzuje, že uživatel nebo serverový systém je ten, za koho se vydává. Vydává ho certifikační autorita. Certifikát je v podstatě veřejný klíč uživatele, podepsaný privátním klíčem certifikační autority. Je určen k identifikaci uživatele nebo systému, autentizaci a několika dalším účelům. U systémů nebo serverů lze použít digitální certifikát např. pro identifikaci firewallů, navazujících společný VPN IPSec tunel. Nebo typicky pro identifikaci webového serveru při navazování https komunikace. Máme několik norem definujících strukturu certifikátu (X.509, EDI, WAP apod.). V internetu se vychází ze standardu X.509 verze 3 (4).

3.3.1 Položky certifikátu

Verze certifikátu souvisí s tím, je-li certifikát odvozen od normy X.509 verze 1, 2 nebo 3. Položka „Version“ má v případě verze 1 hodnotu nula, v případě verze 2 hodnotu jedna a v případě verze 3 hodnotu dva. Dnes se zásadně používají certifikáty verze 3.

Pořadové číslo certifikátu (Serial Number) je definováno jako celé kladné číslo, které musí být jednoznačné v rámci konkrétní certifikační autority. Tj. certifikační autorita nesmí vydat dva certifikáty, které by měly stejné pořadové číslo. Dvojice položek „Serial Number“ + „Issuer“ jednoznačně identifikují certifikát.

Položka **Algoritmus podpisu** (Signature Algorithm) specifikuje algoritmy použité CA pro vytvoření elektronického podpisu certifikátu. Tato položka vždy specifikuje dvojici algoritmů:

- Jeden pro výpočet otisku (hash).
- Druhým algoritmem je asymetrický otisk, kterým je otisk šifrován.

Položka **Platnost** (Validity) určuje platnost certifikátu od (Not Before) do (Not After). Častou otázkou je, proč je omezena doba platnosti certifikátu. Důvody jsou dva:

- Organizační, tj. aplikace má určitou životnost. Bezesporu je i obchodně zajímavé vydávat certifikáty častěji atd.
- Bezpečnostní, což je pádnější důvod. Životnost certifikátu by měla být výrazně kratší než doba nutná k prolomení certifikovaného veřejného klíče. To je ovšem problém zejména u certifikátů certifikačních autorit, které by měly být vydávány na dobu alespoň pětkrát delší, než je životnost uživatelských certifikátů (při kratší době se silně zvyšuje režie obnovování uživatelských certifikátů).

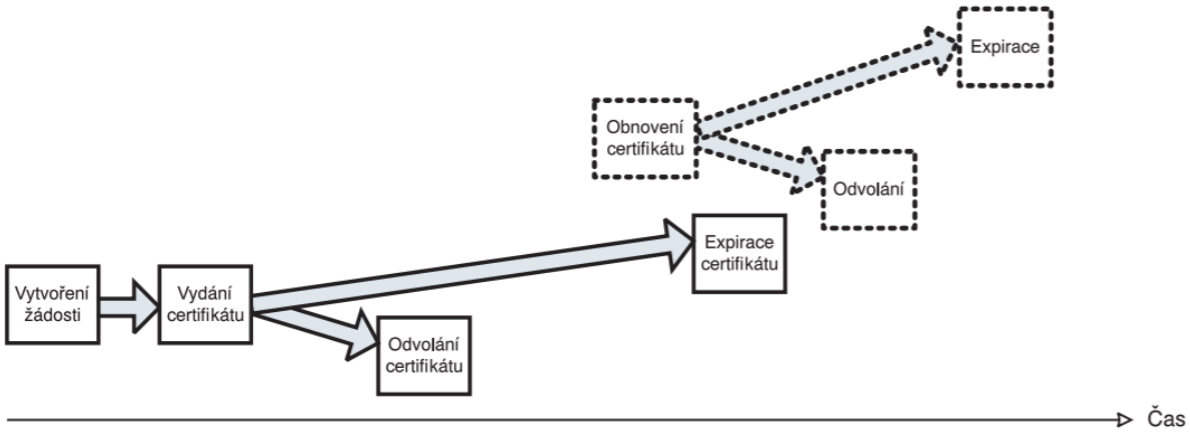
Položka **Vydavatel** (Issuer) obsahuje jedinečné jméno certifikační autority. Je třeba, aby certifikační autorita měla jednoznačnou identifikaci (jedinečné jméno) v rámci všech certifikačních autorit. Útočník bude mít snahu vytvořit certifikační autoritu stejného jména, ale za využití své podvržené dvojice veřejný/soukromý klíč. Zejména pokud naše certifikační autorita používá kořenový certifikát, musíme být na jeho distribuci obzvláště opatrní.

Pokud používáme certifikáty dle X.509 verze 3, musí být **Předmět** certifikátu jedinečný v rámci všech objektů certifikovaných danou certifikační autoritou. Tj. certifikační autorita nesmí vydat dvěma různým osobám certifikát se stejným předmětem. Na druhou stranu je velice praktické, že certifikační autorita může vydávat jedné osobě certifikáty se stále stejným předmětem (5).

3.3.2 Životní cyklus certifikátu

Certifikát v průběhu času prochází několika fázemi, tvořícími životní cyklus certifikátu. Životní cyklus certifikátu se skládá z následujících fází:

1. **Vytvoření žádosti o certifikát** – vytvoření žádosti může, ale i nemusí předcházet generování párových dat (je to sice málo běžné, ale párová data může generovat až certifikační autorita po obdržení žádosti o certifikát).
2. **Vydání certifikátu** a jeho případná publikace.
3. **Platnost certifikátu** – poté co byl certifikát vydán, nemusí být ještě automaticky platný. Platnost certifikátu začíná v době uvedené v položce „od“ a končí buď vypršením platnosti certifikátu nebo odvoláním certifikátu.
4. **Vypršení platnosti certifikátu** (expirace certifikátu) nastane po uplynutí doby „do“ uvedené v certifikátu.
5. **Odvoláním certifikátu** před uplynutím jeho původně deklarované doby platnosti. Certifikát odvolává certifikační autorita zpravidla tím, že identifikaci certifikátu zveřejní na seznamu odvolaných certifikátů (CRL). Odvolaný certifikát se uvádí na všech CRL po dobu jeho původní platnosti (5).



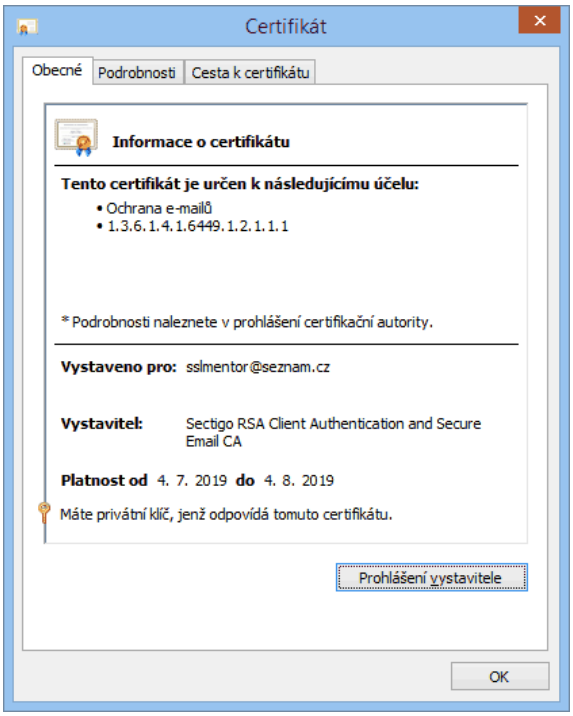
Obrázek 5 - Životní cyklus certifikátu (5)

3.3.3 Typy certifikátů

Tabulka 1 - Klasifikace certifikátů (13)

certifikáty	osobní	kvalifikované (pro podepisování)
		komerční (testovací, emailové, …)
	systémové	kvalifikované (pro označování)
		komerční (testovací, pro šifrování, serverové, …)

Certifikáty mohou být **osobními certifikáty**, tj. takovými, které mohou být vydávány jen fyzickým osobám. Pro vytváření elektronických podpisů přitom připadají v úvahu pouze takovéto osobní certifikáty (ale ne všechny z nich).

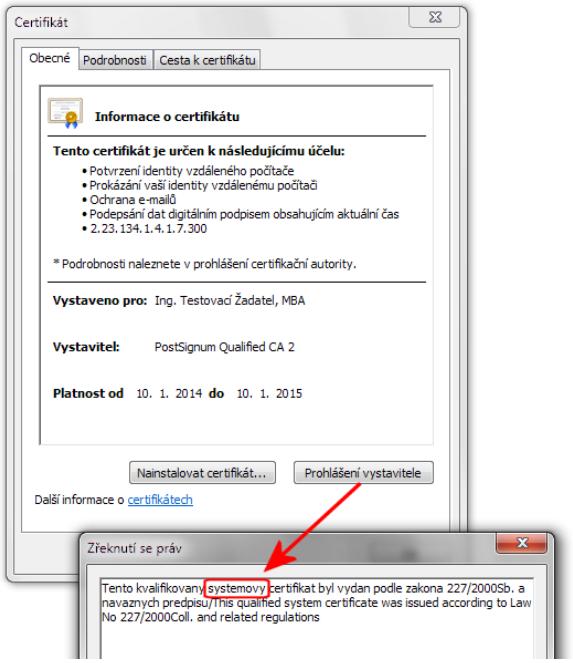


Obrázek 6 - Příklad osobního komerčního certifikátu v prostředí MS Windows (6)

Existují ale i takové certifikáty, které mohou být vydávány jak fyzickým osobám, tak i osobám právnickým (včetně orgánů veřejné moci) či organizačním složkám státu. Jde o tzv. **systémové certifikáty**, které mohou být využívány jak pro vytváření elektronických značek, tak i pro vytváření časových razítek, ale stejně tak i pro další účely, jako je identifikace serverů, šifrování komunikace se servery (například v rámci SSL relací) apod.

Komerční certifikáty a **kvalifikované certifikáty**. Rozdíl mezi nimi je v tom, že požadavky na kvalifikované certifikáty a jejich obsah jsou vymezeny v zákoně, zatímco u komerčních certifikátů zákon jejich obsah nevymezuje. V praxi slouží kvalifikované

certifikáty (ať již osobní či systémové) potřebám podepisování (resp. označování, při tvorbě elektronických značek či vytváření časových razítek) a ověřování podpisů, značek a razítek, zatímco pro všechny ostatní účely – jako je šifrování, přihlašování, prokazování identity a autentizace, zabezpečení apod., by měly být používány certifikáty komerční. Mezi komerční patří i některé poměrně speciální druhy certifikátů, jako například testovací certifikáty, určené na „hraní“ (resp. testování), případně emailové certifikáty, dokládající právě a pouze možnost přístupu k určité emailové adrese, případně ještě další druhy certifikátů (13).

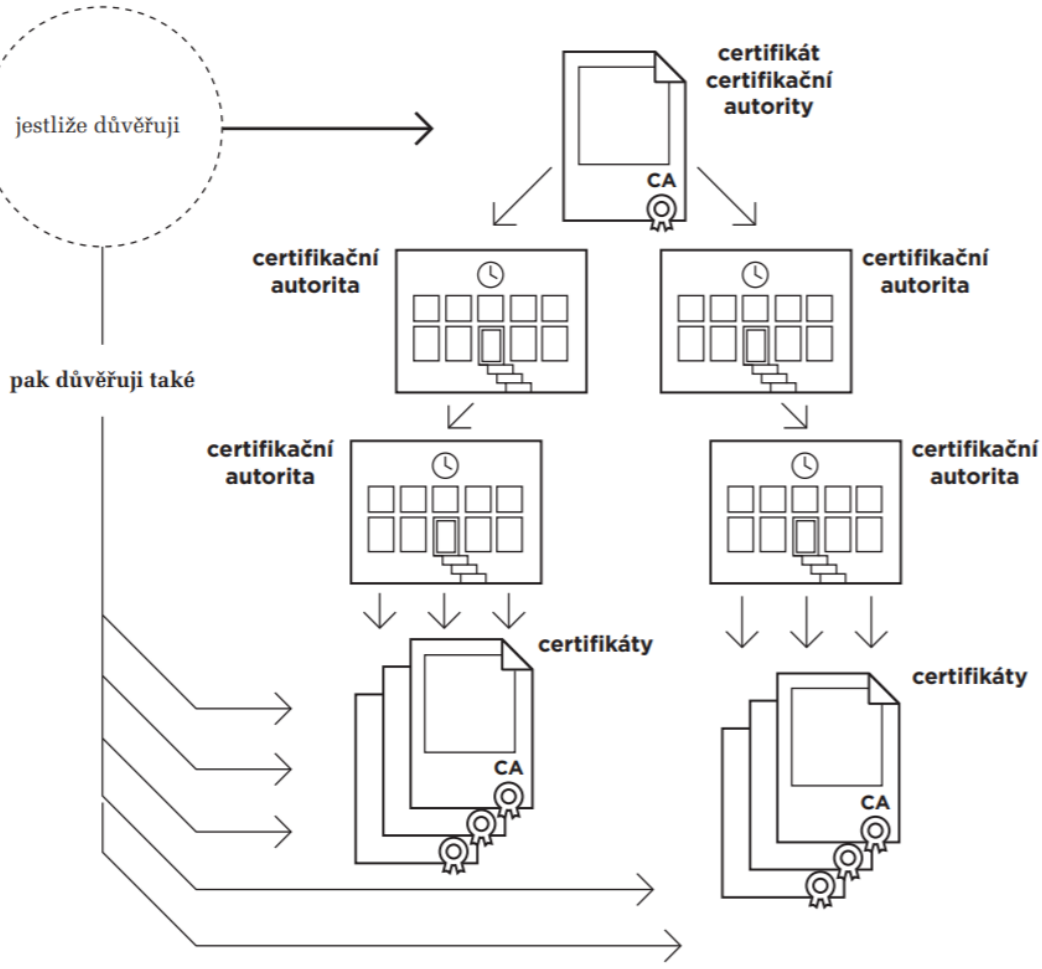


Obrázek 7 - Příklad systémového kvalifikovaného certifikátu v prostředí MS Windows (14)

3.3.4 Důvěryhodnost certifikátů

Snad nejvýznamnějším atributem každého certifikátu je jeho důvěryhodnost. Tedy otázka toho, jak dalece můžeme věřit tomu, co je v certifikátu obsaženo a uvedeno. Důvěryhodnost každého certifikátu samozřejmě můžeme posuzovat individuálně, pro každý jednotlivý certifikát, a to na základě takových informací, jaké máme k dispozici. Třeba pokud nám někdo, koho dobře známe a v koho máme důvěru, sám předá konkrétní certifikát a prohlásí ho za svůj vlastní, asi můžeme tento certifikát zařadit mezi ty, kterým budeme důvěřovat. Pak nám může být celkem jedno, kdo certifikát vydal. Mohl to být třeba sám dotyčný, skrze nějakou vlastní – „na koleně“ provozovanou – certifikační autoritu. V praxi bychom ale touto cestou daleko nedošli. Těžko bychom se totiž dokázali osobně (a dopředu) setkat se všemi osobami, se kterými budeme chtít nějak elektronicky komunikovat, či od nich jen přijímat elektronicky podepsané dokumenty. Navíc by nám to nejspíš nebylo k ničemu, protože bychom tyto osoby tak jako tak nejspíše neznali, a tak bychom ani nemohli důvěřovat těm certifikátům, které by nám předali.

Potřebovali bychom nějakého důvěryhodného prostředníka, který by nám certifikáty různých osob předával a sám se zaručil za autenticitu (pravost) těchto certifikátů. A tím i za identitu osob, kterým byly certifikáty vydány. Takovýmto prostředníkem by měla být sama certifikační autorita, která certifikát vydala. U certifikátů a certifikačních autorit navíc platí něco, co bychom mohli označit jako „delegaci důvěry“: když budu důvěřovat nějaké konkrétní certifikační autoritě, mohu důvěřovat i všem certifikátům, které tato certifikační autorita vydala (13).



Obrázek 8 - Znázornění stromu důvěry (13)

Vše se tedy dá zobecnit, do celého stromu důvěry: v jeho kořeni je jeden certifikát (tzv. kořenový certifikát), který odpovídá jedné (typicky: kořenové) certifikační autoritě. Od něj se odvíjí důvěra v další certifikáty (všechny vnitřní uzly stromu, tj. „podřízené“ certifikační autority, resp. jejich certifikáty) i všechny koncové uzly (certifikáty koncových uživatelů). Pokud pak někdo vyjádří svou důvěru příslušnému kořenovému certifikátu, fakticky tím vyjadřuje svou důvěru rovnou celému stromu. Vše přitom sleduje jeden hlavní

cíl, kterým je zjednodušit vyjadřování důvěry: uživatelé dostávají jeden „pevný bod“, v podobě kořenového certifikátu – a skrze něj mohou „fixovat“ svou důvěru v celý strom certifikátů (vyjádřením důvěry kořeni stromu, viz výše).

Vyjadřování důvěry certifikátům je nesmírně důležitým (ba přímo kardinálním) aspektem elektronického podpisu. To proto, že právě od důvěryhodnosti konkrétních certifikátů se odvozuje důvěra a platnost konkrétních elektronických podpisů, značek či razítek. Je to ostatně logické: máme-li se spoléhat na nějaký podpis (či značku nebo razítko), potřebujeme spolehlivě vědět, čí podpis (či značka, razítko) to je. A to nám spolehlivě řekne pouze dostatečně důvěryhodný certifikát.

V souvislosti s certifikáty si ale musíme uvědomit, že při vyjadřování důvěry neplatí jednoduchá dichotomie: že certifikát je buďto důvěryhodný, nebo naopak nedůvěryhodný. Místo toho musíme pracovat se třemi možnostmi:

- certifikát je důvěryhodný
- certifikát je nedůvěryhodný
- nemáme dostatek informací k hodnocení důvěryhodnosti certifikátu.

Pro první dvě možnosti musíme vždy mít nějaký konkrétní důvod. Aby mohl být nějaký certifikát považován za důvěryhodný, musí být buďto prohlášen za důvěryhodný přímo tento certifikát, nebo musí „patřit“ do některého stromu důvěry, jehož kořen (kořenový certifikát) byl prohlášen za důvěryhodný. Podobně pro nedůvěryhodnost: i zde buďto musí být prohlášen za nedůvěryhodný přímo daný certifikát, nebo musí „patřit“ do některého stromu (ne)důvěry, jehož kořen byl prohlášen za nedůvěryhodný. Pokud nenastane ani jedna z těchto dvou možností, zbývá ještě ona třetí možnost: že nemáme dostatek informací k tomu, abychom dokázali zhodnotit důvěryhodnost daného certifikátu. V praxi bývá tato třetí možnost poměrně častá (13).

3.4 Serverové certifikáty

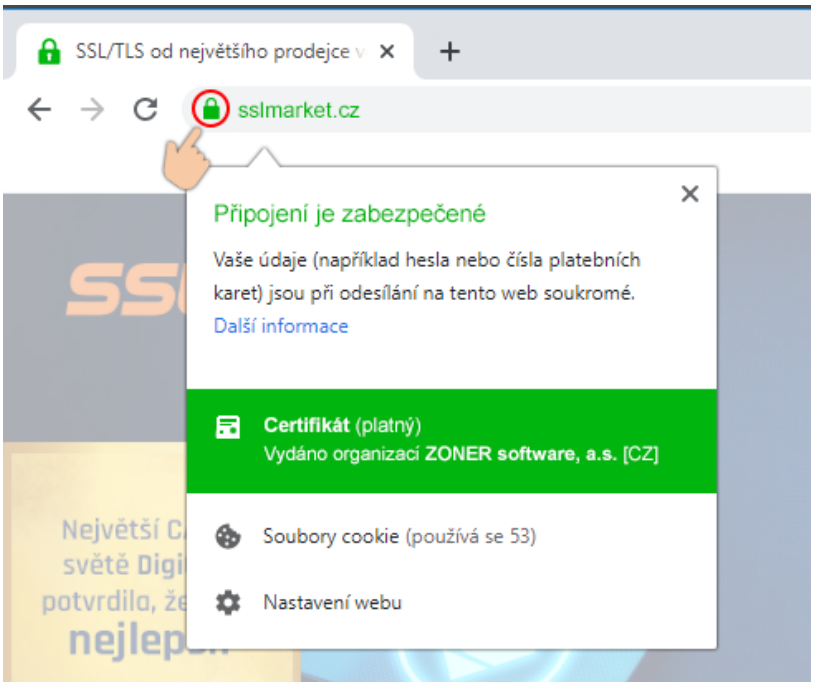
Serverové certifikáty prokazují identitu stránek. Typickým příkladem takových stránek je třeba internetové bankovnictví. Certifikát pak představuje opatření, které uživateli dokazuje, že stránky šifrující svou komunikaci jsou skutečně ty, za které se vydávají. Šifrování je tedy garancí soukromí, certifikát dává jistotu, že v soukromí neodevzdáváte důležité informace podvodníkovi.

Abychom mohli mluvit o tom, že stránky mají certifikát, je potřeba, aby jejich majitel opatřil veřejnou část klíče elektronickým podpisem – souborem dat, který upřesňuje identitu vlastníka klíče. Právě toto „podepsání“ veřejné části klíče lze označit za samotný proces certifikace. Pokud se majitel rozhodne podstoupit o něco náročnější způsob ověření, získaný certifikát pak neslouží pouze jako nástroj ověření, ale přímo k jednoznačné identifikaci vlastníka stránek. Z uživatelského hlediska je ale podstatné, že je navštívená stránka zašifrována, což se mimo jiné projeví i tím, že v adresním řádku prohlížeče se objeví „https“ a pak až název stránky (a před adresou v některých prohlížečích také ikonka zámku). Dále je klíčové, aby certifikát použitý pro ověření daných stránek byl platný. Pokud není, uživatel to pozná podle oznámení prohlížeče ve smyslu „nelze ověřit certifikát“. V takovém případě je na místě opatrnost, zvlášť pokud stránky vyžadují odeslání citlivých informací (18).

SSL certifikát je nástroj, díky kterému můžete SSL šifrování plnohodnotně využívat. Známe různé SSL certifikáty. Některé jsou zdarma, jiné jsou placené – záleží na tom, co všechno od certifikátu očekáváte. Nejpodstatnější důvody, proč si SSL certifikát zajistit a implementovat, jsou tyto:

- Vyšší důvěryhodnost webové stránky. Pokud u vaší URL adresy svítí nápis „nezabezpečeno“, tak můžete počítat s tím, že bude méně důvěryhodná. Ne každý tento detail vnímá, ale je už relativně dost uživatelů, kteří rozdíl poznají a k webové stránce s HTTP nemají důvěru.
- Získáte lepší pozice ve vyhledávání. Značný pozitivní vliv na vyhledávání můžete očekávat pouze do doby, dokud vaše konkurence SSL certifikát nevyužívá. V případě, že budete mít všichni SSL certifikát, tento parametr už nebude konkurenční výhodou ve vyhledávání.
- Neriskujete, že z vašeho webu uniknou důležité uživatelovy údaje.

Většina hostingových providerů poskytuje přímo nákup SSL certifikátu a tím se celá implementace ještě víc zjednodušuje. Máte možnost si koupit placené certifikáty, jako jsou například Rapid SSL, Thawte, Geotrust a mnohé jiné. Dále máte možnost sáhnout po certifikátu, který je zdarma. Nazývá se Let's Encrypt. Většina hostingových providerů tento certifikát poskytuje přímo v administraci hostingu (20).



Obrázek 9 - Příklad platného serverového certifikátu (17)

3.4.1 Druhy serverových certifikátů

SSL certifikát pro jednu doménu, tedy certifikáty pro konkrétní internetovou doménu. Tyto certifikáty zabezpečují firemní, osobní či stránky jakéhokoliv projektu. Všechny SSL certifikáty pro jednu doménu vystavují certifikační autority pro současné použití na adresách s www i bez uvádění www. Takto se vystavují certifikáty již několik let a vystavený SSL certifikát se jednoduše nastaví na serveru a vše funguje (22).

Multi-doménové SSL certifikáty řeší potřebu zabezpečit více různých domén jedním SSL certifikátem pomocí technologie SAN/UCC (Subject Alternative Name/Unified Communications certificate). Tyto certifikáty umožňují zabezpečit primární název domény a až 249 dalších domén současně. Přitom každá doména může být od jiné domény nejvyššího

řádu (.cz, .sk, .com, .eu atd.), čímž se odlišují od WildCard SSL certifikátů pro zabezpečení neomezeně subdomén. Jednou z dalších výhod multi-doménových SAN certifikátů je fakt, že lze domény přidávat do certifikátu během jeho platnosti (12).

WildCard SSL certifikáty - tzv. hvězdičkové SSL certifikáty umožňují zabezpečení všech subdomén pod svojí hlavní doménou. S certifikátem WildCard SSL není nutné objednávat další samostatné SSL certifikáty, když vytváříte více subdomén. WildCard SSL certifikát výrazně šetří náklady na pořízení a správu zabezpečení domén na serveru (25). Možnost zabezpečení neomezeného počtu sub-domén je zajištěno umístěním hvězdičky (*) do certifikátu před název domény. Hvězdička funguje v certifikátu jako „divoká karta – Wild Card“ a prohlížeče tak akceptují místo hvězdičky jakékoliv platné znaky před doménou. Pokud potřebujeme zabezpečit více subdomén, počáteční náklady za WildCard SSL certifikát jsou vyšší než nákup samostatných SSL certifikátů, ale při určitém počtu se náklady vyrovnají a přičteme-li k tomu i snadnější správu, vyplatí se získat WildCard SSL již od potřeby zabezpečení několika subdomén. Jeden WildCard SSL certifikát vystavený pro primární doménu (*.domenaxyz.cz), může zabezpečit neomezený počet subdomén, jako například:

- www.domenaxyz.cz
- admin.domenaxyz.cz
- mail.domenaxyz.cz
- cokoliv.domenaxyz.cz
- atd. (3).

3.5 Self-signed certifikáty

Self-signed certifikát je digitální certifikát, který není podepsán veřejně důvěryhodnou certifikační autoritou. Důvodem, proč se považují za odlišné od tradičních certifikátů podepsaných certifikační autoritou, je to, že jsou vytvářeny, vydávány a podepsány společností nebo vývojářem, který odpovídá za podepsaný web nebo software. Z tohoto důvodu jsou certifikáty podepsané svým držitelem považovány za nebezpečné pro veřejné weby a aplikace.

Výhody self-signed certifikátů:

- self-signed certifikáty jsou zdarma.
- Jsou vhodné pro interní (intranetové) weby nebo testovací prostředí.
- Šifrují příchozí a odchozí data stejnými šiframi jako jakýkoli jiný placený certifikát SSL.

Nevýhody self-signed certifikátů:

- žádné prohlížeče a operační systémy nedůvěřují self-signed certifikátům.
- Prohlížeče nebudou před názvem domény zobrazovat vizuální indikátory důvěryhodnosti, jako je symbol visacího zámku a HTTPS.
- Návštěvníci webových stránek musí pro přístup k obsahu postupovat prostřednictvím stránky s varováním zabezpečení s chybovými zprávami, jako je „error_self_signed_cert“ nebo „sec_error_untrusted_issuer“ nebo „err_cert_authority_invalid“. To znamená, že uživatelé musí ručně kliknout na tlačítko „Přijmout riziko“, aby otevřeli web (24).

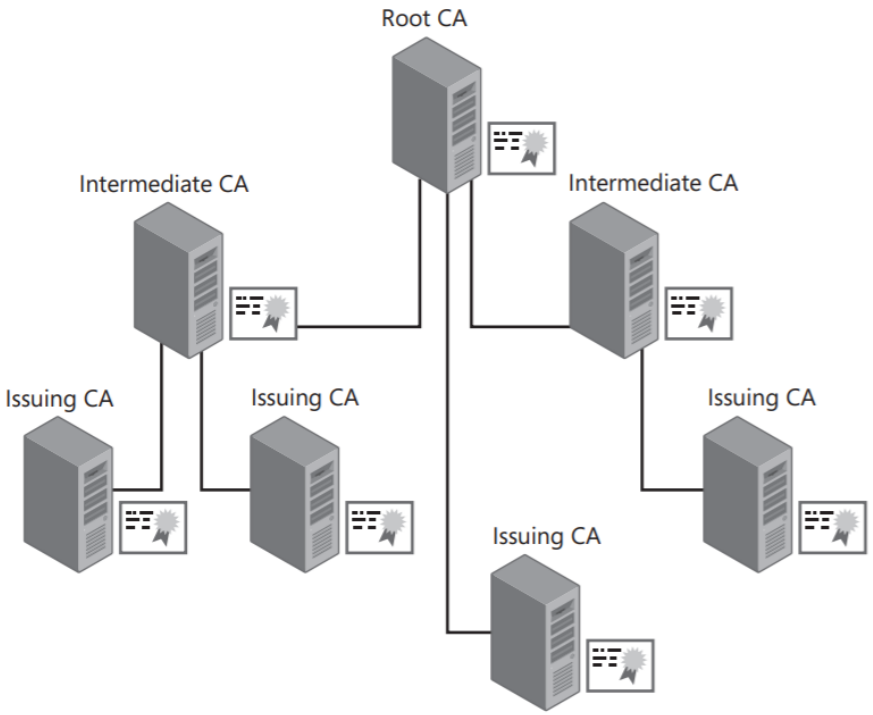
3.6 Certifikační autorita

Certifikační autorita (CA) je nezávislá třetí strana, která vydává certifikáty. Slovní spojení „certifikační autorita“ lze ale chápat dvojím způsobem: buď jako aplikaci (vydávající certifikáty) nebo jako instituci (zajišťující proces vydávání certifikátů). Jako instituce může být CA realizována jako samostatná firma nebo jako samostatný útvar v rámci firmy (5).

Certifikační autorita na základě vaší žádosti vygeneruje digitální certifikát podepsaný vaším soukromým klíčem a vydá k němu i jeho veřejnou část. K tomu musí CA ověřit vaši totožnost na základě průkazu totožnosti, pokud je žadatelem člověk, nebo firemních dokladů (např. výpisu z obchodního rejstříku), pokud je žadatelem firma. Certifikační autorita je součástí infrastruktury veřejných klíčů (PKI). Je to důvěryhodný subjekt pro všechny strany. V zásadě má certifikační autorita dvě funkce:

- Ověřuje identitu osoby.
- Generuje digitální certifikát a veřejný klíč k němu (2).

3.6.1 Hierarchie certifikačních autorit



Obrázek 10 - Hierarchie rolí certifikačních autorit (10)

Certifikační autority jsou organizovány v hierarchii kořenových CA, což zvyšuje zabezpečení a škálovatelnost hierarchie CA tím, že umožňuje, aby nevydávající CA nebyly připojeny k síti. Pokud kořenová CA a CA druhého řádu v hierarchii nejsou připojeny k síti, jsou tyto offline CA chráněny před útoky pocházejícími ze sítě. Hierarchie kořenových CA je podporována všemi předními dodavateli komerčních CA, včetně RSA, Thawte a VeriSign. Hierarchie kořenových CA je také podporována většinou aplikací a síťových zařízení. Kořenová certifikační autorita obvykle vydává certifikáty pouze jiným certifikačním autoritám, nikoli uživatelům, počítačům, síťovým zařízením nebo službám v síti (10).

3.6.2 Kvalifikované certifikační autority v ČR

K důvěryhodné archivaci dokumentů je mimo jiné potřeba vlastnit kvalifikovaný digitální certifikát. Jedná se o certifikát, který je vydán za zákonem definovaných podmínek se zákonem definovanými náležitostmi. Takový certifikát je také vydán akreditovaným poskytovatelem certifikačních služeb. Akreditaci pro vydávání kvalifikovaných certifikátů uděluje Ministerstvo vnitra ČR na základě:

- splnění podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona č. 227/2000 Sb., (zákon o elektronickém podpisu)
- splnění podmínek, požadavků a postupů stanovených vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb)
- ověření kvalifikovaných systémových certifikátů Ministerstvem vnitra podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu (11).

V České republice vydávají zpoplatněné kvalifikované certifikáty tito akreditovaní poskytovatelé:

- První certifikační autorita, a. s. – od roku 2002
- Česká pošta, s. p. – od roku 2005
- eIdentity a. s. – od roku 2005 (15)

3.7 SSL/TLS

Při navázání jakéhokoliv spojení přes internet – například při prohlížení webu nebo třeba odesílání e-mailu – sítí putuje velké množství informací. Posílají si je klient (například internetový prohlížeč) a server (třeba ten, na kterém běží internetová stránka, kterou chceme navštívit). Informace zahrnují prakticky všechen obsah, který na webové stránce vidíme, ale také to, co tam sami děláme. Jelikož ale v síti mezi klientem a cílovým serverem stojí řada dalších síťových prvků, je potřeba spojení mezi hlavními účastníky této komunikace nějak zabezpečit. Jinak by ji mohl někdo „odposlouchávat“, nebo do ní dokonce vstoupit a předstírat, že je jedním z původních účastníků komunikace. To by mohlo mít velmi negativní následky – počínaje ukradenými hesly k e-mailům či bankovním účtům a konče třeba u státní nebo industriální špionáže. Proto je důležité internetovou komunikaci a data, která se skrz ni přenáší, nějakým způsobem chránit. Právě o to se starají také protokoly, kterým se obecně říká SSL (7).

SSL je zkratka tří anglických slov „Secure Socket Layer“. Jde o vrstvu, která šifruje spojení mezi serverem a vaším internetovým prohlížečem. To, že se nějaký z rodiny protokolů

SSL v komunikaci se serverem používá, pozná při brouzdáním internetem i laik – v adresním řádku prohlížeče stojí na začátku místo zkratky protokolu HTTP zkratka HTTPS (tedy Hypertext Transfer Protocol Secure) (20).

SSL byl původně vytvořen pro ochranu spojení mezi zákazníky a online podniky. Bohužel, kybernetičtí zločinci rozšiřují svou síť tak, aby se zaměřili také na neobchodní weby. Jako takový se SSL stal široce adoptovaný. Až v roce 1999 nahradil SSL jako standardní bezpečnostní certifikát aktualizovaný protokol TLS.

TLS znamená „Transport Layer Security“ a je v podstatě SSL, ale bezpečnější. Přesněji řečeno, podpora SSL byla ukončena ve prospěch TLS – ačkoli zkratky se často používají synonymně. Podobně jako SSL, TLS je kryptografický protokol, který poskytuje soukromí, autentizaci a integritu dat v počítačových sítích a používá se při procházení webu, rychlých zpráv, e-mailu a dalších. Ale i když TLS plní stejnou roli jako SSL, činí tak efektivněji. Je to proto, že protokol TLS byl navržen tak, aby řešil známé chyby zabezpečení SSL a podporoval silnější a bezpečnější sady šifrování.

TLS nahrazuje SSL: Jeho původní účinnost a rozšířené používání však získaly trvalé místo v lidovém internetu; pojem SSL je stále široce používán, a to i v technologických a výpočetních kruzích, a mnoho certifikačních úřadů inzeruje služby certifikátů SSL, když skutečně prodávají certifikáty TLS. Ale vzhledem k tomu, že oba protokoly plní stejnou základní funkci (tj. zabezpečují digitální komunikaci proti nežádoucí manipulaci), je pochopitelné, proč běžní uživatelé nerozlišují mezi těmito dvěma protokoly. V zájmu přesnosti uživatelé a orgány často používají termín SSL/TLS.

Aby byl web označen jako bezpečný, potřebuje aktuální certifikát SSL/TLS. A zatímco certifikace SSL/TLS není nutně vyžadována, je důrazně podporována všemi hlavními prohlížeči. Ve skutečnosti v červenci 2018 začal prohlížeč Google Chrome označovat weby bez certifikace SSL/TLS jako „nezabezpečené“, což varuje potenciální návštěvníky webu. Následovaly další hlavní prohlížeče. Protokol SSL/TLS je nyní téměř všudypřítomný po celém webu (21).

3.7.1 Princip SSL spojení

SSL spojení funguje na principu asymetrické šifry. Každá z komunikujících stran má dvojici šifrovacích klíčů – veřejný a soukromý. Veřejný klíč je nutné zveřejnit a zajistit jeho správné předání všem, kteří jej budou chtít použít. Pokud pomocí tohoto klíče kdokoliv zašifruje zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče odpovídajícím soukromým klíčem. SSL umožňuje volitelně i autentizaci klienta pomocí certifikátu. Server může také požadovat, aby certifikát byl vystaven důvěryhodnou certifikační autoritou.

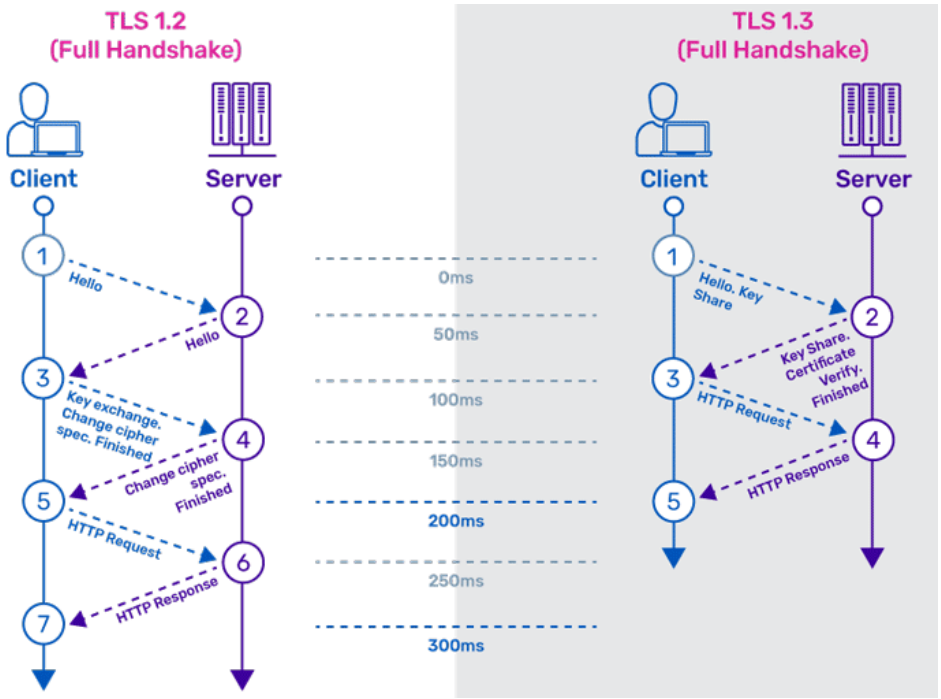
SSL spojení (SSL handshake, tedy potřásání rukou) pak probíhá následovně:

1. Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
2. Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací, a hlavně certifikát serveru.
3. Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
4. Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
5. Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
6. Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze „handshake“ tímto končí.
7. Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
8. Aplikace od teď dál komunikují přes šifrované spojení (19).

3.7.2 Nejnovější TLS verze 1.3 oproti předchozí verzi 1.2

Nejnovější TLS verze 1.3, byl vydán v srpnu 2018. Rozdíly mezi TLS 1.2 a 1.3 jsou rozsáhlé a významné a nabízejí vylepšení výkonu i zabezpečení. TLS 1.2 zároveň zůstává široce používán vzhledem k absenci známých zranitelností a nadále je vhodný pro podnikové použití. TLS 1.3 nabízí oproti dřívějším verzím několik vylepšení, zejména rychlejší

handshake a jednodušší a bezpečnější šifrovací sady. V rámci protokolu TLS 1.2 bylo počáteční předání provedeno v otevřeném textu (nezašifrovaný text), což znamená, že i toto předání bylo za potřebí zašifrovat a dešifrovat. Vzhledem k tomu, že typický handshake zahrnoval 5 – 7 paketů vyměňovaných mezi klientem a serverem, přidalo to značné náklady na připojení. Ve verzi 1.3 bylo přijato výchozí šifrování certifikátu serveru, což umožnilo uskutečnění spojení s 0 – 3 pakety. To snižuje nebo eliminuje zmíněné náklady a umožňuje rychlejší připojení. Kromě snížení počtu paketů, které mají být vyměněny během spojení, verze 1.3 také zmenšila velikost šifrovacích sad používaných pro šifrování. V TLS 1.2 a dřívějších verzích představovalo použití šifer s kryptografickými slabinami potenciální chyby zabezpečení. TLS 1.3 zahrnuje podporu pouze pro algoritmy, které v současné době nemají žádné známé chyby zabezpečení (9).

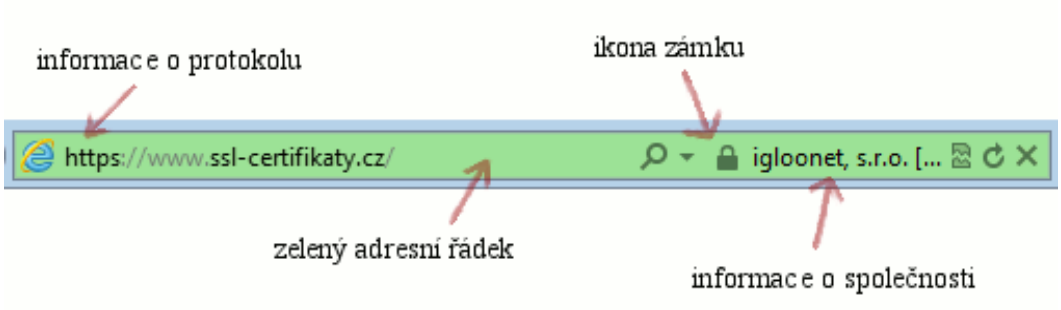


Obrázek 11 - Rozdíl v rychlosti spojení TLS 1.3 od přechozí verze (9)

3.8 HTTPS

Internet – konkrétně web – je obrovským distribuovaným informačním systémem klient/server. To znamená, že funguje prostřednictvím klientů (obvykle osobních počítačů nebo mobilních zařízení) kontaktujících servery, aby si vyžádali informace. Server poté přijme nebo odmítne požadavek klienta. Pokud je požadavek přijat, server vytvoří spojení s klientem přes konkrétní protokol. Protokol funguje jako standardní sada pravidel, která umožňují komunikaci serverů a klientů (21).

HTTPS představuje bezpečnější způsob používání internetu. Jeho předchůdcem nebo alternativou je HTTP. Právě poslední písmeno „S“ na konci je velmi důležité a znamená, že jde o zabezpečené/šifrované připojení. Jde o zkratku slov „HyperText Transfer Protocol Secure“ (20). HTTPS byl původně navržen speciálně pro e-commerce a obchodní weby, které pravidelně zpracovávají citlivé informace (jako jsou hesla a podrobnosti o kreditních kartách), ale nová doporučení naznačují, že každý web – i ty, které jsou čistě informativní – by měl používat HTTPS. Google propaguje toto myšlení tím, že nabízí mírné hodnocení vyhledávačů na weby HTTPS a zobrazením „nezabezpečených“ varování v adresních řádcích prohlížeče Google Chrome na webech, které nemají HTTPS (21).



Obrázek 12 - Příklad zabezpečené webové stránky (8)

Pokud k přenosu slouží HTTPS, pak kdokoli, kdo by se dostal ke přenášené informaci, ji nepřečte. Je čitelná pouze odesílateli a příjemci, kteří mají ten správný „kód“. SSL jsou zásadním prvkem protokolu HTTPS, bez nich by nemohl fungovat. Díky certifikátům si mohou klient a server důvěřovat, a to i v případě, že se k sobě v minulosti ještě nepřipojovali. Funguje to obdobně, jak certifikace v nějakém oboru, kterou když máte od respektované certifikační autority znamená to, že vaše znalosti jsou důvěryhodné (16).

4 Praktická část

Jak již bylo zmíněno v metodice bakalářské práce, autor realizuje porovnání vybraných certifikačních autorit pomocí komparativní metody. Nejprve provede výběr samotných certifikačních autorit. Následně budou zvolena a vysvětlena hodnotící kritéria, jako například typy certifikátů, jejich cena či délka klíče. U každého kritéria autor po důkladné analýze webových stránek či certifikačních politik zvolí váhu daného kritéria a následné bodové ohodnocení.

Veškeré tyto informace by měly být obsaženy v certifikačních politikách na webových stránkách konkrétní certifikační autority. Každá CA doporučuje tyto politiky pročíst, ačkoli to není povinností uživatele. Mimo jiné je v těchto politikách uveden životní cyklus certifikátu, profil certifikátu atd. Provedení bude zaznamenáno v tabulkách a následné porovnání prezentováno pomocí grafu. Ke konci hodnoty v tabulkách vynásobíme, konkrétně váhy a body kritérií, a následně výsledky sečteme. Nejvyšší hodnota součtu nám pak znázorní nejlepší CA.

4.1 Postup vyhodnocení certifikačních autorit

Pomocí získaných informací z analýzy certifikačních politik a webových stránek, autor vyhodnotí výsledky pro každou CA. Na celkovém výsledku se budou s určitou vahou podepisovat ostatní zvolená kritéria.

4.1.1 Určení váhy kritéria

Každé zvolené kritérium je ohodnoceno váhou, která určuje důležitost daného kritéria. Nejzásadnější kritéria budou ohodnocena váhou 3, naopak nejméně důležité váhou 1. Váha 3 je přiřazena zejména kritériím, které se týkají bezpečnosti a důvěryhodnosti. Váha 2 je u méně důležitých kritérií a nejnižší váha 1 pak u zbývajících.

4.1.2 Bodové hodnocení

Pro bodové hodnocení se autor rozhodl vytvořit škálu 0-5, kde 5 znamená nejlepší hodnocení. Může se stát, že dané kritérium CA nesplňuje, potom bude ohodnoceno 0 body. Zároveň můžou mít CA shodné hodnocení, z čehož plyne, že bude udělen stejný počet bodů.

4.2 Výběr certifikačních autorit pro první porovnání

V České republice jsou tři akreditované certifikační autority:

1. **První certifikační autorita, a.s.**
2. **Česká pošta, s.p.**
3. **eIdentity, a.s.**

Akreditaci pro vydávání kvalifikovaných certifikátů uděluje Ministerstvo vnitra České republiky na základě splnění podmínek předepsaných zákonem. Tyto CA byly vybrány zejména proto, že patří mezi nejvyužívanější v ČR a lze pomocí nich komunikovat se státní správou.

4.2.1 První certifikační autorita, a.s.

První certifikační autorita (I.CA) převzala veškerou činnost související s poskytováním služeb CA po mateřské společnosti PVT, a.s. K tomu došlo roku 2001, kdy se datuje i založení společnosti. V roce 2006 získala akreditaci pro vydávání kvalifikovaných certifikátů a kvalifikovaných časových razítek. V současné době je největším poskytovatelem služeb vydávání a správy certifikátů v České republice a na Slovensku. Webové stránky I.CA jsou www.ica.cz.

4.2.2 Česká pošta, s.p.

Služby CA **PostSignum** provozované Českou poštou jsou dostupné na adrese www.postsignum.cz nebo na kterékoli poště se službou Czech POINT. Kromě webových stránek si může uživatel stáhnout aplikaci **iSignum**, která slouží pro správu certifikátů. Stažení je bezplatné, aplikace je přehledná a lze pomocí ní generovat žádosti o certifikát,

importovat vydaný certifikát na HW zařízení nebo jen zkontrolovat položky certifikátu, jako je například platnost.

4.2.3 eIdentity, a.s.

Tato společnost vznikla počátkem roku 2004. Akreditace ministerstvem vnitra byla udělena v září roku 2005 a společnost eIdentity se tudíž stala třetím, a tak posledním akreditovaným poskytovatelem certifikačních služeb v ČR. Jelikož se dostala na trh jako poslední, měla poměrně těžké postavení, oproti dlouho se na trhu pohybující I.CA a co se týče cen služeb levnější České pošty. Webový server společnosti je přístupný na adresách www.eidentity.cz nebo také www.ie.cz.

4.3 Výběr porovnávaných kritérií pro první porovnání

4.3.1 Typy certifikátů

Typy certifikátů pojmou tři položky – Komerční certifikát, Kvalifikovaný certifikát a Komerční serverový certifikát. Komerční certifikáty jsou prakticky samozřejmostí, proto jsou ohodnoceny váhou 1. Pro vydávání kvalifikovaných certifikátů už musela CA dostat akreditaci. Z tohoto důvodu je kvalifikovaný certifikát ohodnocen váhou 2.

4.3.2 Ceny služeb

Pro mnoho uživatelů poměrně zásadní ukazatel, avšak z pohledu této práce už tak důležitý není. Nejlépe ohodnocena je ta autorita, která má nejlevnější služby. Jelikož cena služeb nemá takový dopad na bezpečnost, je ohodnocena váhou 1.

4.3.3 Počet registračních míst

Tento ukazatel podobně jako ceny služeb je důležitý pro klientelu, ačkoli z technického pohledu na certifikáty vliv nemá, proto je ohodnocen stejně váhou 1. Čím větší počet registračních míst a čím lepší rozmístění, tím lépe.

4.3.4 Služba OCSP

OCSP (Online Certificate Status Protocol) je internetový protokol sloužící k ověření stavu certifikátu. Jeho předchůdcem byl CRL (Certificate Revocation List), který je dnes už zastaralý, ale ještě má v dnešní době své využití. Možnost ověřování statutu certifikátu on-line (službou OCSP) je veřejně dostupné a bezplatné. Služba OCSP ověřuje důležité informace o certifikátu, zejména zda nebyl certifikát zneplatněn. Váha tohoto kritéria je proto 2.

4.3.5 Periodicita vydávání CRL

Když uživatel podá žádost o zneplatnění certifikátu a CA tuto žádost zpracuje, okamžitě vydá nový CRL (seznam zneplatněných certifikátů). Pokud uživatel žádnou žádost nepodá, nový CRL se vydává každých několik hodin. Periodicita vydávání CRL nám ukazuje rychlost CA pracovat s certifikáty, váha tohoto ukazatele je tedy 2.

4.3.6 Standard kryptografického modulu

Ochranu kryptografického modulu specifikuje standard FIPS 140-2. Tento modul zajišťuje bezpečnost privátního klíče, což je jedna z nejpodstatnějších částí bezpečné komunikace na internetu. Standard FIPS 140-2 má 4 úrovně. Čtvrtá úroveň zajišťuje nejlepší zabezpečení. Váha tohoto kritéria je 3, protože se týká plně bezpečnosti certifikátu.

4.3.7 Délka klíče

Klíč určuje průběh šifrovacího algoritmu neboli transformaci zprávy do šifrovaného textu a naopak. V současné době se používají klíče délky 2048 bitů, která by měla být zatím postačující, popřípadě 4096 bitů. Menší hodnoty délky klíčů by znamenali větší riziko rychlejšího prolomení klíčů. Toto kritérium patří tedy také mezi nejdůležitější, a proto mu přiřadíme váhu 3.

4.3.8 Doba platnosti certifikátu

Tento ukazatel se pojí s délkou klíče, jelikož s delší dobou platnosti certifikátu roste riziko prolomení klíče. Standartní doba platnosti certifikátů u klíčů délky 2048 bitů je 1 rok. U klíčů délky 4096 bitů jsou to pak roky 3. Provázanost s délkou klíče a samotnou bezpečností řadí tento ukazatel k váze 3.

4.4 Výběr certifikačních autorit pro druhé porovnání

Pro toto porovnání budou vybrány největší a nejvyužívanější zahraniční CA. Nejprve bych chtěl ale zmínit CA **Let's Encrypt**, která nabízí své služby zcela zdarma. Pomocí zautomatizovaného procesu poskytuje doménově ověřené certifikáty. Certifikáty od Let's Encrypt jsou sice snadno k dostání, ale musí se obnovovat každé 3 měsíce. Pro porovnání jsou vybrány následné CA:

1. **DigiCert**
2. **GeoTrust**
3. **Thawte**
4. **Comodo**
5. **RapidSSL**

4.5 Výběr porovnávaných kritérií pro druhé porovnání

Hodnocení kritérií proběhne po analýze jednotlivých stránek certifikačních autorit a následujících dvou stránek - https://cheapsslsecurity.com/, https://www.ssl2buy.com/. Ze zmíněných stránek budou čerpány hlavně ceny a záruka, pro jednotnost zdroje a tedy kvalitnější porovnání. Při výběru kritérií pro druhé porovnání nemá cenu zohledňovat některé ukazatele. Například délku klíče nebo kolika bitové je symetrické šifrování a další. Ačkoli jsou tyto kritéria důležitá, u porovnávaných CA mezi nimi není žádný rozdíl a proto nemá smysl tyto ukazatele zabrat do porovnání. Naopak následující výčet kritérií lze dobře porovnat a vypracovat pomocí nich finální komparaci.

4.5.1 Nabídka služeb

Rozmanitost produktů je poměrně důležitý ukazatel, proto je toto kritérium ohodnoceno váhou 2. Tento ukazatel bude vypovídat o tom, jestli CA nabízí certifikát pro jednu doménu, multi-doménové certifikáty, wildcard certifikáty atd. Čím rozmanitější nabídka služeb, tím lepší hodnocení.

4.5.2 Ceny služeb

Z technického hlediska, ne tak podstatný ukazatel. Přiřazena je váha 1. Kromě zohlednění standardních cen, budou také zohledněny ceny zlevněné při koupi certifikátu na více let dopředu. Ceny budou zaznamenány v kolonce hodnocení jako rozsah od certifikátů pro jednu doménu po wildcard certifikáty. Zároveň budou zaokrouhleny. Samozřejmě platí, čím levnější služby, tím lepší ohodnocení.

4.5.3 Záruka

Další ukazatel, který rozhodně stojí za zmínku je záruka a garantované vrácení peněz. Zde je váha kritéria stejná jako u cen služeb, tedy 1. Záruka bude taktéž zaznamenána jako záruka za certifikát pro jednu doménu až výše záruky pro wildcard certifikát. Znovu platí, čím větší záruka je, tím lépe je kritérium ohodnoceno.

4.5.4 Doba vystavení

Doba vystavení certifikátu se může lišit, některé certifikáty jsou vystaveny v řádu několika minut, jiné v řádu několika dnů. Čím rychlejší vystavení certifikátu CA zprostředkovává, tím lepší ohodnocení. Stejně jako u předchozích dvou ukazatelů doba vystavení se bude týkat certifikátů pro jednu doménu až wildcard certifikátů. Z technického pohledu na certifikáty je toto kritérium o něco podstatnější než ceny služeb a záruka, proto je mu přiřazena váha 2.

5 Výsledky a diskuse

5.1 První porovnání

5.1.1 Výsledné tabulky

V následující tabulce jsou zobrazeny výsledky **První certifikační autority**.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Komerční certifikát	1	Ano	1	1
Kvalifikovaný certifikát	2	Ano	1	2
Komerční serverový certifikát	1	Ano	1	1
Ceny služeb	1	Vysoké	2	2
Počet registračních míst	1	33 míst	2	2
Služba OCSP	2	Ano	2	4
Periodicita vydávání CRL	2	12h, max 24h	2	4
Standard kryptografického modulu	3	FIPS 140-2 úrovně 3	4	12
Délka klíče	3	Min 2048 bitů	3	9
Doba platnosti certifikátu	3	1 rok	3	9
Celkový součet				**46**

Tabulka 2 - Výsledná tabulka První certifikační autority

V následující tabulce jsou zobrazeny výsledky **PostSignum** od České pošty.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Komerční certifikát	1	Ano	1	1
Kvalifikovaný certifikát	2	Ano	1	2
Komerční serverový certifikát	1	Ano	1	1
Ceny služeb	1	Nízké	4	4
Počet registračních míst	1	951 míst	5	5
Služba OCSP	2	Ano	2	4
Periodicita vydávání CRL	2	4h, max 24h	3	6
Standard kryptografického modulu	3	FIPS 140-2 úrovně 3	4	12
Délka klíče	3	2048 bitů, 4096 bitů	4	12
Doba platnosti certifikátu	3	1 rok, 3 roky	4	12
Celkový součet				**59**

Tabulka 3 - Výsledná tabulka PostSignum

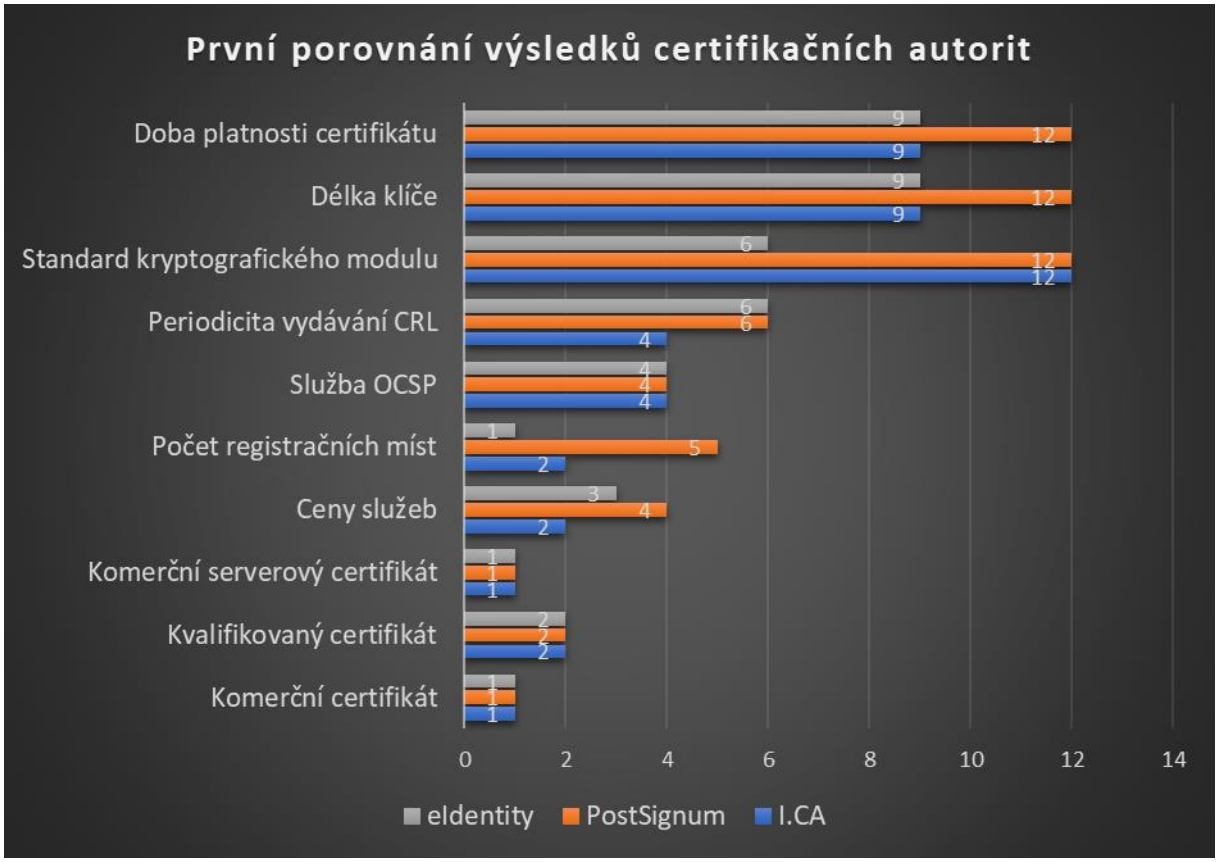
V následující tabulce jsou zobrazeny výsledky **eIdentity**.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Komerční certifikát	1	Ano	1	1
Kvalifikovaný certifikát	2	Ano	1	2
Komerční serverový certifikát	1	Ano	1	1
Ceny služeb	1	Střední	3	3
Počet registračních míst	1	3 místa	1	1
Služba OCSP	2	Ano	2	4
Periodicita vydávání CRL	2	4h, max 24h	3	6
Standard kryptografického modulu	3	FIPS 140-1 nebo novější	2	6
Délka klíče	3	Min 2048 bitů	3	9
Doba platnosti certifikátu	3	1 rok	3	9
Celkový součet				**42**

Tabulka 4 - Výsledná tabulka eIdentity

5.1.2 Výsledný graf

Následující graf zobrazuje srovnání výsledků certifikačních autorit v jednotlivých kritériích. Už na první pohled je dobře vidět, že kritéria, kterým autor přiřadil největší váhu, jsou v horní polovině grafu, počínaje standardem kryptografického modulu. Jak již bylo zmíněno, čím více u jednotlivého kritéria, tím lépe.



Obrázek 13 - Graf výsledků prvního porovnání certifikačních autorit

5.1.3 Výsledky porovnání

Po analýze výsledných tabulek a grafu prvního porovnání byly vyvozeny následující závěry:

- Zmíněné **typy certifikátů** vydávají všechny CA, proto je hodnocení u těchto parametrů naprosto stejné.
- V **cenách služeb** už určitý rozdíl je, ačkoli není tak markantní. Z tohoto důvodu není ani hodnocení tak rozdílné. Lze vidět, že s nejvyšším výsledkem, tedy nejlevnější služby, je PostSignum od České pošty. Pro příklad cena

za Komerční serverový certifikát u PostSignum je 800 Kč. Naopak nejdražší služby nabízí První certifikační autorita (Komerční serverový certifikát – 1170 Kč).

- Znatelný rozdíl činí **počet registračních míst**. Česká pošta s počtem 951 registračních míst, kterými jsou Czech POINTY, s přehledem vede. Na rozdíl od toho eIdentity se třemi registračními místy pouze v hlavním městě Praze neposkytuje zákazníkům takovou flexibilitu.
- Stejně jako typy certifikátů, **službu OCSP** poskytují všechny CA. To znamená rychlé aktualizace seznamu zneplatněných certifikátů (CRL).
- Dalším kritériem byla **periodicita vydávání CRL**, kde nejhůře skončila I.CA s aktualizacemi každých 12h. PostSignum i eIdentity aktualizuje seznam každé 4h.
- Dále už figurují nejdůležitější kritéria s váhou 3 a prvním z nich je **standard kryptografického modulu**. Zde všechny autority splňují požadavky na bezpečnost standardu FIPS 140-2. Jak již bylo řečeno (viz. kapitola 4.3.6) tento standard má 4 úrovně. CA eIdentity ve své certifikační politice pro komerční certifikáty uvádí standard FIPS 140-2 úrovně 1, tedy nejnižší a nejméně bezpečné úrovně. Z tohoto důvodu má eIdentity horší hodnocení než zbylé dvě CA.
- Dalším důležitým ukazatelem z hlediska bezpečnosti je **délka klíče** a s ní spojená **doba platnosti certifikátu**. Všechny CA nabízejí stejnou délku klíče 2048 bitů na 1 rok. Avšak PostSignum navíc nabízí klíče s délkou 4096 bitů a to na 3 roky. Jelikož to není až tak velký rozdíl z pohledu zabezpečení jako spíše z pohledu pohodlí uživatelů, je bodové hodnocení jen lehce vyšší.

5.2 Druhé porovnání

5.2.1 Výsledné tabulky

V následující tabulce jsou zobrazeny výsledky CA **DigiCert**.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Nabídka služeb	2	Velká	4	8
Ceny služeb	1	3 500 – 12 200 Kč	1	1
Záruka	1	1 mil USD	5	5
Doba vystavení	2	<1 den	1	2
Celkový součet				**16**

Tabulka 5 - Výsledná tabulka DigiCert

V následující tabulce jsou zobrazeny výsledky CA **GeoTrust**.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Nabídka služeb	2	Střední	3	6
Ceny služeb	1	1 000 – 3 800 Kč	3	3
Záruka	1	500 000 USD	3	3
Doba vystavení	2	<30 min	4	8
Celkový součet				**20**

Tabulka 6 - Výsledná tabulka GeoTrust

V následující tabulce jsou zobrazeny výsledky CA **Thawte**.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Nabídka služeb	2	Malá	2	4
Ceny služeb	1	750 – 6 000 Kč	2	2
Záruka	1	500 000 – 1,25 mil USD	4	4
Doba vystavení	2	<10 min – 1 den	2	4
Celkový součet				**14**

Tabulka 7 - Výsledná tabulka Thawte

V následující tabulce jsou zobrazeny výsledky CA **Comodo**.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Nabídka služeb	2	Největší	5	10
Ceny služeb	1	170 – 2 800 Kč	4	4
Záruka	1	10 000 – 250 000 USD	2	2
Doba vystavení	2	<5 min – 1 den	3	6
Celkový součet				**22**

Tabulka 8 - Výsledná tabulka Comodo

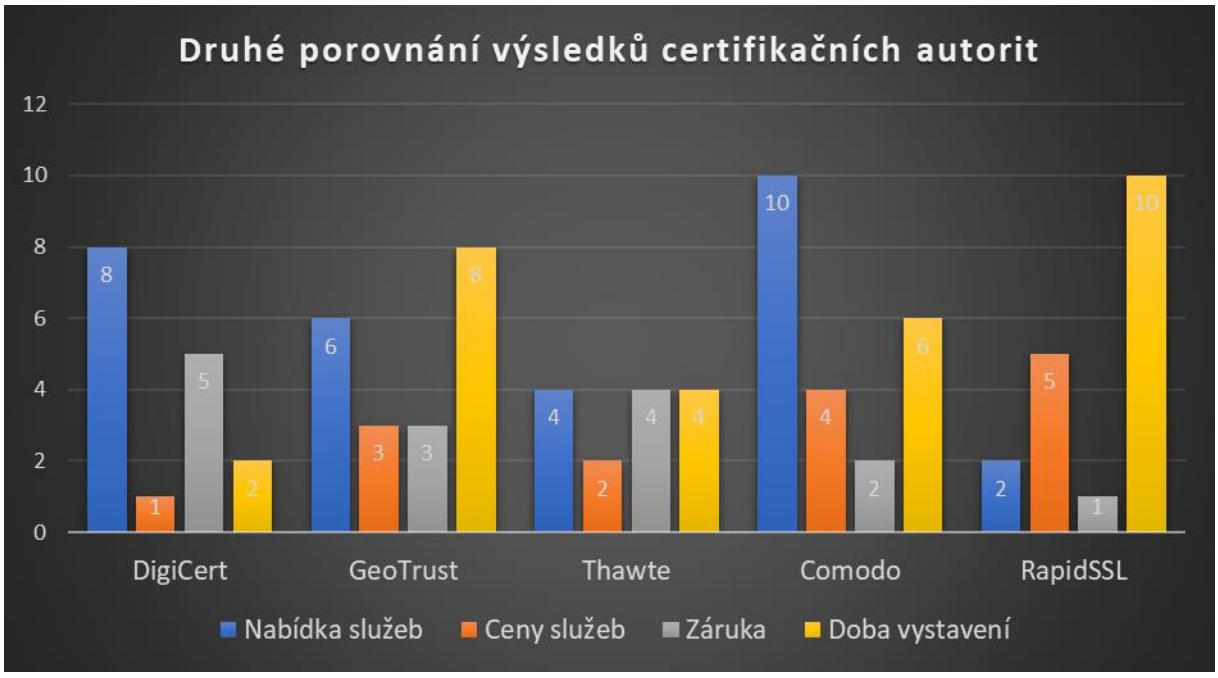
V následující tabulce jsou zobrazeny výsledky CA **RapidSSL**.

Hodnocené kritérium	Váha	Hodnocení	Body	Výsledek
Nabídka služeb	2	Nejmenší	1	2
Ceny služeb	1	250 – 1 900 Kč	5	5
Záruka	1	10 000 USD	1	1
Doba vystavení	2	<10 min	5	10
Celkový součet				**18**

Tabulka 9 - Výsledná tabulka RapidSSL

5.2.2 Výsledný graf

Následující graf zobrazuje srovnání výsledků certifikačních autorit v jednotlivých kritériích. Můžeme vidět, že nejpodstatnější rozdíly jsou u kritérií s váhou 2, tedy u nabídky služeb a doby vystavení.



Obrázek 14 - Graf výsledků druhého porovnání certifikačních autorit

5.2.3 Výsledky porovnání

Po analýze výsledných tabulek a grafu druhého porovnání byly vyvozeny následující závěry:

- U **nabídky služeb** s přehledem vede certifikační autorita Comodo (nabízí přes 60 produktů) před společností DigiCert. Naopak RapidSSL nabízí pouze dva produkty, certifikáty pro jednu doménu a wildcard certifikáty, a má tak nejnižší ohodnocení. V závěsu je společnost Thawte, která má ve své nabídce 6 produktů.
- Nejdražší produkty nabízí DigiCert. Rozdíl u cen za wildcard certifikáty od druhé společnosti Thawte činí přibližně 6 000 Kč. Nejnižší **ceny služeb** má RapidSSL a společnost Comodo. Konkrétně RapidSSL nabízí nejlevnější wildcard certifikáty a Comodo nejlevnější certifikáty pro jednu doménu. U wildcard certifikátů je mezi těmito certifikačními autoritami větší rozdíl, proto je RapidSSL lépe ohodnocena ve výsledném porovnání.
- Co se týče výše **záruk**, zde si nejlépe stojí DigiCert a Thawte. Naopak nejnižší záruky, 10 000 USD, nabízí RapidSSL.
- RapidSSL dostává svého jména a vystavení certifikátu zde trvá pouze několik sekund až minut. Hned za RapidSSL je společnost GeoTrust s **dobou vystavení** do půl hodiny. Nejdéle vystavení certifikátů trvá certifikační autoritě DigiCert.

5.3 Diskuse

Nejprve několik slov k prvnímu porovnání nejvyužívanějších českých certifikačních autorit. Na pomyslném třetím místě skončila certifikační autorita **eIdentity s celkovým součtem 42**. Druhá pak byla **První certifikační autorita s výsledkem 46** a nejlépe hodnocená skončila certifikační autorita od České pošty, **PostSignum, s celkovým součtem 59**. Samozřejmě každá CA má své klady a zápory, což lze z výsledků dobře poznat (viz Obrázek 12).

PostSignum se nejvíce vydává vstříc uživateli a jeho pohodlí. Má nejnižší ceny služeb, je nejsnáze dostupná a vystavuje i tříleté certifikáty, pro uživatele, kteří nechtějí být každoročně obtěžováni obnovováním certifikátu. U První certifikační autority lze vyzdvihnout množství jejích pozitivních referencí a také to, že na trhu figuruje nejdéle, což jen vypovídá o její kvalitě. Na druhou stranu nabízí služby za nejdražší ceny. Ačkoli CA eIdentity skončila s nejnižším celkovým součtem, nezaostává o tolik. Fakt, že dostala

akreditaci jako poslední a naskočila tak jako nová společnost na nabytý trh nebo například to, že má do dnešní doby pouze tři registrační místa, vzrůstu její klientely moc nepomáhá.

Výsledné součty jednotlivých certifikačních autorit u druhého porovnání jsou následující:

1. **Comodo – 22**
2. **GeoTrust – 20**
3. **RapidSSL – 18**
4. **DigiCert – 16**
5. **Thawte – 14**

Společnost Comodo je na pomyslném prvním místě zaslouženě. Nabízí největší výběr produktů za velmi přívětivé ceny. Soustředí se tak na rozsáhlý záběr zákazníků. Srovnáme-li Comodo se společností DigiCert, která skončila na místě čtvrtém, DigiCert se zaměřuje zejména na velké firmy a organizace. Proto má ceny nastavené značně vysoko, stejně jako výši záruk. Záruka za certifikát pro jednu doménu u DigiCert činí 1 milion USD. Společnost Thawte je v porovnávaných ukazatelích průměrná až podprůměrná, což zapříčinilo to, že skončila na posledním místě. Na druhou stranu certifikační autorita GeoTrust v ničem nevyčnívá, ale její nadprůměrné výsledky ji pomohly na druhé místo v celkovém hodnocení. Certifikační autorita RapidSSL by se v rámci porovnání dala označit jakožto opak společnosti DigiCert. Sice nenabízí takový rozptyl produktů a záruky činí 10 000 USD, ale její produkty jsou velmi levné a jejich vystavení probíhá prakticky okamžitě.

6 Závěr

Tato bakalářská práce vysvětluje problematiku digitálních certifikátů, od základů šifrování a kryptografie, popisu certifikátů až po protokol HTTPS a certifikační autority, které jsou poté porovnány v praktické části práce.

Digitální certifikáty jsou v dnešní době velmi využívané v on-line prostředí, konkrétně v oblasti zabezpečení a ochrany osobních údajů. Avšak samotní zákazníci s certifikáty tolik obeznámeni nejsou.

Praktická část byla rozdělena na dvě porovnání. U prvního se porovnávaly nejvyužívanější české certifikační autority a u druhého největší zahraniční certifikační autority. Na základě výsledků lze zákazníkovi doporučit vhodnou certifikační autoritu a také na které ukazatele by se měl při výběru certifikátu nejvíce zaměřit. Ceny služeb nebo počet registračních míst hrají při volbě certifikační autority určitou roli, ale zákazník by se měl zaměřit hlavně na bezpečnostní prvky certifikátů. Mezi ty patří například délka klíčů, která se bude v budoucnu pravděpodobně ještě zvyšovat, kvůli možnému prolomení.

Dnes by již každá webová stránka, kde uživatel zadává své osobní údaje, hesla nebo čísla účtů apod., měla být pomocí certifikátu zabezpečená. Pokud tomu tak není, prohlížeč na takové stránky automaticky upozorňuje a jsou označovány jako nedůvěryhodné.

7 Seznam použitých zdrojů

(1) BURDA, Karel. *Kryptografie okolo nás* [online]. Praha: CZ.NIC, z. s. p. o., 2019 [cit. 2021-02-16]. CZ.NIC. ISBN 978-80-88168-52-2. Dostupné z: https://knihy.nic.cz/files/edice/Kryptografie_okolo_nas.pdf. Stránka 15 – 25.

(2) CA (Certifikační autorita). In: ManagementMania.com [online]. Wilmington (DE) 2011-2021, 20.04.2018 [cit. 10.03.2021]. Dostupné z: https://managementmania.com/cs/ca-certifikacni-autorita

(3) Co je to WildCard SSL certifikát. *SSLmentor* [online]. Brno, 2021, 13. 4. 2019 [cit. 2021-02-16]. Dostupné z: https://blog.sslmentor.cz/clanky/ssl/co-je-to-wildcard-ssl-certifikat/

(4) Digitální certifikát. *Earchivace.cz* [online]. 2014 [cit. 2021-02-16]. Dostupné z: http://www.earchivace.cz/technologie/digitalni-certifikat/

(5) DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., aktualiz. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6. Dostupné také z: https://static.artforum.sk/media/products-files/32/bf/129787-DB65092.pdf. Stránka 30 – 76.

(6) Elektronický podpis online: Co je Elektronický podpis. In: *SSLmentor* [online]. Brno, 2021 [cit. 2021-02-16]. Dostupné z: https://www.sslmentor.cz/napoveda/elektronicky-podpis-online

(7) HANÁK, Jiří. Vysvětlení SSL certifikátů: Co jsou, jak fungují a proč je používat. *MasterDC* [online]. Brno, 2021, 29. 03. 2016 [cit. 2021-02-16]. Dostupné z: https://www.master.cz/blog/co-jsou-ssl-certifikaty-a-ssl-protokoly-jak-funguji-vysvetleni-navod/

(8) Jak poznat zabezpečené stránky?: Adresní řádek. In: *SSLcertifikaty.cz* [online]. Brno: igloonet, 2021, 19. 9. 2012 [cit. 2021-02-16]. Dostupné z: https://www.ssl-certifikaty.cz/blog/ze-sveta-certifikatu/8881-jak-poznat-zabezpecene-stranky.html

(9) KHAN, Babur. Key differences Between TLS 1.2 and TLS 1.3. *A10 Networks* [online]. 3. 8. 2020 [cit. 2021-03-11]. Dostupné z: https://www.a10networks.com/blog/key-differences-between-tls-1-2-and-tls-1-3/

(10) KOMAR, Brian. *Windows Server 2008 PKI and Certificate Security* [online]. Washington: Microsoft Press, 2008 [cit. 2021-02-16]. ISBN 978-80-88168-52-2. Dostupné z: https://kvazar.files.wordpress.com/2008/12/unencrypted.pdf. Stránka 4 – 30.

(11) Kvalifikované certifikační autority: Akreditovaní poskytovatelé certifikačních služeb. *Earchivace.cz* [online]. 2014 [cit. 2021-02-16]. Dostupné z: http://www.earchivace.cz/clanky/kvalifikovane-certifikacni-autority/

(12) Multi-doménové SSL certifikáty (SAN). *SSLmentor* [online]. Brno, 2021 [cit. 2021-02-16]. Dostupné z: https://www.sslmentor.cz/ssl/multidomain

(13) PETERKA, Jiří. *Báječný svět elektronického podpisu* [online]. Praha: CZ.NIC, z. s. p. o., 2011 [cit. 2021-02-16]. CZ.NIC. ISBN 978-80-904248-3-8. Dostupné z: https://knihy.nic.cz/files/edice/bajecny_svet_elektronickeho_podpisu_cznic.pdf. Stránka 37 – 50.

(14) PETERKA, Jiří. Není certifikát jako certifikát. CA PostSignum týden mátla své zákazníky. In: *Lupa.cz: Server o českém Internetu* [online]. Praha: Internet Info, 2021, 20. 1. 2014 [cit. 2021-02-16]. Dostupné z: https://www.lupa.cz/clanky/neni-certifikat-jako-certifikat-ca-postsignum-tyden-matla-sve-zakazniky/

(15) Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb. *Ministerstvo vnitra České republiky* [online]. Praha, 30. 5. 2016 [cit. 2021-02-16]. Dostupné z: https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx

(16) Rozdíl mezi HTTP a HTTPS? Víme bezpečně. *PC Poradenství.cz* [online]. Praha: PCPoradenstvi.cz, 2020 [cit. 2021-02-16]. Dostupné z: http://www.pcporadenstvi.cz/rozdil-mezi-http-https-vime-bezpecne

(17) Rozšířené ověření (Extended Validation). In: *SSLmarket* [online]. Brno [cit. 2021-02-16]. Dostupné z: https://www.sslmarket.cz/ssl/ev-certifikaty-rozsirene-overeni/

(18) Serverové certifikáty. *Jak na internet* [online]. Praha: CZ.NIC, 2021 [cit. 2021-02-16]. Dostupné z: https://www.jaknainternet.cz/page/1784/serverove-certifikaty/

(19) SSL protokol. *SSLcertifikaty.cz* [online]. Brno: igloonet, 2021 [cit. 2021-02-16]. Dostupné z: https://www.ssl-certifikaty.cz/o-certifikatech/ssl-protokol/

(20) SUJA, Róbert. Jaký je rozdíl mezi HTTPS a SSL? *Bridge ecommerce magazine* [online]. Bratislava, 2021, 12. 6. 2020 [cit. 2021-02-16]. Dostupné z: https://www.ecommercebridge.cz/jaky-je-rozdil-mezi-https-a-ssl/

(21) Šifrování a autentizace: Co je to SSL, TLS a HTTPS. *ICTBLOG* [online]. 22. 10. 2019 [cit. 2021-02-16]. Dostupné z: https://www.ictblog.cz/sifrovani-a-autentizace-co-je-to-ssl-tls-a-https/

(22) Typy SSL certifikátů pro zabezpečení domén: SSL certifikát pro jednu doménu. *SSLmentor* [online]. Brno, 2021, 14. 2. 2019 [cit. 2021-02-16]. Dostupné z: https://blog.sslmentor.cz/clanky/typy-ssl-certifikatu-pro-zabezpeceni-domen/

(23) VOCŮ, Michal. Šifrování a šifrovací systémy. *Ikaros* [online]. 1997, **1**(6) [cit. 2021-02-16]. ISSN 1212-5075. Dostupné z: https://ikaros.cz/sifrovani-sifrovaci-systemy

(24) What Is a Self Signed Certificate? Know the Advantages and Disadvantages. *SECTIGO* [online]. St. Petersburg, 2021 [cit. 2021-03-10]. Dostupné z: https://sectigostore.com/page/what-is-a-self-signed-certificate/

(25) WildCard SSL certifikáty. *SSLmentor* [online]. Brno, 2021 [cit. 2021-02-16]. Dostupné z: https://www.sslmentor.cz/ssl/wildcard