Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Důvěryhodnost serverových certifikátů

Alex Kroča

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Alex Kroča

Informatika

Název práce

Důvěryhodnost serverových certifikátů

Název anglicky

Trustworthiness of server certificates

Cíle práce

Hlavní cíl: Hlavním cílem práce je vytvořit doporučení pro výběr důvěryhodného certifikátu pro zabezpečení serveru s ohledem na ekonomické faktory spojené s tímto výběrem.

Dílčí cíle:
- Vymezit problematiku důvěryhodnosti serverových certifikátů.
- Charakterizovat problematiku self-signed certifikátů s ohledem na jejich využití a dopad na bezpečnost a důvěru v online prostředí v porovnání s certifikáty podepsanými důvěryhodnou certifikační autoritou.
- Porovnat vybrané certifikační autority na trhu.

Metodika

Metodika řešení teoretické části bakalářské práce je založena na studiu a analýze odborných a vědeckých informačních zdrojů a současného stavu serverových certifikátů pro https se zaměřením na problematiku self-signed certifikátů a důvěryhodnosti certifikačních autorit pro koncové uživatele.

Na základě znalostí získaných v teoretické části práce autor v praktické části porovná důvěryhodnost serverových certifikátů podepsaných důvěryhodnou certifikační autoritou se self-signed certifikáty za pomocí analýzy bezpečnosti a následně pomocí komparativní analýzy mezi sebou porovná vybrané certifikační autority. Na základě syntézy poznatků teoretické části a vyhodnocení výsledků praktické části budou formulovány závěry práce.

Doporučený rozsah práce

40-50

Klíčová slova

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

---

Doporučené zdroje informací

DOSTÁLEK, Libor a Marta VOHNOUTOVÁ. Velký průvodce infrastrukturou PKI. 2., aktualiz. 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

2023/24 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 04. 03. 2024

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 15.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Tomáši Vokounovi za věcné připomínky, trpělivost a vstřícnost při konzultacích a tvorbě bakalářské práce.

Důvěryhodnost serverových certifikátů

Abstrakt

Tato bakalářská práce se zabývá problematikou serverových certifikátů a jejich vlivem na zabezpečení online serverů. V první kapitole jsou popsány základy kryptografie a metody šifrování. V další kapitolách jsou popsány digitální a serverové certifikáty a jejich typy. V následné kapitole jsou popsány certifikační autority a jejich fungování. A na závěr teoretické části jsou vysvětleny principy protokolů HTTPS, SSL a TLS.

V praktické části je vypracováno porovnání důvěryhodnosti serverových certifikátů podepsaných důvěryhodnou certifikační autoritou se self-signed certifikáty a následně je vypracováno porovnání vybraných certifikačních autorit. Výsledky obou porovnání jsou zapsány do tabulek a prezentovány pomocí grafů. Na závěr jsou všechny výsledky porovnání shrnuty a je vytvořeno doporučení pro výběr certifikátu od nejvhodnější certifikační autority.

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

Trustworthiness of server certificates

Abstract

This bachelor thesis deals with the issue of server certificates and their impact on the security of online servers. The first chapter describes the basics of cryptography and encryption methods. The next chapters describe digital and server certificates and their types. In the following chapter, certificate authorities and their functioning are described. Finally, the theoretical part explains the principles of HTTPS, SSL and TLS.

In the practical part, a comparison of the trustworthiness of server certificates signed by a trusted certificate authority with self-signed certificates is developed, followed by a comparison of selected certificate authorities. The results of both comparisons are tabulated and presented using graphs. Finally, all the results of the comparison are summarized and a recommendation is made for selecting the certificate from the most suitable certification authority.

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

Obsah

1 Úvod

Kromě zvýšené propojenosti a poskytnutí obrovského množství nových služeb poskytuje internet také útočiště pro hackery a jiné osoby snažící se o odcizení osobních údajů. I proto se klade s neustále narůstajícím počtem hackerských útoků čím dál tím větší pozornost internetové bezpečnosti. Je nezbytné, aby se uživatelé mohli proti takovým útokům bránit. K tomu jim slouží mimo jiné i serverové certifikáty.

Online prostředí je čím dál tím větší a s ním i počet webových stránek, které vyžadují zadání osobních údajů, hesel a dalších citlivých informací. Je tedy důležité, aby byl zabezpečen přenos dat mezi klientem a serverem. Toho docílíme pomocí šifrované komunikace. Právě serverové certifikáty a certifikační autority nám zaručí, že daná komunikace je šifrována. K tomu abychom měli jistotu, že je komunikace dobře zabezpečená, musí daný server používat takový certifikát, který je vydán důvěryhodnou certifikační autoritou.

Tato bakalářská práce se zaměřuje na problematiku důvěryhodnosti serverových certifikátů, což je téma nesmírně aktuální a významné v dnešním digitálním světě. Naše společnosti a organizace stále více závisí na bezpečné komunikaci online, což představuje výzvy v oblasti kybernetické bezpečnosti. Zajištění, že serverový certifikát je skutečný a důvěryhodný, je základním předpokladem pro vytvoření důvěry mezi uživateli a online službami.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je vytvořit doporučení pro výběr důvěryhodného certifikátu pro zabezpečení serveru s ohledem na ekonomické faktory spojené s tímto výběrem.

Mezi dílčí cíle patří vymezit problematiku důvěryhodnosti serverových certifikátů, charakterizovat problematiku self-signed certifikátů s ohledem na jejich využití a dopad na bezpečnost a důvěru v online prostředí v porovnání s certifikáty podepsanými důvěryhodnou certifikační autoritou a porovnat vybrané certifikační autority na trhu.

2.2 Metodika

Metodika řešení teoretické části bakalářské práce je založena na studiu a analýze odborných a vědeckých informačních zdrojů a současného stavu serverových certifikátů pro https se zaměřením na problematiku self-signed certifikátů a důvěryhodnosti certifikačních autorit pro koncové uživatele.

Na základě znalostí získaných v teoretické části práce autor v praktické části porovná důvěryhodnost serverových certifikátů podepsaných důvěryhodnou certifikační autoritou se self-signed certifikáty za pomocí analýzy bezpečnosti a následně pomocí komparativní analýzy mezi sebou porovná vybrané certifikační autority. Na základě syntézy poznatků teoretické části a vyhodnocení výsledků praktické části budou formulovány závěry práce.

3 Teoretická východiska

3.1 Základy kryptografie a metody šifrování

Kryptografie představuje vědu, která se zabývá matematickými metodami utajování obsahu a prokazování původu přenášených zpráv. V tomto kontextu definujeme zprávu jako číselnou posloupnost, kde informace je zakódována do veřejně známého kódu. V praxi se často jedná o textové informace, obrázky nebo dokonce instrukce vyjádřené jako posloupnost binárních číslic, známých jako bity. (1)

Autor zprávy, označovaný jako původce, přenáší svou zprávu přes vhodný přenosový systém, obvykle počítačovou síť, k zamýšlenému příjemci, označovanému jako adresát. Z kryptografického pohledu jsou tyto přenosové systémy často vnímány jako veřejné přenosové kanály, což znamená, že kromě původce a adresáta mají k nim přístup také jiné, neoprávněné osoby. Někteří z těchto osob se snaží číst nebo dokonce modifikovat přenášené zprávy, a proto jsou považováni za hrozbu. Kryptografické techniky jsou navrženy tak, aby původce a adresát mohli zajistit ochranu svých přenášených zpráv před těmito hrozbami. V případě ochrany důvěrnosti zpráv útočníci nemohou zjistit obsah přenášených zpráv. A co se týče prokázání původu zpráv, adresát může ověřit, zda přijatá zpráva skutečně pochází od uvedeného původce, a zda nebyla během přenosu nějakým způsobem narušena nebo padělána. (1)

Zabezpečená komunikace mezi původcem a adresátem je definována pomocí kryptografických protokolů. Základními stavebními kameny kryptografických protokolů jsou datové jednotky, což jsou bloky bitů, které si původce a adresát mezi sebou vyměňují. Každý typ datové jednotky má svou specifickou strukturu a význam. Kromě různých typů datových jednotek obsahuje protokol i soubor pravidel, kterými se řídí výměna datových jednotek mezi původcem a adresátem, což jsou strany protokolu. Existují i vícestranné protokoly, kde se účastní více subjektů. Příkladem jsou platební protokoly, na nichž se kromě plátce a příjemce podílí také banky zúčastněných. (1)

3.1.1 Otisk (Haš)

Hašovací funkce je matematická jednocestná funkce, která převádí vstup libovolné délky na šifrovaný výstup pevné délky. Bez ohledu na původní množství dat nebo velikost souboru, výsledný otisk bude vždy stejné délky. Navíc haše nelze použít k tzv. „revers engineering" vstupu z hašovaného výstupu, protože hašovací funkce jsou "jednosměrné" (jako masový mlýnek na maso; nemůžete zpět udělat steak z mletého masa). Přesto, pokud použijete takovou funkci na týchž původních datech, bude její haš identický, takže můžete ověřit, zda jsou data stejná (tj. nezměněná), pokud již znáte jejich haš. Typické hašovací funkce přijímají vstupy různých délek a vracejí výstupy pevné délky. Kryptografická hašovací funkce kombinuje schopnosti hašovacích funkcí s bezpečnostními vlastnostmi. Hašovací funkce jsou algoritmy, které určují, jak je informace šifrována. (2)

Například bezpečný hašovací algoritmus 256 (SHA-256) projde procesem šifrování přijatého vstupu takto:

- Převedení na binární formát
- Vytvoření hašovacích hodnot
- Inicializace konstant
- Rozdělení dat na bity
- Vytvoření plánu zpráv
- Spuštění smyčky komprese
- Modifikace finálních hodnot

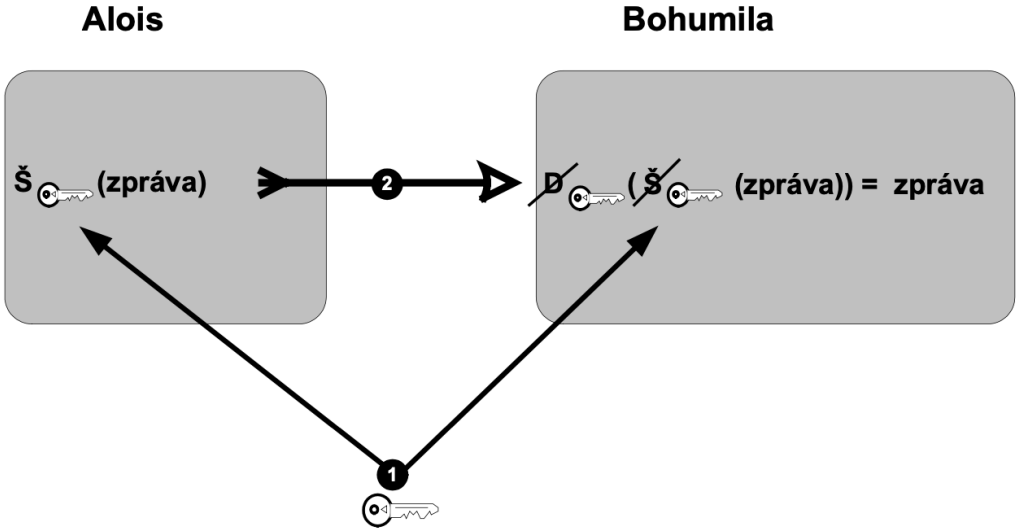
Použitím algoritmu SHA-256 slovo „Ahoj" vytvoří výstup, který má stejný počet znaků (64) jako „Ahoj světe" nebo „Ahoj Honzo." Hašovací hodnota však bude výrazně odlišná pro všechny tři slova:

- **Ahoj**: 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969
- **Ahoj světe**: 64ec88ca00b268e5ba1a35678a1b5316d212f4f366b2477232534a8aeca37f3c
- **Ahoj Honzo:** a8119595d77342cc73c93697a7f70920d3f4ded5d458e31907607e997ff76868 (2)

Avšak u některých algoritmů (např. MD-5) se již daří nacházet texty se stejným otiskem. Výsledkem je pak opouštění těchto algoritmů a nahrazení je jinými novějšími algoritmy. (2)

3.1.2 Symetrické šifrování

Symetrické šifrování používá stejný klíč pro šifrování a dešifrování. Algoritmy související se symetrickým šifrováním jsou schopny zašifrovat velké množství dat v krátkém časovém období díky použití jediného klíče a skutečnosti, že symetrické šifrovací algoritmy jsou mnohem jednodušší než asymetrické šifrovací algoritmy. Při šifrování dat pomocí symetrického algoritmu systém generuje náhodný symetrický klíč. Délka klíče, obvykle vyjádřená v bitech, je definována algoritmem a aplikací využívající symetrický algoritmus. Po vygenerování symetrického klíče se používá k šifrování dat ve formátu prostého textu do zašifrovaného stavu, který se nazývá šifrovaný text. Šifrovaný text je poté odeslán nebo zpřístupněn příjemci dat. Symetrický klíč musí být bezpečně odeslán příjemci, než může příjemce dešifrovat šifrovaný text. Odeslání symetrického klíče je největším bezpečnostním rizikem při použití symetrického šifrovacího algoritmu. (3)



Obrázek 1: Symetrická šifra *(3)*

3.1.3 Asymetrické šifrování

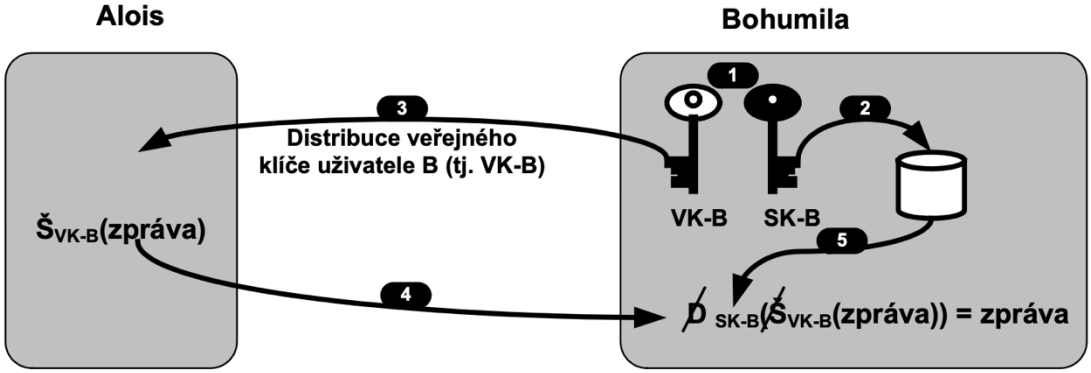
Dalším typem šifry je asymetrická šifra. Tyto šifry nepoužívají pouze jeden tajný šifrovací klíč sdílený mezi odesílatelem a příjemcem, ale vždy používají dvojici šifrovacích klíčů. Jeden klíč se používá pro šifrování a jeden klíč pro dešifrování. Asymetrické

kryptografické systémy představují způsob šifrování, kde zásadní vlastností je, že je prakticky nemožné odvodit dešifrovací klíč z hodnoty šifrovacího klíče, což zvyšuje bezpečnost komunikace. V rámci těchto systémů je třeba pečlivě střežit pouze hodnotu dešifrovacího klíče. (4)

Představme si situaci, kdy adresát B chce zabezpečit svou komunikaci. Nejprve provede proces vytvoření dvou klíčů: šifrovacího a dešifrovacího. Tyto klíče se odvozují z velkých náhodných čísel a pravděpodobnost, že dva různí uživatelé vytvoří identickou dvojici klíčů, je téměř nulová. Dešifrovací klíč zůstává tajný a zná ho pouze tvůrce klíče B, což se označuje jako soukromý klíč. (4)

Naopak šifrovací klíč tvůrce systému kryptografie zveřejní, což se označuje jako veřejný klíč strany B. Tedy platí, že dešifrovací klíč je soukromým klíčem, zatímco šifrovací klíč je veřejným klíčem. Důležitou výhodou tohoto přístupu je, že kdokoli může adresátovi B poslat šifrovanou zprávu (kryptogram), aniž by bylo nutné se s ním předem dohodnout na sdílení šifrovacího klíče. Tím se zjednodušuje proces komunikace. (4)

Nevýhodou je, že asymetrické kryptografické systémy jsou obecně pomalejší než systémy používající symetrické šifrování, a proto se obvykle používají pro šifrování dat o malém objemu, jako jsou například klíče pro symetrické šifrování nebo hesla. (4)

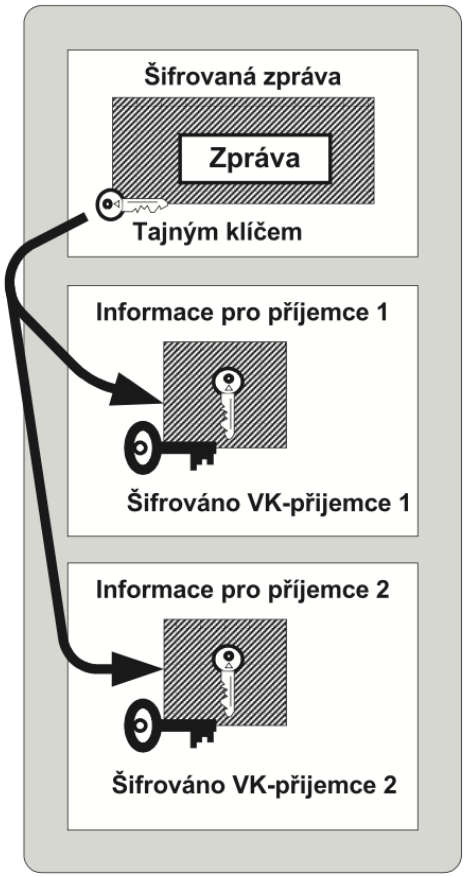


Obrázek 2: Asymetrická šifra *(3)*

3.1.4 Elektronická obálka

Šifrování je vždy operací, do které vstupují data, která mají být zašifrována a šifrovací klíče. V případě použití asymetrické kryptografie, ve které se používají výpočetně

náročné matematické procesy, je doba výpočtů velmi dlouhá. Řešením tohoto problému je elektronická obálka. Odesílatel zašifruje zprávu náhodným tajným (symetrickým) klíčem, což je rychlá operace. Ke zprávám zašifrovaným tímto způsobem jednoduše přidá „informace pro příjemce“ (Recipient info), který obsahuje náhodný klíč zašifrovaný veřejným klíčem příjemce. Asymetricky je tedy šifrován pouze kraťoučký tajný klíč. Výsledek je rychlý a efektivní. Má to ještě jednu výhodu. Pokud zprávu posíláme více adresátům, šifrujeme ji pouze jednou, a to náhodným tajným klíčem a každému adresátovi ke zprávě přibalíme tajný klíč šifrovaný jeho veřejným klíčem. (3)



Obrázek 3: Elektronická obálka *(3)*

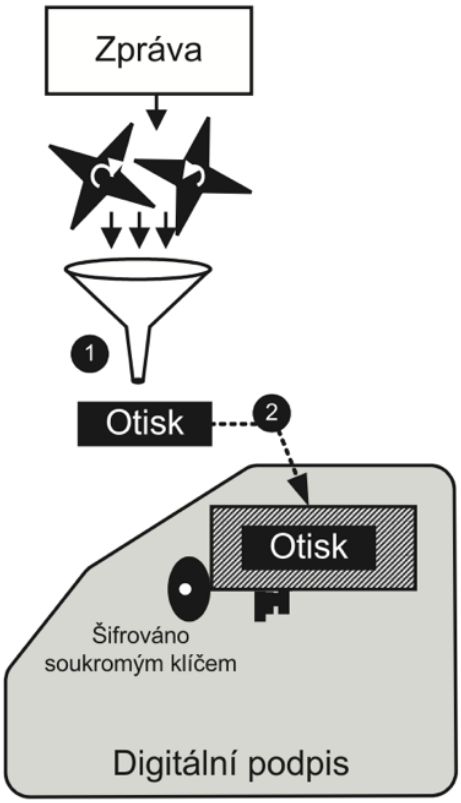
3.1.5 Digitální podpis

Digitální podpis je mechanismus, který slouží k doložení nepopiratelnosti dat (pravosti dokumentů). Digitální podpis hraje klíčovou roli v ověřování pravosti a nepopiratelnosti dokumentů a dat. Jeho základem je vlastnictví soukromého klíče, který je třeba chránit pečlivě, podobně jako důležité identifikační dokumenty. Ztráta soukromého

klíče by mohla mít vážné následky, podobně jako záměna fotky na občanském průkazu nebo otisků prstů v kriminální evidenci. Nedbalost v ochraně soukromého klíče může být srovnávána s podepsáním nevyplněného šeku. Je důležité poznamenat, že digitální podpis využívá klíč odesílatele (tj. osoby, která vytváří podpis) a ne klíč příjemce, jak je tomu u šifrování. Můžeme si představit proces digitálního podpisu tak, že nejprve "dešifrujeme" zprávu soukromým klíčem a poté "zašifrujeme" výsledek veřejným klíčem. Tímto způsobem jsou operace šifrování a dešifrování vzájemně zaměnitelné. RSA algoritmus je jedním z těch, které tento proces umožňují a je používán k vytváření digitálních podpisů. (3)

Pro vytvoření digitálního podpisu se postupuje dvěma hlavními kroky (obrázek 4):

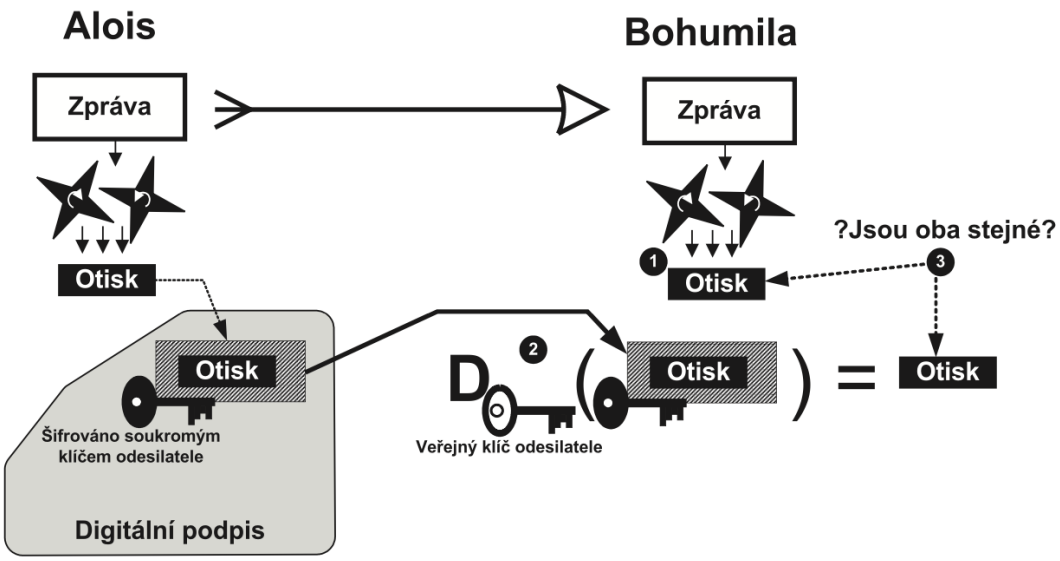
1. Prvním krokem je vytvoření otisku z dokumentu. To je speciální výpočet, který reprezentuje obsah dokumentu.
2. Poté se tento otisk šifruje pomocí soukromého klíče uživatele, který vytváří digitální podpis. Tím vznikne digitální podpis zprávy, což je šifrovaný otisk dokumentu. (3)



Obrázek 4: Digitální podpis *(3)*

Obrázek 5 ukazuje proces ověření digitálního podpisu, který se provádí v třech krocích:

1. Příjemce samostatně vytvoří otisk z přijaté zprávy, což je stejný proces, jaký byl použit při vytváření původního otisku dokumentu.
2. Příjemce následně dešifruje přijatý digitální podpis pomocí veřejného klíče odesilatele.
3. Nakonec příjemce porovná výsledek z prvního kroku s výsledkem z druhého kroku. Pokud jsou tyto výsledky totožné, potvrzuje to, že digitální podpis mohla vytvořit pouze osoba s přístupem ke soukromému klíči odesilatele, což znamená odesilatele samotného. Navíc tato shoda dokazuje, že zpráva nebyla během přenosu upravována, což zajišťuje integritu zprávy. (3)



Obrázek 5: Verifikace digitálního podpisu *(3)*

3.1.6 Kryptografie v České republice

V České republice funguje Národní bezpečnostní úřad (NBÚ), který má na starosti vývoj a výzkum v oblasti kryptografie a řídí bezpečnostní opatření pro uchovávání utajovaných informací. Pro zajištění bezpečnosti utajovaných dat v České republice byl přijat Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, konkrétně se jedná o Předpis č. 412/2005 Sb. Tento zákon upravuje certifikaci kryptografických technologií, které slouží k ochraně tajných informací, a to v souladu s jeho ustanoveními. (5)

Proces certifikace kryptografických prostředků a postupy pro zajištění kryptografické ochrany utajovaných informací jsou dále detailně specifikovány ve vyhlášce č. 432/2011 Sb., známé jako Vyhláška o zajištění kryptografické ochrany utajovaných

informací. Elektronický podpis, který má rovněž významný význam v ochraně dat, je upraven zákonem č. 227/2000 Sb. s názvem Zákon o elektronickém podpisu. Tento zákon se zabývá právním rámcem pro používání elektronického podpisu a jeho platnost v elektronických transakcích. (5)

3.1.7 Šifrovací algoritmy

DES

Data Encryption Standard (DES) je typický představitel symetrického šifrovacího algoritmu. Vznikl v roce 1975 na popud americké vlády, která usilovala o vytvoření jednoduchého, spolehlivého, uživatelsky přívětivého a standardizovaného nástroje pro šifrování dat, který by mohl být využíván státními institucemi i komerčními organizacemi. Bezpečnost DES byla podrobně zkoumána různými metodami kryptoanalýzy, přičemž úspěšnou se nakonec ukázala být diferenciální kryptoanalýza. Nicméně její praktické využití vyžaduje značné finanční a výpočetní prostředky. DES je tudíž poměrně snadno rozluštitelný pro velké podniky a organizace, a proto se pro klíčové sektory jako bankovnictví nehodí. Jeho vhodnost závisí na konkrétním použití, a pro osobní využití může být stále přijatelný. DES zůstává součástí mnoha softwarových systémů, od Kerbera až po různé implementace UNIXu, které ho využívají především pro šifrování hesel. (6)

IDEA

V roce 1990 vznikl šifrovací algoritmus IDEA, který se řadí mezi nejlepší symetrické algoritmy, využívané v otevřeném prostředí. Klíče používané u tohoto algoritmu mají délku 128 bitů, což znamená, že jsou odolnější proti odhalení než klíče v rámci DESu. Zatím neexistuje žádná známá kryptoanalytická metoda, která by dokázala efektivně narušit bezpečnost algoritmu IDEA. Přestože jde o relativně nový algoritmus, opírá se o pevné teoretické základy, což přispívá k jeho věrohodnosti a spolehlivosti. (6)

RSA

Algoritmus RSA představuje jeden z nejpopulárnějších a nejrozšířenějších algoritmů pro šifrování veřejným klíčem. Jeho bezpečnostní základ spočívá v obtížnosti nalezení rozkladu čísla na prvočinitele. I když tuto teorii nikdo neprokázal, ačkoli je velmi nepravděpodobné, že by byla prolomena, výzkumníci stále hledají nové způsoby, jak by

teoreticky mohla být bezpečnost algoritmu ohrožena. Zvláště hledání prvočísel, která jsou základem RSA, se stále zdokonaluje a vyžaduje delší klíče pro zachování dostatečné bezpečnosti. RSA je považováno za standard pro systémy s veřejným klíčem a nachází uplatnění zejména při distribuci sdílených symetrických klíčů a pro digitální podpisy. Nicméně pro běžné šifrování dat, například při přenosu dat po síti, se RSA příliš nehodí. Má své omezení, včetně pomalého zpracování a náročnosti generování klíčů, zvláště kvůli požadované velikosti prvočísel. Pro tyto účely existují rychlejší a efektivnější algoritmy. (6)

3.2 Digitální certifikáty

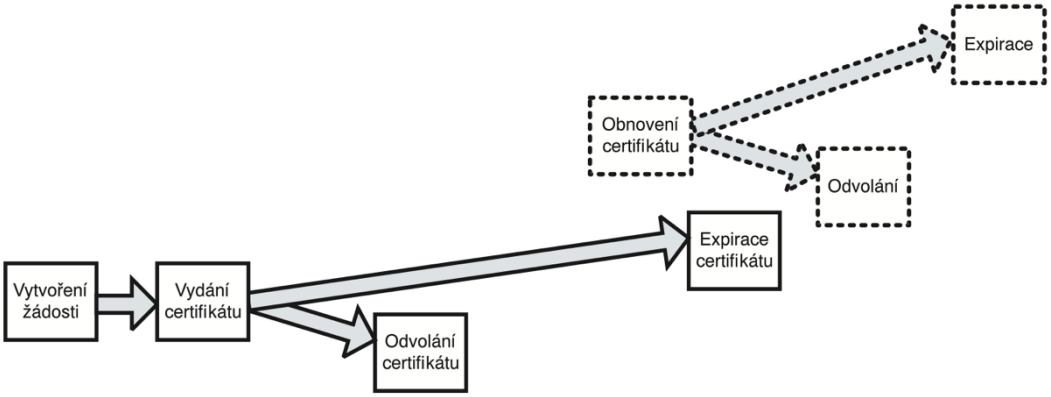
Certifikát nebo digitální certifikát je jedinečný, digitálně podepsaný dokument, který jednoznačně identifikuje totožnost jednotlivce nebo organizace. Pomocí asymetrické kryptografie lze ověřit jeho pravost, aby se zajistilo, že používaný software nebo webová stránka je legitimní. Na internetu je certifikát podepsán důvěryhodnou certifikační autoritou a ověřen pomocí veřejného klíče této autority. Dešifrovaný certifikát obsahuje ověřený veřejný klíč držitele certifikátu, s nímž lze navázat šifrovanou komunikaci přes HTTPS. Certifikáty využívané na internetu vycházı́ z normy X.509 verze 3, která nám definuje strukturu certifikátů. (7)

3.2.1 Životní cyklus certifikátu

V průběhu času prochází certifikát několika fázemi tvořícími životní cyklus certifikátu. Životní cyklus certifikátu se skládá z následujících fází:

1. Vytvoření žádosti o certifikát – žádost o vytvoření může, ale nemusí předcházet vygenerování párovacích dat (párovací data může vygenerovat i certifikační autorita po obdržení žádosti o certifikát).
2. Vydání certifikátu a jeho případné zveřejnění.
3. Platnost certifikátu – po vydání nemusí být certifikát automaticky platný. Certifikát je platný od doby uvedené v položce "Od" do vypršení platnosti certifikátu nebo do odvolání certifikátu.
4. Platnost certifikátu (vypršení platnosti certifikátu) nastane po uplynutí doby „Do“ uvedené v certifikátu.
5. Certifikační autorita obvykle anuluje certifikát před datem vypršení jeho platnosti zveřejněním jeho identifikace na seznamu odvolaných certifikátů (CRL), a tím jej zneplatní.

Toto odvolání je zaznamenáno na všech CRL pro původně deklarovanou dobu platnosti certifikátu. Certifikační autorita odvolává certifikát v případě, že jiný uživatel požádal o certifikaci již certifikovaného veřejného klíče, nebo certifikační autorita zjistila, že údaje v certifikátu již nejsou pravdivé, nebo v případě, že o něj držitel certifikátu zažádá. (3)



Obrázek 6: Životní cyklus certifikátu *(3)*

3.2.2 Druhy certifikátů

Certifikáty dělíme na několik druhů, zejména na komerční a kvalifikované. Komerční certifikáty hrají důležitou roli, zejména tam, kde kvůli platné legislativě není možné použít certifikáty s kvalifikací. Jsou ideální pro obchodní transakce mimo komunikaci s veřejnými orgány, kde je vyžadováno použití kvalifikovaných certifikátů. Tyto certifikáty jsou často využívány ve vzájemné komunikaci mezi komerčními subjekty k šifrování a ověření identity. Typicky jde o neanonymní přístup na webové servery a zabezpečený přenos dat, jak e-mailem, tak prostřednictvím webových formulářů. Platnost komerčních certifikátů je stanovena na jeden rok. (8)

Kvalifikované certifikáty jsou navrženy pro interakci občanů s veřejnými institucemi, avšak mohou být také využity pro komerční účely. Tyto certifikáty mohou být použity pro vytváření a ověření elektronických podpisů, ale jsou omezeny v jiných aspektech, jako je šifrování komunikace, což je regulováno právními předpisy. Kvalifikované certifikáty pro ověření internetových stránek jsou určeny k poskytnutí nejvyššího stupně důvěryhodnosti webovým stránkám. Tímto způsobem zajišťují důvěryhodnost organizace na internetu pro potenciální návštěvníky a představují důležitý prvek bezpečnosti. Následně se certifikáty, také dělí podle toho, pro koho jsou vydávány. Fyzickým osobám jsou vydávány osobní certifikáty, zatímco certifikáty vydávané nejenom

fyzickým osobám, ale také osobám právnickým nebo například organizačním složkám státu se nazývají systémové certifikáty. (8)

3.2.3 Položky certifikátu

Každý digitální certifikát může být velmi odlišný. Nicméně většina certifikátů sdílí některé společné položky s konkrétními informacemi. (9)

- **Sériové číslo:** Sériové číslo je unikátní identifikátor certifikátu v systému certifikační autority. Nikdy nesmí být vydané stejné sériové číslo dvakrát.
- **Verze:** Verze certifikátu označuje, zda certifikát vychází z normy X.509 verze 1, 2 nebo 3. V případě verze 1 má pole verze hodnotu nula, ve verzi 2 má hodnotu jedna a ve verzi 3 má hodnotu dva. V současnosti se zásadně používají certifikáty verze 3.
- **Předmět:** Tato položka obvykle ukazuje, kdo vlastní certifikát. Může to být jednotlivec, organizace nebo konkrétní zařízení.
- **Vydavatel:** Tato řádka ukazuje na entitu (zejména certifikační autoritu) zodpovědnou za podepisování a ověřování informací v digitálním certifikátu.
- **Not Before:** Každý certifikát by měl mít jasně definované časové rámce platnosti. Řádka Not Before ukáže, od kdy je certifikát považován za platný.
- **Not After:** Toto pole obsahuje datum a čas, kdy certifikát vyprší.
- **Použití klíče:** Každý certifikát potřebuje toto pole, protože jasně definuje přijaté kryptografické použití veřejného klíče.
- **Rozšířené použití klíče (pokud je nutné):** Certifikát může být použit v několika aplikacích. V takovém případě se objeví pole rozšířeného použití klíče, které ukazuje na další použití, jako je ověřování TLS serveru, podepisování kódu atd.
- **Veřejný klíč:** Toto je pole, kde je uveden veřejný klíč, který vlastní majitel certifikátu.
- **Algoritmus podpisu:** Pole algoritmu podpisu ukazuje jak šifrovací, tak hashovací algoritmy použité k šifrování nebo hašování daného certifikátu.
- **Podpis:** Toto je jedno z nejdůležitějších polí, tzv. „tělo“ certifikátu. Obsahuje podpis, který je nejprve zahašován a poté šifrován pomocí algoritmů uvedených v poli „Algoritmus podpisu". (9)

3.3 Serverové certifikáty

Serverové certifikáty hrají klíčovou roli v zajištění identity a bezpečnosti webových stránek, které využívají šifrovací mechanismy při komunikaci s počítači uživatelů. To je zejména důležité v případech, jako je internetové bankovnictví. Šifrování dat, které se přenáší mezi webovým prohlížečem uživatele a webovým serverem stránek, využívá speciální klíče. Tyto klíče jsou informace, které určují, jaká data budou zakódována na straně odesílatele (například při odesílání přihlašovacích údajů nebo informací o platební kartě) a jak budou dekódována na straně serveru při provádění operací (například při ověřování uživatele nebo při zpracování platebních příkazů). Pro zvýšení bezpečnosti se často používají asymetrické šifry, které pracují s veřejným klíčem na straně odesílatele (uživatele) a privátním klíčem na straně příjemce (provozovatele stránek). (10)

Certifikát potom funguje jako způsob, jakým uživateli dokazujete, že stránky, které šifrují svou komunikaci, jsou skutečně ty, za které se vydávají. Tímto způsobem šifrování zajišťuje soukromí, a certifikát poskytuje jistotu, že vaše důvěrné informace nejsou odesílány podvodníkům. Aby bylo možné říci, že stránky mají certifikát, musí majitel stránek podepsat veřejnou část svého klíče elektronickým podpisem. Tento podpis je soubor dat, který slouží k potvrzení identity majitele klíče. To je základní proces certifikace. Pokud majitel stránek podstoupí náročnější ověření, certifikát může sloužit nejen jako nástroj ověření, ale také k jednoznačné identifikaci majitele stránek. (10)

Z pohledu uživatele je klíčové, že navštívená stránka je šifrována, což se projeví v adresním řádku prohlížeče, kde se objeví „https" a pak až název stránky (a někdy ikonka zámku před adresou). Důležité je také zajistit, že použitý certifikát pro ověření stránek je platný. Pokud není, uživatel obdrží upozornění prohlížeče, že „certifikát nelze ověřit". V takovém případě je moudré být opatrný, zvláště pokud jsou stránky náročné na odesílání citlivých informací. (10)

3.3.1 Druhy serverových certifikátů

Standardní SSL certifikáty

SSL certifikáty, které označujeme jako „standardní," jsou nejběžnějším druhem SSL certifikátů dostupných na trhu. Tyto certifikáty jsou určeny k zabezpečení jedné konkrétní domény na internetu, jako například „www.ssls.cz" nebo „klient.ssls.cz." Je zajímavé, že

některé standardní SSL certifikáty jsou dokonce zdarma a dokážou zajistit jak doménu s předponou „www," tak i bez této předpony. Tím pádem můžete chránit svou webovou stránku bez ohledu na to, zda ji návštěvníci navštěvují s či bez „www" předpony. (11)

Hvězdičkové certifikáty

Hvězdičkový certifikát, známý také jako WildCard certifikát, se používá pro zabezpečení subdomén. Pokrývá subdomény 3. řádu na hlavní doméně, což znamená, že může chránit domény jako domena1.domenaxyz.cz. Jedním z hlavních benefitů WildCard certifikátu je možnost zabezpečit více subdomén 3. řádu pomocí jediného certifikátu, což uživatele osvobozuje od potřeby zakoupit samostatný certifikát pro každou z nich. Dále je možné použít WildCard certifikát pro zabezpečení domén 4. řádu. (11)

Tato forma certifikátu je velmi oblíbená, protože na internetu jsou subdomény běžně využívány. Firmy ho často využívají pro zabezpečení subdomén s názvy jako admin, mail, intranet nebo test. Další výhodou WildCard certifikátu je, že po jeho nasazení neexistují žádná omezení ohledně toho, kolik subdomén může být zabezpečeno. Administrátor může přidat libovolný počet subdomén na server, a všechny budou zabezpečeny. Hvězdičkový certifikát dostává své jméno od hvězdičky, která se přidává k názvu domény, například *. domenaxyz.cz. Tímto způsobem certifikát označuje, že vše, co zde nahradí hvězdičku, je zabezpečené a platné. Podobně jako u certifikátu pro jednu doménu lze s WildCard certifikátem zabezpečit i samotnou hlavní doménu, jako například domenaxyz.cz. Toto pravidlo však platí pouze pro domény 2. řádu. (11)

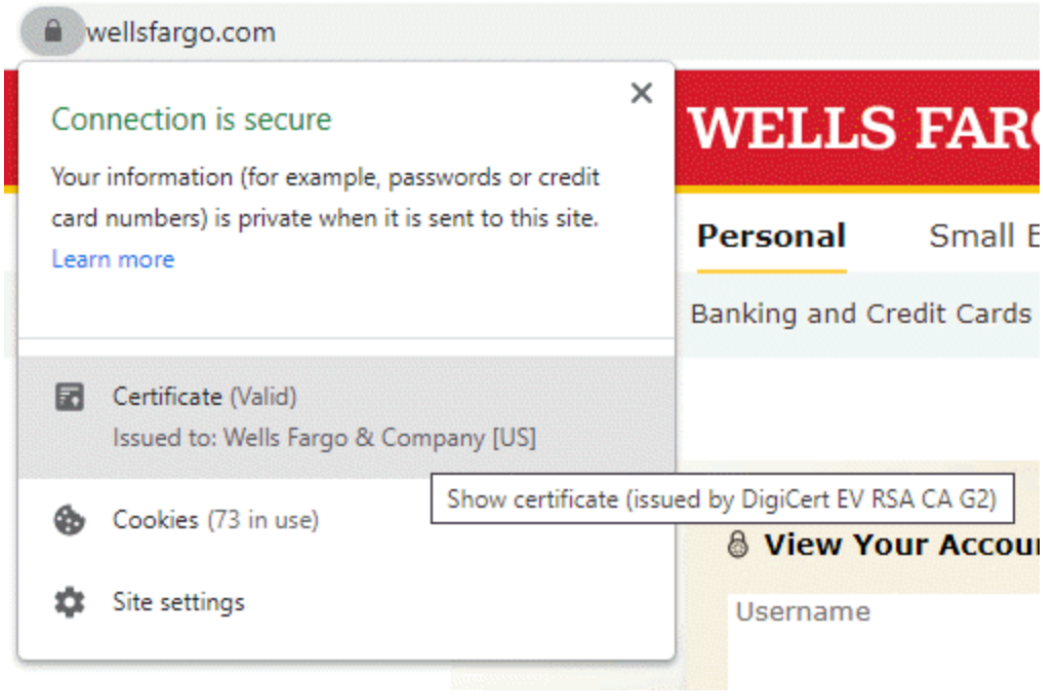
Multidoménové SSl certifikáty

Multidoménový SSL certifikát je certifikát, který pokrývá více domén na jedné IP adrese. Pokud jde o sílu šifrování, SAN (Subject Alternative Name) nebo UCC (Unified Communications Certificate) multidoménový certifikát používá stejné šifrovací standardy jako ostatní řešení nabízená jakoukoliv důvěryhodnou certifikační autoritou. Rozdíl spočívá v rozšíření SAN, které slouží k určení dalších domén. Základní doména je uvedena jako „common name“. Podporuje ji 99,9 % všech webových prohlížečů a je k dispozici pro každou úroveň ověření. SAN SSL certifikáty mohou zabezpečit až 250 domén, subdomén nebo externích IP adres na jednom certifikátu. (12)

EV certifikáty

EV certifikát je nejvyšší úrovní SSL certifikátů. Poskytuje nejvyšší úroveň digitálního ověření identity tím, že ověřuje právní identitu majitele webové stránky. Potvrzení identity webové stránky se provádí podle přísných směrnic CAB Forum a zahrnuje přísný proces ověřování veřejnou certifikační autoritou. Certifikační autorita musí ověřit provozní a fyzickou identitu osoby, která žádá o EV certifikát. To se provádí potvrzením právní identity majitele webu a toho, že žadatel je vlastníkem a jediným kontrolorem domény. Kvůli náročnému procesu ověřování identity majitele webu poskytuje EV certifikát vysokou míru důvěry pro návštěvníky webové stránky. (13)

Před podzimem 2019 mohl návštěvník webové stránky ověřené pomocí EV certifikátu tuto stránku rozeznat buď podle názvu webu zbarveného do zeleného textu, nebo na zeleném pruhu, který zobrazoval právní název a geografické umístění společnosti vlastnící certifikát. Nicméně od té doby Mozilla Firefox a Google Chrome tuto indikaci odstranily. Všechny SSL certifikáty nyní zobrazují šedý zámek v adresním řádku prohlížeče. Pokud chce uživatel zjistit, zda webová stránka používá EV certifikát, může kliknout na šedý zámek vedle adresního řádku. (13)



Obrázek 7: Kontrola, jestli se jedná o EV certifikát *(13)*

3.3.2 Self-signed certifikáty

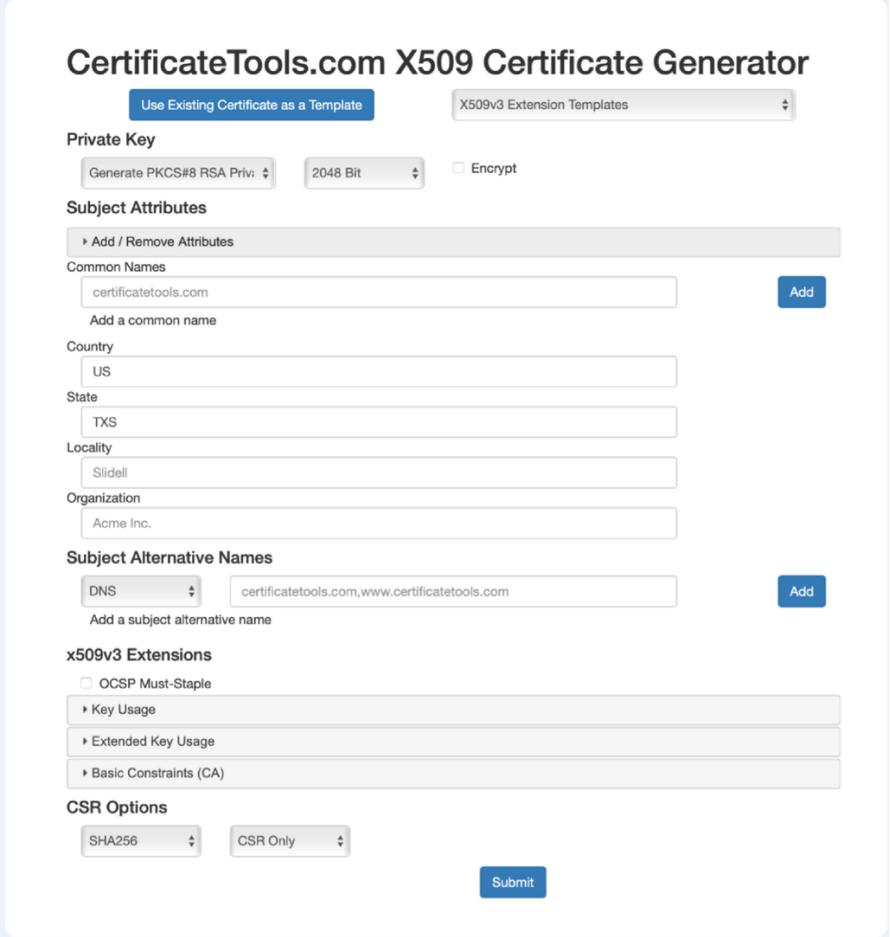
Na rozdíl od standardních SSL certifikátů jsou self-signed certifikáty podepsány subjektem žádající o certifikát, namísto certifikační autority. Z toho vyplývá, že si je může podepsat jakýkoliv uživatel, vývojář nebo majitel webových stránek a žádná třetí strana takové podepsání neověřuje. Základní šifrovací technologie self-signed certifikátů je ovšem bezpečná a téměř nemožná k dešifrování hackery. Jejich zranitelnost tak spočívá v nedostatku nezávislého ověření. (14)

Self-signed certifikáty jsou zdarma, ale obvykle se používají pouze pro interní testování nebo ve starších prostředích kde jsou potřeba certifikáty s určitou délkou (často již nedostačující pro moderní zabezpečení serverů). V dnešní době by se self-signed certifikáty na webových stránkách dostupných veřejnosti již neměli používat. Jejich použití se dá přirovnat k použití certifikátů s vypršelou platností. (15)

Většina prohlížečů upozorní uživatele, že takový certifikát nelze ověřit, a téměř okamžitě odradí většinu návštěvníků. Self-signed certifikát je svou povahou také snáze padělatelný než certifikát vydaný certifikační autoritou. Většina profesionálních veřejných domén by se měla vyvarovat těmto negativním konotacím a raději zakoupit standardní SSL certifikát od důvěryhodné CA. Protože jsou zdarma, self-signed SSL certifikáty jsou častěji používány na interních testovacích webech, kde společnost může zaměstnance informovat, aby ignorovali varování prohlížeče. Nicméně to stále představuje určitá rizika, protože taková firemní politika může podporovat nebezpečné návyky při veřejném prohlížení, což může následně ovlivnit i běžné prohlížení webu. (16)

3.3.3 Postup pro získání self-signed certifikátu

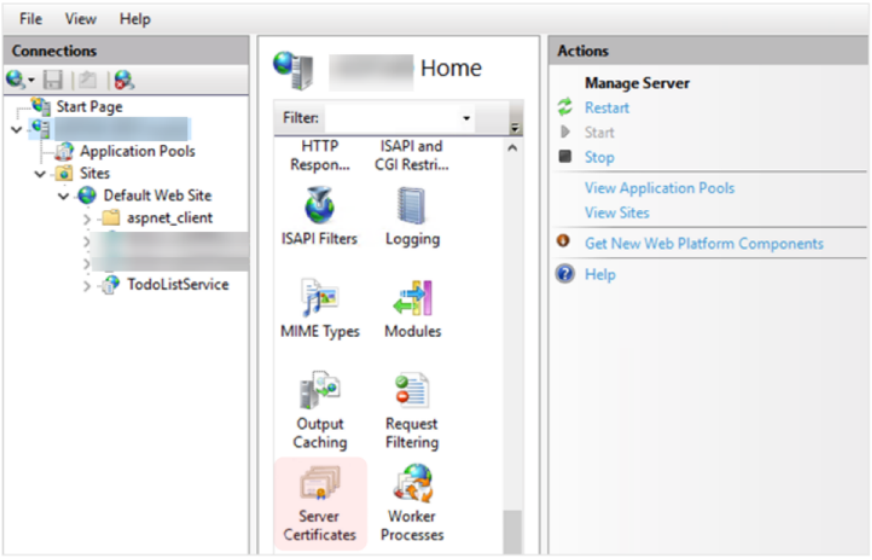
Existuje mnoho metod, jakými se dá získat self-signed certifikát, mezi nejjednodušší metodu patří různé webové stránky, na kterých si během pár minut lze vlastní self-signed certifikát vytvořit. (17)



Obrázek 8: Příklad vytvoření certifikátu přes web *(17)*

Další metodou, jak můžeme získat self-signed certifikát, je ho vygenerovat pomocí IIS Serveru, budeme postupovat následovně:

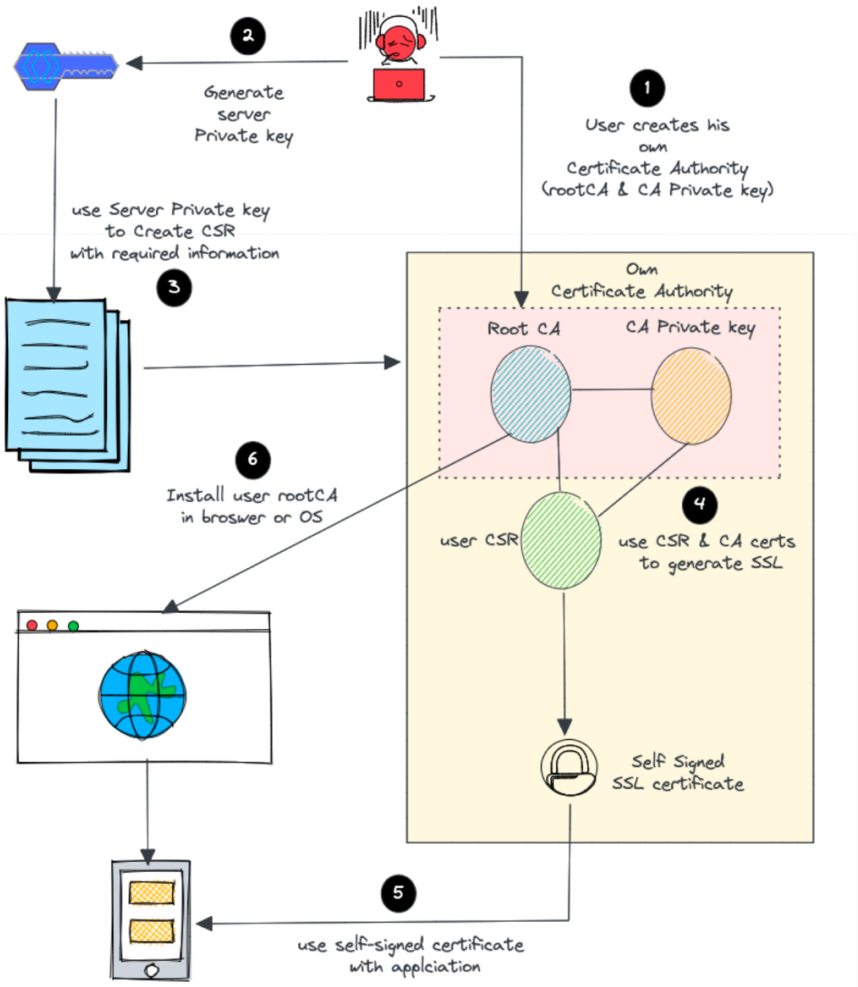
1. V horní části IIS Manageru vybereme „Serverové certifikáty";
2. Poté klikneme na pravé straně na tlačítko „Vytvořit";
3. Tím vytvoříme self-signed certifikát platný po dobu jednoho roku s privátním klíčem. Tento certifikát bude fungovat pouze pro „localhost.“ (17)



Obrázek 9: Generování certifikátu v IIS Manager *(17)*

V neposlední řádě, můžeme vytvořit self-signed certifikát za pomocí různých nástrojů a aplikací, například můžeme využít nástroj OpenSSl, tímto nástrojem vytvoříme certifikát následovně:

1. Vytvoříme si vlastní kořenový certifikát CA a privátní klíč CA (Sami jednáme jako CA).
2. Vytvoříme privátní klíč serveru pro generování žádosti o vydání certifikátu (CSR).
3. Vytvoříme SSL certifikát s CSR pomocí našeho kořenového CA a privátního klíče CA.
4. Nainstalujeme certifikát do prohlížeče nebo operačního systému, abychom zabránili bezpečnostním upozorněním. (18)



Obrázek 10: Postup vytváření certifikátu přes nástroj OpenSSL *(18)*

3.4 Certifikační autority

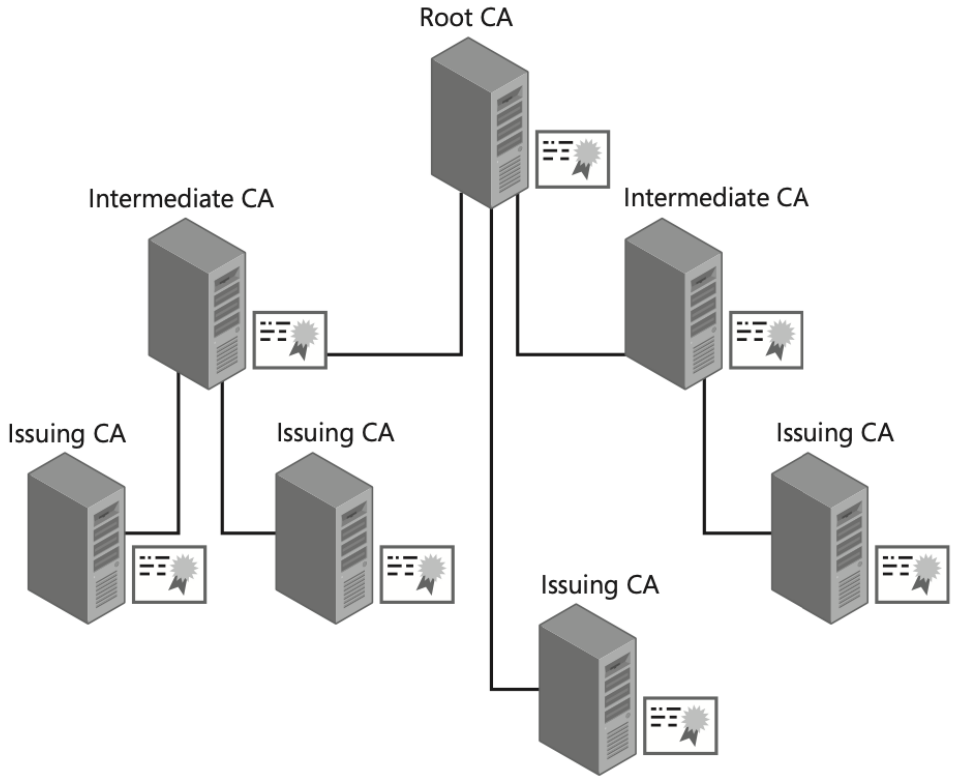
Certifikační autority (CA) jsou společnosti, které vydávají digitální certifikáty třetím stranám. Tyto certifikáty slouží k ověření totožnosti subjektů, jako jsou webové stránky, e-mailové adresy, firmy nebo živnostníci, a k jejich spojení s kryptografickými klíči prostřednictvím digitálních certifikátů. Certifikační autority mají klíčovou roli v ověřování webových stránek a jejich vlastníků, a to v závislosti na typu certifikátu. Poté mohou vydávat důvěryhodné certifikáty TLS pro největší světové prohlížeče, jako je Chrome, Safari a Firefox. Tím pomáhají zabezpečit internet tím, že zajišťují, že webové stránky a jejich provozovatelé jsou důvěryhodní, což vytváří důvěru při online komunikaci a transakcích. (19)

Podvodníci se snaží vytvořit falešné webové stránky s certifikáty, které napodobují originální. Je důležité, aby uživatelé byli schopni rozpoznat základní znaky, které naznačují důvěryhodnost webu, a pečlivě ověřovali jeho bezpečnost. Pokud navštívíte web s protokolem HTTPS a uvidíte malý zámek v adresním řádku, můžete si být jisti, že jste na zabezpečeném webu ověřeném certifikační autoritou. Naopak, pokud vidíte zprávu „Nezabezpečeno" a ikonu s vykřičníkem, web nepoužívá šifrování a nebyl ověřen certifikační autoritou. Každá webová stránka, která chce používat HTTPS a mít zámkovou ikonu v adresním řádku, musí získat platný certifikát TLS od některé certifikační autority. To zahrnuje předložení informací o vlastnictví webu, názvu firmy a jejím umístění CA, která musí dodržovat přísné standardy a stejné podmínky pro schválení všech žadatelů. (19)

3.4.1 Hierarchie certifikačních autorit

V podnikovém prostředí se obvykle používá více než jedna certifikační autorita. Tyto CA jsou strukturovány do hierarchie CA, která se skládá z jednoho centrálního kořenového CA a několika dalších podřízených CA, jak je naznačeno na obrázku 8. V této hierarchii jsou CA organizovány do systému kořenové CA. Tato hierarchická struktura přináší zvýšenou bezpečnost a rozšiřitelnost, jelikož umožňuje, aby ty CA, které nevydávají certifikáty, nebyly připojeny k síti. Tím jsou offline CA chráněny před potenciálními útoky pocházejícími ze sítě. (20)

Hierarchie kořenové CA umožňuje delegaci správy různým obchodním jednotkám nebo oddělením uvnitř organizace. Tím, že lze rozlišit role správy u každé CA v hierarchii, dává možnost různým skupinám administrátorů spravovat jednotlivé CA v této hierarchii, aniž by měli kontrolu nad ostatními CA. (20)



Obrázek 11: Hierarchie certifikačních autorit *(20)*

3.5 Protokoly SSL/TLS

SSL (Secure Sockets Layer) a jeho nástupce TLS (Transport Layer Security) jsou protokoly pro vytváření ověřených a šifrovaných spojení mezi počítači v síti. Ačkoli byl protokol SSL po vydání TLS 1.0 v roce 1999 označen za zastaralý, stále je běžné používat termíny „SSL" nebo „SSL/TLS" k označení těchto souvisejících technologií. (21)

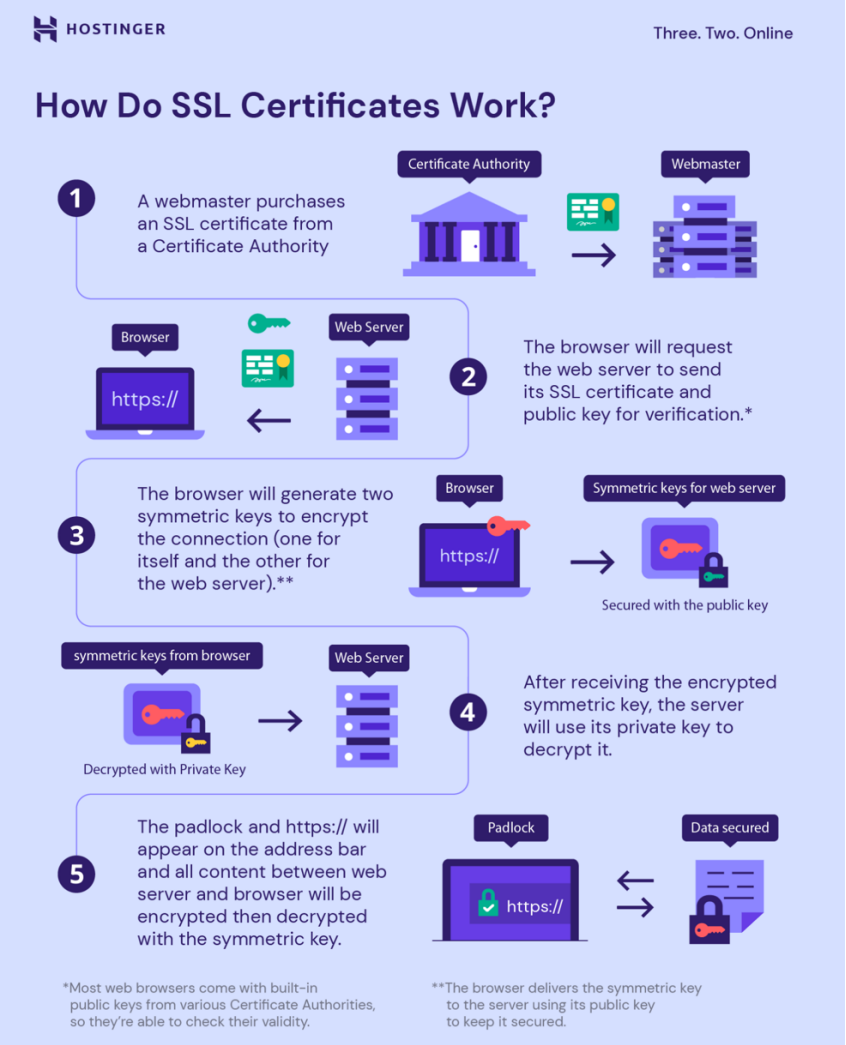
3.5.1 Protokol SSL

SSL je digitální bezpečnostní prvek, který umožňuje šifrované spojení mezi webovou stránkou a prohlížečem. SSL si klade za cíl poskytnout bezpečný způsob přenosu citlivých dat, včetně osobních informací, údajů o platební kartě a přihlašovacích údajů. Protokol SSL může být použit pouze webovými stránkami s SSL certifikátem. SSL certifikáty chrání přenos dat pomocí asymetrických a symetrických šifrovacích technik. Nejprve vlastník webové stránky zakoupí SSL certifikát od certifikační autority a nainstaluje ho na své stránky. Když návštěvník prochází webovou stránkou, prohlížeč a webový server navážou

SSL spojení pomocí tzv. metody SSL handshake. Během SSL handshake prohlížeč požádá server o jeho SSL certifikát a veřejný klíč k ověření jeho platnosti. (22)

Jakmile je certifikát ověřen, prohlížeč a webový server vymění privátní a veřejné klíče k vytvoření symetrického klíče. Obě strany poté použijí tento symetrický klíč k šifrování veškeré komunikace. Tento klíč zůstane platný po omezený čas a pouze pro danou relaci. Jakmile je SSL protokol aktivován, bude webová stránka bezpečná a šifrovaná. Neoprávněné třetí strany již nebudou schopny zachytit danou komunikaci. URL adresy jsou buď předcházeny protokolem HTTP (Hypertext Transfer Protocol) nebo HTTPS (Hypertext Transfer Protocol Secure). Tyto protokoly v podstatě určují, jak jsou přenášena data, která odesíláme a přijímáme. (22)

Webové stránky, které nemají SSL certifikát, běží na HTTP a přenášejí data v otevřeném textovém formátu, což znamená, že kdokoli na internetu může zachytit a přečíst obsah zprávy. To může představovat problém, pokud přenášená data obsahují důvěrné informace, které útočníci mohou zneužít k provádění kybernetických zločinů. Když se nastavuje SSL certifikát, konfiguruje se tak, aby přenášel data šifrovaně pomocí protokolu HTTPS. Tyto dvě technologie jdou ruku v ruce – nemůžeme používat jednu bez druhé. (22)



Obrázek 12: Jak funguje SSL certifikát *(22)*

3.5.2 Protokol TLS

TLS je pouze novější verzí protokolu SLL. Před zahájením TLS byla finální verzí SSL verze 3.0. Oba bezpečnostní protokoly fungují podobně, jelikož používají kryptografické klíče v různých aplikačních protokolech jako jsou HTTP, FTP, IMAP a SMTP. Nicméně TLS spojení nabízí odlišný proces tzv. handshake, silnější šifrovací algoritmy a bezpečnější šifrovací sady. V důsledku toho má TLS certifikát lepší zabezpečení dat a ověřování než SSL. (23)

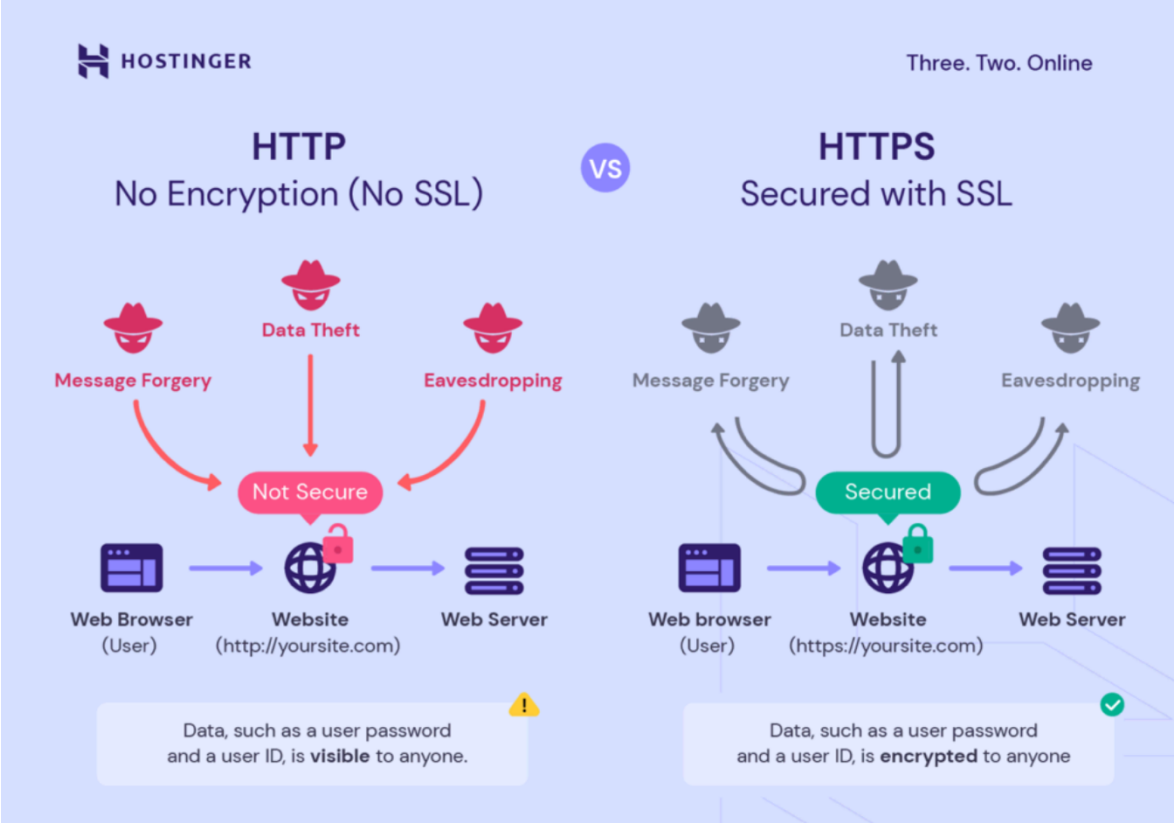
Například při ověřování zpráv používá TLS silnější autentizační kód – HMAC, zatímco SSL používá pouze standardní kód pro ověřování zpráv – MAC. Nicméně oba pojmy jsou často zaměňovány, protože první verze TLS byla vydána jako upgrade SSL 3.0. Proto mnoho lidí používá termín TLS/SSL k odkazování na tento protokol. Pokud používáte

webovou stránku s TLS, měla by být vedle adresního řádku URL viditelná ikona zámečku, což signalizuje, že spojení je zabezpečené. Kliknutím na ni můžete zobrazit podrobnosti, jako jsou informace o jejím TLS/SSL certifikátu. (23)

3.5.3 Protokol HTTPS

HTTPS (Hypertext Transfer Protocol Secure) je zabezpečená verze protokolu HTTP (Hypertext Transfer Protocol). HTTP je protokol používaný k přenosu dat po webu prostřednictvím modelu klient-server (webový prohlížeč – webový server). HTTPS šifruje všechna data, která procházejí mezi prohlížečem a serverem pomocí protokolu SSL/TLS. Tato šifrování dat činí data nerozluštitelnými, dokud je majitel stránky neodemkne, což umožňuje uživatelům sdílet citlivá data, jako jsou hesla a další osobní informace, bezpečně přes internet nebo síť. (24)

HTTPS může zahájit šifrované a bezpečné spojení pouze po zřízení důvěry mezi prohlížečem a serverem. Důležitost této důvěry je zdůrazněna následným zavedením HTTP Strict Transport Security (HSTS), mechanismu webové bezpečnosti, který umožňuje přístup k webovým stránkám pouze prostřednictvím zabezpečených spojení. HTTPS a HTTP jsou stejným protokolem. Hlavní rozdíl spočívá v tom, že protokol HTTPS má dodatečnou vrstvu šifrování (SSL/TLS). Webové stránky s protokolem HTTP se stávají stránkami s protokolem HTTPS získáním SSL certifikátu. Aby se doména mohla stát s protokolem HTTPS, musí obdržet SSL certifikát od důvěryhodné certifikační autority. (24)



Obrázek 13: Rozdíl mezi HTTP a HTTPS *(22)*

Když se webový prohlížeč pokusí připojit k serveru přes HTTPS, ověřuje, že SSL certifikát odpovídá doménovému jménu, které uživatel pokouší zadat, a to pomocí procesu nazývaného SSL/TLS handshake. Certifikát obsahuje digitální podpis od certifikační autority, aby se ověřilo, že certifikát byl vydán pro určené doménové jméno. Jakmile webový prohlížeč ověří podpis certifikátu k navázání důvěry se serverem, spojení se stává zabezpečeným. Všechny důvěryhodné certifikační autority jsou automaticky rozpoznány webovými prohlížeči. Naopak, HTTP spojení nejsou bezpečná, zejména pokud jsou prováděna přes veřejné Wi-Fi sítě. Kdokoli může snadno zachytit komunikaci na síti pomocí volně dostupného softwaru. Protože HTTP nepoužívá SSL certifikáty, jsou všechny informace, které webový prohlížeč přenáší na webový server, dostupné v otevřeném textu. HTTP také nemůže ověřit autentičnost vlastníka domény, protože nemá proces ověření. Nejprve autor porovná důvěryhodnost serverových certifikátů podepsaných důvěryhodnou certifikační autoritou se self-signed certifikáty za pomocí komparativní analýzy a vypracuje analýzu bezpečnosti. (24)

4 Praktická část

Autor na základě získaných informací z analýzy certifikačních politik a webových stránek provede vyhodnocení výsledků pro porovnání self-signed certifikátu s certifikátem podepsaným důvěryhodnou CA z hlediska bezpečnosti a následně pro porovnání vybraných CA s ohledem na ekonomické faktory.

Provedená analýza bude systematicky zaznamenána v tabulkách, a následné srovnání výsledků bude prezentováno pomocí grafů. K dosažení finálního hodnocení budou kritéria porovnávána Saatyho metodou a bodovací metodou. Po sečtení výsledků nám nejvyšší součet ukáže, který certifikát a CA vyniká jako nejlepší.

Nejprve se určí certifikáty a certifikační autority k porovnání a jejich kritéria. Poté se za pomocí Saatyho metody a bodovací metody určí váhy všech kritérií a vypočítá se nejlepší varianta pro první porovnání self-signed certifikátu s certifikátem podepsaným důvěryhodnou CA a následně pro druhé porovnání vybraných CA.

4.1 Výběr kritérií a variant pro první porovnání

4.1.1 Cenová dostupnost

Poměrně důležitý ukazatel pro mnoho uživatelů, avšak nemá přímý vliv na bezpečnost. Jeden z hlavních důvodu, proč by se uživatel rozhodl využít právě self-signed certifikát. Nejlépe ohodnocený certifikát je ten nejlevnější na pořízení.

4.1.2 Vizuální indikátor důvěryhodnosti certifikátu

Kritérium zahrnuje přítomnost vizuálních indikátorů poskytovaných webovými prohlížeči. Konkrétně se bude sledovat, zda SSL/TLS certifikát získal důvěru webového prohlížeče a zda je vizuálně označen, například symbolem zámku před doménovým jménem v adresním řádku webového prohlížeče. Pokud uživatelé zámek nevidí, mohou stránce nedůvěřovat a mohou být varováni webovými prohlížeči před nedůvěryhodným webem. Certifikáty, které správně zobrazují vizuální indikátory důvěryhodnosti, budou považovány za úspěšné v tomto kritériu.

4.1.3 Dodržování pravidel CA/B Fóra

Toto kritérium se zaměřuje na následování pravidel a směrnic, které jsou specifikovány CA/B Fórem. V rámci veřejné infrastruktury klíčů (PKI) mohou certifikační autority získat a udržet důvěru prohlížečů pouze v případě, že jsou členy CA/B Fóra a striktně respektují všechny ustanovené směrnice. Pokud CA poruší jakoukoliv směrnici, i v případě jediného certifikátu, prohlížeče mají oprávnění odebrat důvěru všem certifikátům, které tato CA vydala. Certifikáty, které se musí řídit touto směrnicí budou považovány za úspěšné v tomto ukazateli.

4.1.4 Doba platnosti

Na první pohled by se mohla zdát delší doba platnosti jako výhoda, ale čím delší má certifikát platnost, tím méně mu můžeme věřit. Jelikož s delší dobou platnosti certifikátu roste riziko prolomení klíče. Nejlépe ohodnocený certifikát v tomto kritériu je tedy ten s nejkratší dobou platnosti.

4.1.5 Zneplatnění certifikátu

Toto kritérium se zaměřuje na schopnost rychlé a efektivní revokace certifikátu v případě jeho zneužití nebo kompromitace privátních klíčů. Centralizované systémy revokace, jako jsou CRL nebo OCSP umožňují rychlou a efektivní revokaci certifikátů, což umožňuje rychle reagovat na potenciální bezpečnostní incidenty a chránit důvěryhodnost certifikátu. Čím efektivněji a rychleji lze zneplatnit certifikát, tím je toto kritérium lépe ohodnoceno.

4.1.6 Autentizace

Toto kritérium zajišťuje, že jsou certifikáty spojeny s legitimními subjekty. To snižuje riziko zneužití a podvrhnutí, protože CA ověřuje identitu certifikátu. Žádná externí kontrola jejich pravosti vytváří riziko zneužití, neboť mohou být snadno zneužity hackery. Tohle kritérium je úspěšné, pokud je certifikát autentizovaný.

4.1.7 Rychlost vystavení

Rychlost vystavení je kritérium, které určuje dobu, za kterou je certifikát vystaven. Toto kritérium nemá přímý vliv na bezpečnost, přesto by se při rozhodování nemělo opominout. Čím rychleji je možné certifikát vystavit, tím lépe je toto kritérium ohodnoceno.

4.1.8 Self-signed certifikát

Pro potřeby této analýzy jsem si vybral self-signed certifikát, který lze zdarma vygenerovat na stránce www.certificatetools.com. Tento certifikát je, co se délky klíče a dalších technických parametrů konkurenceschopný v porovnání s certifikáty od důvěryhodných certifikačních autorit.

4.1.9 Certifikát podepsaný důvěryhodnou CA

Pro tuto analýzu jsem si vybral komerční doménový certifikát od CA DigiCert. Zejména proto, že patří mezi jednu z využívanějších CA na trhu. Certifikát lze zakoupit na stránce www.digicert.com.

4.2 Výběr kritérií a variant pro druhé porovnání

4.2.1 Cenová dostupnost

Toto kritérium se zaměřuje na cenu služeb. Čím levnější certifikační autorita nabízí své služby, tím lépe je v tomto kritériu ohodnocena.

4.2.2 Délka klíče

Délka klíče má vliv na průběh šifrovacího algoritmu, což znamená transformaci zprávy do šifrované podoby a zpět. V současné době jsou standardně používány klíče o délce 2048 bitů, která je dostačující, některé certifikační autorita však již nabízí i klíče o délce 4096 bitů. Všechny porovnávané certifikáty nabízejí minimálně délku 2048 bitů, proto tohle kritérium nebude mít příliš velkou váhu. Čím větší délku klíče CA nabízí, tím lépe je toto kritérium ohodnoceno.

4.2.3 Nabídka služeb

Toto kritérium bude indikovat, jak širokou nabídku služeb CA nabízí. Certifikační autorita může poskytovat například certifikáty pro jednu konkrétní doménu, certifikáty pro více domén nebo certifikáty s podporou pro všechny subdomény (wildcard). Čím širší a rozmanitější je nabídka certifikátů, tím vyšší bude hodnocení.

4.2.4 Záruka

Záruka vrácení peněz v případě prolomení certifikátu. Čím větší je garance vrácení peněz, tím vyšší bude hodnocení.

4.2.5 Rychlost vystavení

V tomto kritériu se poměřuje doba, za kterou CA vydá certifikát. Čím rychleji je CA schopna vystavit certifikát, tím lepší dostane v tomto kritériu hodnocení.

4.2.6 Výběr certifikačních autorit pro druhé porovnání

Pro toto srovnání budou vybrány největší a nejvyužívanější CA na trhu. Jedná se o tyto autority:

1. GeoTrust
2. Thawte
3. RapidSSL
4. Sectigo
5. DigiCert
6. GoDaddy

Rád bych ještě zmínil důvěryhodnou certifikační autoritu Let's Encrypt, která nabízí své služby zdarma. Ovšem svým modelem je atypická a nejedná se o běžnou certifikační autoritu, proto se špatně s ostatními certifikačními autoritami porovnává a do výběru jsem ji nezahrnul.

4.3 Výpočet pomocí vícekriteriální analýzy variant

Jednotlivá porovnání se uskuteční pomocí Saatyho metody párového srovnání a bodovací metody. Tyto dvě metody byly vybrány s cílem dosáhnout co nejpřesnějších výsledků. Obě porovnání budou mít stanovené váhy pro jednotlivá kritéria tak, aby co nejvíce odrážela potřeby porovnání certifikátů z bezpečnostního hlediska a certifikačních autorit z ekonomického hlediska.

4.3.1 Saatyho metoda

Saatyho metoda zohledňuje všechny prvky, včetně jejich vzájemných vazeb a intenzity jejich ovlivňování. K určení vah a vyjádření preferencí mezi jednotlivými kritérii se používá Saatyho škála.

Tabulka 1 Saatyho škála

Číselné preference	Slovní preference
1	Kritéria (varianty) jsou **stejně** významná
3	První kritérium (varianta) je **slabě** významnější než druhé
5	První kritérium (varianta) je **silně** významnější než druhé
7	První kritérium (varianta) je **velmi silně** významnější než druhé
9	První kritérium (varianta) je **absolutně** významnější než druhé

Zdroj: (25)

Pro přesné porovnání je možné využít také sudé hodnoty, konkrétně 2, 4, 6 a 8, tyto hodnoty se nazývají mezihodnotami. Při určování preferencí mezi jednotlivými variantami se využívá metoda párového srovnání. Tato metoda spočívá v určení, která varianta má vyšší preferenci a přiřazení hodnoty ze Saatyho škály. Variantě, která má menší preferenci, je pak přiřazena hodnota ve formě inverzní hodnoty vyšší preference, například 1/3 pokud má vyšší preference hodnotu 3.

4.4 První porovnání

4.4.1 Bodové ohodnocení kritérií pro první porovnání

Kritéria byla stanovena jako maximalizační neboli čím vyšší hodnota tím lépe. Bodové ohodnocení kritérií v bylo založeno na důkladné analýze certifikátů a certifikačních autorit. Kritéria byla ohodnocena na škále od nuly do deseti.

Self-signed certifikát je velmi cenově dostupný, jelikož si ho může kdokoliv vygenerovat zcela zdarma, cena se odvíjí pouze od stráveného času, který uživatel vynaloží na generování certifikátu. Dále u stránek využívající self-signed certifikát není přítomen vizuální indikátor poskytovaný webovými prohlížeči. Self-signed certifikát nepodléhá pravidlům CA/B Fóra a nelze jej efektivně a systematicky zneplatnit. Nemá maximálně stanovenou dobu platnosti, uživatel si tak může nastavit libovolnou dobu platnosti. Self-signed certifikát není autentizovaný důvěryhodnou třetí stranou. Má dobu vystavení v rámci minut, kdy záleží pouze na uživateli, jak dlouho ho bude konfigurovat.

DigiCert certifikát je méně cenově dostupný, jeho cena se pohybuje v rámci tisíců až desetitisíců. Stránky využívající tento certifikát mají viditelný vizuální indikátor poskytovaný webovými prohlížeči. Certifikát od CA Digicert podléhá pravidlům CA/B Fóra a lze jej efektivně a systematicky zneplatnit za pomocí centralizovaných systémů revokace, jako jsou CRL nebo OCSP. Jeho maximální délka platnosti činní 397 dní. Certifikát je autentizovaný důvěryhodnou certifikační autoritou. Dobu vystavení má v rámci jednoho až několika dní.

Tabulka 2 Bodové ohodnocení kritérií prvního porovnání

Kritéria	Self-signed certifikát	DigiCert certifikát
Cenová dostupnost	9	4
Indikátor	2	10
CA/B	0	10
Doba platnosti	4	10
Zneplatnění certifikátu	0	10
Autentizace	0	10
Rychlost vystavení	10	3

Zdroj: Vlastní zpracování

4.4.2 Váhy pro první porovnání

Váhy kritérií v Saatyho metodě se vypočítají jako podíl mezi geometrickým průměrem jednotlivého kritéria a sumou geometrického průměru všech kritérií. Pro první porovnání certifikátů byly stanoveny váhy kritérií pro Saatyho metodu následovně:

Tabulka 3 Stanovení vah pro Saatyho metodu pro první porovnání

Kritéria	Cenová dostupnost	Indikátor	CA/B	Doba platnosti	Zneplatnění certifikátu	Autentizace	Rychlost vystavení	Geometrický průměr	Váhy
Cena	1,00	0,33	0,11	0,20	0,14	0,14	1,00	0,2845837	0,02624405
Indikátor	3,00	1,00	0,13	0,33	0,20	0,20	3,00	0,548834759	0,05061304
CA/B	9,00	7,00	1,00	5,00	3,00	3,00	9,00	4,261301124	0,39297327
Doba platnosti	5,00	3,00	0,20	1,00	0,33	0,33	5,00	1,07570374	0,09920041
Zneplatnění certifikátu	7,00	5,00	0,33	3,00	1,00	1,00	7,00	2,194367895	0,20236259
Autentizace	7,00	5,00	0,33	3,00	1,00	1,00	7,00	2,194367895	0,20236259
Rychlost vystavení	1,00	0,33	0,11	0,20	0,14	0,14	1,00	0,2845837	0,02624405
Celkem	-	-	-	-	-	-	-	10,84374281	1

Zdroj: Vlastní zpracování

Pro bodovací metodu byly stanoveny váhy kritérií v prvním porovnání následovně:

Tabulka 4 Stanovení vah pro bodovací metodu pro první porovnání

Kritéria	Body	Váhy
Cena	2	0,05555556
Indikator	4	0,11111111
CA/B	10	0,27777778
Doba platnosti	5	0,13888889
Zneplatnění certifikátu	7	0,19444444
Autentizace	8	0,22222222
Rychlost vystavení	2	0,05555556
Celkem	36	1

Zdroj: Vlastní zpracování

4.4.3 Výpočet prvního porovnání

Pro každé kritérium se vytvoří Saatyho matice, kde jsou porovnávány jednotlivé varianty. Výsledek každého kritéria je pak získán pomocí váženého geometrického průměru. Postup výpočtu pro jednotlivá kritéria je znázorněn v tabulkách (**Tabulka *5*** až **Tabulka 11**).

Tabulka 5 Saatyho matice pro cenovou dostupnost

Cenová dostupnost	Self-signed certifikát	DigiCert certifikát	Geometrický průměr	Dílčí váhy
Self-signed certifikát	1,00	5,00	2,24	0,83
DigiCert certifikát	0,20	1,00	0,45	0,17
Celkem	-	-	2,68	1,00

Zdroj: Vlastní zpracování

Tabulka 6 Saatyho matice pro indikátor

Indikátor	Self-signed certifikát	DigiCert certifikát	Geometrický průměr	Dílčí váhy
Self-signed certifikát	1,00	0,20	0,45	0,17
DigiCert certifikát	5,00	1,00	2,24	0,83
Celkem	-	-	2,68	1,00

Zdroj: Vlastní zpracování

Tabulka 7 Saatyho matice pro CA/B

CA/B	Self-signed certifikát	DigiCert certifikát	Geometrický průměr	Dílčí váhy
Self-signed certifikát	1,00	0,11	0,33	0,10
DigiCert certifikát	9,00	1,00	3,00	0,90
Celkem	-	-	3,33	1,00

Zdroj: Vlastní zpracování

Tabulka 8 Saatyho matice pro dobu platnosti

Doba platnosti	Self-signed certifikát	DigiCert certifikát	Geometrický průměr	Dílčí váhy
Self-signed certifikát	1,00	0,33	0,58	0,25
DigiCert certifikát	3,00	1,00	1,73	0,75
Celkem	-	-	2,31	1,00

Zdroj: Vlastní zpracování

Tabulka 9 Saatyho matice pro zneplatnění certifikátu

Zneplatnění certifikátu	Self-signed certifikát	DigiCert certifikát	Geometrický průměr	Dílčí váhy
Self-signed certifikát	1,00	0,11	0,33	0,10
DigiCert certifikát	9,00	1,00	3,00	0,90
Celkem	-	-	3,33	1,00

Zdroj: Vlastní zpracování

Tabulka 10 Saatyho matice pro autentizaci

Autentizace	Self-signed certifikát	DigiCert certifikát	Geometrický průměr	Dílčí váhy
Self-signed certifikát	1,00	0,11	0,33	0,10
DigiCert certifikát	9,00	1,00	3,00	0,90
Celkem	-	-	3,33	1,00

Zdroj: Vlastní zpracování

Tabulka 11 Saatyho matice pro rychlost vystavení

Rychlost vystavení	Self-signed certifikát	DigiCert certifikát	Geometrický průměr	Dílčí váhy
Self-signed certifikát	1,00	7,00	2,65	0,88
DigiCert certifikát	0,14	1,00	0,38	0,13
Celkem	-	-	3,02	1,00

Zdroj: Vlastní zpracování

Optimální varianta se určuje jako součet součinu vah a jednotlivých vážených geometrických průměrů kritérií. Na základě těchto výsledků je vytvořena finální tabulka, která identifikuje optimální variantu jako součet součinu vah a jednotlivých vážených geometrických průměrů. Celkové výsledky jsou následně seřazeny, přičemž nejvyšší číslo značí nejlepší výsledek a nejnižší číslo označuje nejhorší výsledek.

Tabulka 12 Výsledná Saatyho matice pro první porovnání

Celkem	Cenová dostupnost	Indikátor	CA/B	Doba platnosti	Zneplatnění certifikátu	Autentizace	Rychlost vystavení	Součet hodnocení	Pořadí
Self-signed certifikát	0,83	0,17	0,10	0,25	0,10	0,10	0,88	0,16	2.
DigiCert certifikát	0,17	0,83	0,90	0,75	0,90	0,90	0,13	0,84	1.
Váhy kritérií	0,02624405	0,05061304	0,392973275	0,099200411	0,20236259	0,20236259	0,02624405	-	-

Zdroj: Vlastní zpracování

Optimální varianta pro bodovací metodu je získána jako součet součinu vah a jednotlivých bodových hodnocení kritérií. Varianta s nejvyšším počtem bodů je považována za optimální pro dané porovnání. Výsledky bodovací metody vypadají následovně:

Tabulka 13 Výsledná tabulka bodovací metody pro první porovnání

Varianty	Body	Pořadí
Self-signed certifikát	1,833333333	2.
DigiCert certifikát	9,8333333	1.

Zdroj: Vlastní zpracování

4.5 Druhé porovnání

4.5.1 Bodové ohodnocení kritérií pro druhé porovnání

Kritéria byla stanovena jako maximalizační neboli čím vyšší hodnota tím lépe. Bodové ohodnocení kritérií v tabulce (Tabulka 14) bylo založeno na důkladné analýze stránek - https://www.servertastic.com/, https://www.ssl2buy.com/, https://cheapsslsecurity.com/, https://www.gogetssl.com/ a jednotlivých stránek certifikačních autorit. Kritéria byla ohodnocena na škále od nuly do deseti.

Certifikační autorita Sectigo, dříve známá jako Comodo, nabízí certifikáty ve všech cenových kategorií, a to od 200 Kč do 8 000 Kč. Díky tomu je velmi cenově dostupná. Zatím nenabízí délku klíče o délce 4096 bitů, ale nabízí standardních 2048 bitů. Ze všech certifikačních autorit nabízí nejširší nabídku certifikátů. S velkým rozpětím nabízených služeb nabízí také velké rozpětí záruk, které se pohybují od 50 000 USD do 1 750 000 USD. U doby vystavení má tato certifikační autorita také velký rozptyl, který se odvíjí od daného certifikátu, a to od pár minut do několika dní.

Certifikační autorita GeoTrust nabízí střední cenovou dostupnost, a to v rozmezí přibližně 1 000 – 10 000 Kč. Také nabízí délku klíče pouze o délce 2048 bitů. Dále nabízí středně velkou nabídku certifikátů a záruku od 500 000 USD po 1 500 000 USD, avšak většina certifikátů má spíše tu menší záruku. Nabízí velmi dobrou rychlost vystavení, u vybraných certifikátu do 5 minut po certifikáty s dobou vystavení pár dnů.

Certifikační autorita Thawte nabízí certifikáty již od 750 Kč po nejdražší certifikáty za 10 000 Kč. Kromě délky klíče o délce 2048 bitů nabízí i délku klíče 4096 bitů. Nemá příliš velkou nabídku služeb. Záruka se pohybuje od 500 000 USD do 1 500 000 USD a u většiny certifikátů se záruka pohybuje spíše u té větší částky. Nabízí průměrnou dobu vystavení a to od 10 minut po několik dní.

Certifikační autorita RapidSSL nabízí pouze velmi cenově dostupné certifikáty a to od 500 Kč do 2000 Kč. Nabízí jenom délku klíče 2048 bitů, tedy nenabízí klíč o délce 4096 bitů. Ze všech certifikačních autorit má nejmenší výběr služeb. Také má nejmenší záruku, a to 10 000 USD. Nabízí nejrychlejší dobu vystavení, a to do 5 minut.

Certifikační autorita DigiCert nabízí pouze certifikáty v dražší cenové kategorii, nejlevnější certifikát stojí 6000 Kč a nejdražší až 38 000 Kč. Nabízí délku klíče 4096 bitů, společně se standardní délkou klíče 2048 bitů. Dále nabízí velmi širokou nabídku služeb.

Také nabízí největší záruku, a to v rozmezí 1 500 000 – 1 750 000 USD. Na druhou stranu má velmi pomalou rychlost vystavení, a to v řádu jednotek dnů.

Certifikační autorita GoDaddy nabízí spíše dražší certifikáty v rozmezí od 1300 Kč do 7000 Kč. Poskytuje délku klíče pouze 2048 bitů. Nabízí průměrný výběr certifikátů a záruku od 10 000 USD do 1 000 000 USD. Rychlost vystavení se pohybuje od 5 minut do několika dní.

Tabulka 14 Bodové ohodnocení kritérií pro druhé porovnání

Kritéria	Sectigo	GeoTrust	Thawte	RapidSSL	DigiCert	GoDaddy
Cenová dostupnost	7	4	5	9	1	3
Délka klíče	9	9	10	9	10	9
Nabídka služeb	10	6	4	2	8	5
Záruka	4	6	8	2	10	3
Rychlost vystavení	6	8	4	10	2	7

Zdroj: Vlastní zpracování

4.5.2 Váhy pro druhé porovnání

Stejným způsobem jako u prvního porovnání byly pro druhé porovnání certifikačních autorit stanoveny váhy kritérií pro Saatyho metodu:

Tabulka 15 Stanovení vah pro Saatyho metodu pro druhé porovnání

Kritéria	Cenová dostupnost	Délka klíče	Nabídka služeb	Záruka	Rychlost vystavení	Geometrický průměr	Váhy
Cenová dostupnost	1	3	0,33333333	3	1	1,24573094	0,19526401
Délka klíče	0,33333333	1	0,2	1	0,33333333	0,46704368	0,07320748
Nabídka služeb	3	5	1	5	3	2,95417694	0,46305701
Záruka	0,33333333	1	0,2	1	0,33333333	0,46704368	0,07320748
Rychlost vystavení	1	3	0,33333333	3	1	1,24573094	0,19526401
Celkem	-	-	-	-	-	6,37972617	1

Zdroj: Vlastní zpracování

Pro bodovací metodu jsou stanovené váhy následovně:

Tabulka 16 Stanovení vah pro bodovací metodu pro druhé porovnání

Kritéria	Body	Váhy
Cenová dostupnost služeb	6	0,25
Délka klíče	2	0,0833333
Nabídka služeb	10	0,4166667
Záruka	2	0,0833333
Rychlost vystavení	4	0,1666667
Celkem	24	1

Zdroj: Vlastní zpracování

4.5.3 Výpočet druhého porovnání

Výpočet matic probíhá stejně jako u prvního porovnání.

Tabulka 17 Saatyho matice pro cenovou dostupnost

Cenová dostupnost	Sectigo	GeoTrust	Thawte	RapidSSL	DigiCert	GoDaddy	Geometrický průměr	Dílčí váhy
Sectigo	1	4	3	0,3333333	7	5	2,2787045	0,2496655
GeoTrust	0,25	1	0,5	0,2	4	2	0,7647245	0,0837868
Thawte	0,3333333	2	1	0,1666667	6	3	1,122462	0,1229822
RapidSSL	3	5	6	1	9	7	4,2227676	0,4626661
DigiCert	0,1428571	0,25	0,1666667	0,1111111	1	0,3333333	0,2457845	0,0269293
GoDaddy	0,2	0,5	0,3333333	0,1428571	3	1	0,4925878	0,0539702
Celkem	-	-	-	-	-	-	9,1270309	1

Zdroj: Vlastní zpracování

Tabulka 18 Saatyho matice pro délku klíče

Délka klíče	Sectigo	GeoTrust	Thawte	RapidSSL	DigiCert	GoDaddy	Geometrický průměr	Dílčí váhy
Sectigo	1	1	0,3333333	1	0,3333333	1	0,6933613	0,1
GeoTrust	1	1	0,3333333	1	0,3333333	1	0,6933613	0,1
Thawte	3	3	1	3	1	3	2,0800838	0,3
RapidSSL	1	1	0,3333333	1	0,3333333	1	0,6933613	0,1
DigiCert	3	3	1	3	1	3	2,0800838	0,3
GoDaddy	1	1	0,3333333	1	0,3333333	1	0,6933613	0,1
Celkem	-	-	-	-	-	-	6,9336127	1

Zdroj: Vlastní zpracování

Tabulka 19 Saatyho matice pro nabídku služeb

Nabídka služeb	Sectigo	GeoTrust	Thawte	RapidSSL	DigiCert	GoDaddy	Geometrický průměr	Dílčí váhy
Sectigo	1	4	6	8	2	5	3,5254688	0,4044316
GeoTrust	0,25	1	3	5	0,3333333	2	1,1649931	0,1336447
Thawte	0,1666667	0,3333333	1	3	0,1666667	0,5	0,4902805	0,0562436
RapidSSL	0,125	0,2	0,3333333	1	0,1428571	0,25	0,2583906	0,0296418
DigiCert	0,5	3	6	7	1	4	2,5132369	0,2883113
GoDaddy	0,2	0,5	2	4	0,25	1	0,7647245	0,087727
Celkem	-	-	-	-	-	-	8,7170943	1

Zdroj: Vlastní zpracování

Tabulka 20 Saatyho matice pro záruku

Záruka	Sectigo	GeoTrust	Thawte	RapidSSL	DigiCert	GoDaddy	Geometrický průměr	Dílčí váhy
Sectigo	1	0,3333333	0,2	3	0,1428571	2	0,6206218	0,0645796
GeoTrust	3	1	0,3333333	6	0,1666667	5	1,3076605	0,1360704
Thawte	5	3	1	7	0,3333333	6	2,438016	0,253691
RapidSSL	0,3333333	0,1666667	0,1428571	1	0,1111111	0,5	0,2758838	0,0287075
DigiCert	7	6	3	9	1	8	4,5668545	0,4752102
GoDaddy	0,5	0,2	0,1666667	2	0,125	1	0,401142	0,0417414
Celkem	-	-	-	-	-	-	9,6101785	1

Zdroj: Vlastní zpracování

Tabulka 21 Saatyho matice pro rychlost vystavení

Rychlost vystavení	Sectigo	GeoTrust	Thawte	RapidSSL	DigiCert	GoDaddy	Geometrický průměr	Dílčí váhy
Sectigo	1	0,3333333	3	0,2	5	0,5	0,8908987	0,101015099
GeoTrust	3	1	5	0,333333333	7	2	2,0300949	0,230183558
Thawte	0,3333333	0,2	1	0,142857143	3	0,25	0,4388458	0,049758806
RapidSSL	5	3	7	1	8	4	3,8701091	0,438814704
DigiCert	0,2	0,1428571	0,3333333	0,125	1	0,1666667	0,2415062	0,027383326
GoDaddy	2	0,5	4	0,25	6	1	1,3480062	0,152844506
Celkem	-	-	-	-	-	-	8,8194609	1

Zdroj: Vlastní zpracování

Stejným způsobem jako v minulém porovnání vytvoříme finální tabulky obou metod a seřadíme výsledky pro nalezení optimální varianty:

Tabulka 22 Výsledná Saatyho matice pro druhé porovnání

Celkem	Cenová dostupnost	Délka klíče	Nabídka služeb	Záruka	Rychlost vystavení	Součet hodnocení	Pořadí
Sectigo	0,24966547	0,1	0,40443164	0,06457963	0,1010151	0,2677987	1.
GeoTrust	0,08378678	0,1	0,13364465	0,13607036	0,23018356	0,1404743	4.
Thawte	0,12298217	0,3	0,05624356	0,25369102	0,04975881	0,1003084	5.
RapidSSL	0,46266608	0,1	0,02964183	0,02870746	0,4388147	0,199175	3.
DigiCert	0,02692929	0,3	0,28831131	0,47521016	0,02738333	0,2008611	2.
GoDaddy	0,05397021	0,1	0,087727	0,04174137	0,15284451	0,0913826	6.
Váhy kritérií	0,19526401	0,07320748	0,46305701	0,07320748	0,19526401	-	-

Zdroj: Vlastní zpracování

Tabulka 23 Výsledná tabulka bodovací metody pro druhé porovnání

Varianty	Body	Pořadí
Sectigo	8	1.
GeoTrust	6,08333333	2.
Thawte	5,08333333	5.
RapidSSL	5,66666667	3.
DigiCert	5,58333333	4.
GoDaddy	5	6.

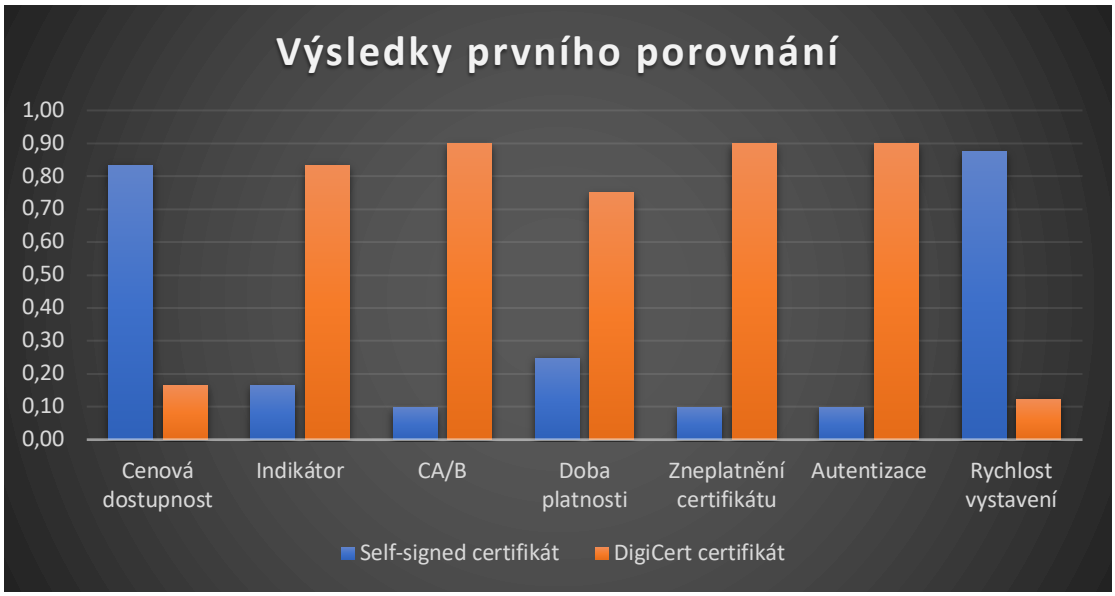
Zdroj: Vlastní zpracování

5 Výsledky a diskuse

5.1 Výsledné grafy

Následující graf srovnává výsledky analýzy bezpečnosti self-signed certifikátu a certifikátu podepsaného důvěryhodnou certifikační autoritou:

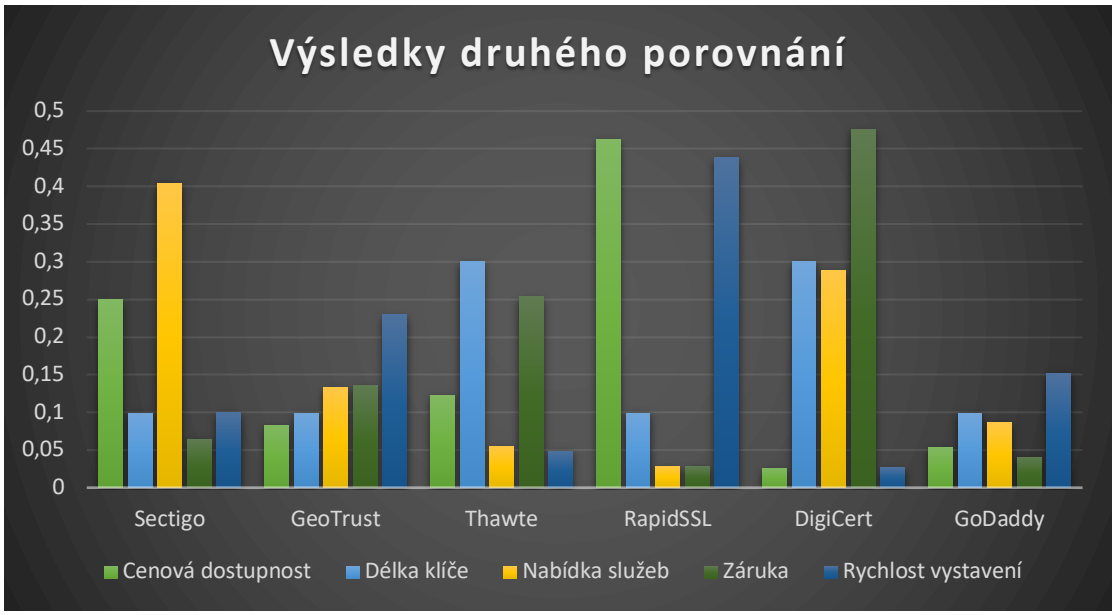
Graf 1 Výsledky prvního porovnání



Zdroj: Vlastní zpracování

Tento graf srovnává výsledky komparativní analýzy, která byla použita pro porovnání vybraných certifikačních autorit na trhu:

Graf 2 Výsledky druhého porovnání



Zdroj: Vlastní zpracování

5.2 První porovnání

Z výsledků obou metod je zřejmé, že self-signed certifikát je ve všech ohledech kromě ceny a rychlosti vystavení horší a není zdaleka tak bezpečný a důvěryhodný, jako certifikát podepsaný důvěryhodnou certifikační autoritou, v tomto případě certifikát od CA DigiCert.

U certifikátu podepsaného důvěryhodnou certifikační autoritou zaplatí zákazník cenu za certifikát a službu spojenou s jeho vystavením, zatímco u self-signed certifikátu zákazník platí pouze svým časem, případně časem zaměstnance, který self-signed certifikát podepíše a spravuje. Z toho vyplývá, že výsledný sloupec u cenové dostupnosti vyšel lépe u self-signed certifikátu.

Naopak vizuální indikátor důvěryhodnosti certifikátu vyšel lépe u certifikátu podepsaného důvěryhodnou certifikační autoritou, jelikož webové prohlížeče vizuální identifikátor u stránek s tímto certifikátem zobrazují, na rozdíl od stránek používající self-signed certifikát, kde tento identifikátor chybí.

Podobně se umístilo i kritérium dodržování pravidel CA/B Fóra, které musí dodržovat pouze důvěryhodné certifikační autority a proto, se v tomto kritériu umístil certifikát od důvěryhodné certifikační autority mnohem lépe.

V kritériu doba platnosti se také lépe umístil certifikát podepsaný důvěryhodnou certifikační autoritou, protože tyto certifikáty se musí prodlužovat každý rok, u self-signed certifikátu žádná taková nutnost neexistuje.

Následně v kritériu zneplatnění certifikátu se lépe umístil certifikát podepsaný důvěryhodnou certifikační autoritou, a to z toho důvodu, že díky centralizovaným systémům revokace, které důvěryhodné certifikační autority používají, lze rychle a efektivně certifikát zneplatnit. To neplatí u self-signed certifikátů, které takto plošně a efektivně zneplatnit nejdou.

V neposlední řadě se v kritériu autentizace lépe umístil certifikát podepsaný důvěryhodnou certifikační autoritou, jelikož tyto certifikační autority ověřují, zda jsou jejich certifikáty spojeny s legitimními subjekty. U self-signed certifikátů k žádné takové kontrole nedochází.

Nakonec v kritériu rychlost vystavení se umístil lépe self-signed certifikát, který lze vystavit během několika minut, na rozdíl od DigiCert certifikátu, u které je doba vystavení v rámci dnů.

Z výsledků všech těchto kritérií se jeví certifikát podepsaný důvěryhodnou certifikační autoritou jako důvěryhodnější a bezpečnější varianta. Pokud uživateli záleží na bezpečnosti a

nepotřebuje certifikát pouze pro testovací prostředí, měl by vždy volit certifikát ověřený důvěryhodnou certifikační autoritou.

5.3 Druhé porovnání

Z výsledků druhého porovnání je patrné, že nejlépe obstála certifikační autorita Sectigo a to v obou použitých metodách. Vyniká zejména v cenové dostupnosti a ve velké nabídce služeb. Proto je serverový certifikát od této certifikační autority nejlepší univerzální volbou.

Na druhém, třetím a čtvrtém místě se o místo dělí certifikační autority RapidSSL, GeoTrust a DigiCert. Důvod proč tyto metody vyšli v obou metodách rozdílně je takový, že při použití vah v Saatyho matici byla určena vyšší váha kritérií nabídka služeb a cenová dostupnost a nižší váha kritéria rychlost vystavení. Saatyho metoda byla také přesnější, jelikož autor porovnával jednotlivé certifikační autority mezi sebou v každém jednotlivém kritériu, na rozdíl od bodové metody, která byla vypočítána pouze pomocí dvou tabulek.

Certifikační autorita RapiSSL je vhodná zákazníkům, kteří potřebují rychle a levně serverový certifikát, jelikož vyniká zejména v cenové dostupnosti a rychlosti vystavení.

Naopak certifikační autorita DigiCert je vhodná velkým firmám, které si mohou dovolit zaplatit větší cenu a společně s ní mít i velkou záruku.

Na předposledním místě se v obou metodách umístila certifikační autorita Thawte, která je zajímavá svou velkou zárukou, ovšem nabízí malou nabídku služeb. Je tak dobrou alternativou k certifikační autoritě DigiCert.

Na posledním místě se nachází certifikační autorita GoDaddy, která se specializuje zejména na pronájem domén a její kvalitu lze tedy ocenit převážně v jiných službách jako je právě web hosting.

Certifikační autorita GeoTrust v žádné kategorii kromě rychlosti vystavení nevyniká, ale ani v žádné nepropadá. Z toho vyplývá, že to je solidní volba a dobrá alternativa ke všem ostatním certifikačním autoritám.

6 Závěr

Tato bakalářská práce se zabývá problematikou serverových certifikátů a jejich vlivem na zabezpečení online serverů. Hlavním cílem práce bylo vytvořit doporučení pro výběr důvěryhodného certifikátu pro zabezpečení serveru s ohledem na ekonomické faktory spojené s tímto výběrem. Za tímto účelem byly vytvořeny dílčí cíle, díky kterým autor došel k závěru.

Prvním dílčím cílem bylo vymezit problematiku důvěryhodnosti serverových certifikátů. Tento cíl autor zpracoval v teoretické části práce, kde byly popsány základy kryptografie a druhy šifrování, následně autor popsal fungování digitálních, serverových a self-signed certifikátů. V neposlední řadě autor popsal certifikační autority a jejich úlohu na internetu a vysvětlil fungování protokolů SSL, TLS a HTTPS.

Druhým dílčím cílem bylo charakterizovat problematiku self-signed certifikátů s ohledem na jejich využití a dopad na bezpečnost a důvěru v online prostředí v porovnání s certifikáty podepsanými důvěryhodnou certifikační autoritou. Tento cíl autor zpracoval v prvním porovnání praktické části, za pomocí analýzy bezpečnosti, kde byly porovnávány self-signed certifikáty s certifikáty podepsanými důvěryhodnou certifikační autoritou za pomocí Saatyho metody a bodovací metody. Výsledek toho porovnání byl prezentován tabulkami a grafy.

Třetím a posledním dílčím cílem bylo porovnat vybrané certifikační autority na trhu. Tento cíl autor zpracoval v druhém porovnání praktické části, kde autor porovnal vybrané certifikační autority na trhu na základě několika stanovených kritérií s rozdílnými váhami pomocí komparativní analýzy, kde byla k porovnání znovu použita Saatyho metoda a bodovací metoda. Použitím obou metod a prezentováním tabulek a výsledného grafu došel autor k výsledku.

Na základě splnění všech tří dílčích cílů lze zákazníkovi doporučit vhodnou certifikační autoritu pro výběr serverového certifikátu. Druh certifikátu od vybrané certifikační autority si poté zákazník musí zvolit na základě svých osobních, případně firemních požadavků a potřeb. Tedy jestli potřebuje certifikát pouze pro jednu doménu nebo subdoménu, pro všechny subdomény nacházející se na hlavní doméně nebo rovnou pro více domén, případně si může vybrat vhodný certifikát podle toho, zda potřebuje ověření domény, organizace nebo rozšířené ověření (EV).

7 Citovaná literatura

1. **Burda, Karel.** *Kryptografie okolo nás.* Praha : Z.NIC, z. s. p. o., 2019. stránky 15-19. ISBN 978-80-88168-52-2.
2. **Frankenfield, Jake.** What Is a Hash? Hash Functions and Cryptocurrency Mining. *Investopedia.* [Online] 28. Květen 2023. [Citace: 3. Srpen 2023.] https://www.investopedia.com/terms/h/hash.asp.
3. **DOSTÁLEK, Libor a Marta VOHNOUTOVÁ.** *Velký průvodce infrastrukturou PKI. 2., aktualiz.* Brno : Computer Press, 2015. stránky 21-77. ISBN 978-80-251-2619-6.
4. **PETERKA, J.** *Báječný svět elektronického podpisu.* Praha : CZ.NIC, 2011. stránky 36-39. ISBN 978-80-904248-3-8.
5. **Národní bezpečnostní úřad.** Právní předpisy. *NBÚ.* [Online] [Citace: 11. Srpen 2023.] https://www.nbu.cz/cs/pravni-predpisy/.
6. **Voců, Michal.** Šifrování a šifrovací systémy. *Ikaros.* [Online] 1997. [Citace: 5. Srpen 2023.] https://ikaros.cz/sifrovani-sifrovaci-systemy.
7. **Computer Hope.** Certificate. *Computer Hope.* [Online] 7. Červen 2021. [Citace: 6. Srpen 2023.] https://www.computerhope.com/jargon/c/certific.htm.
8. **První certifikační autorita, a.s.** Kvalifikovaný certifikát pro elektronickou pečeť. *I. Certification Authority.* [Online] [Citace: 18. Srpen 2023.] https://www.ica.cz/produkty.
9. **Moes, Tibor.** What is a Digital Certificate? 4 Types You Need to Know. *SoftwareLab.org.* [Online] Červen 2023. [Citace: 15. Srpen 2023.] https://softwarelab.org/blog/what-is-a-digital-certificate/.
10. **CZ.NIC, z. s. p. o.** Jak na internet. *Jak na internet.* [Online] 2014. [Citace: 6. Srpen 2023.] https://www.jaknainternet.cz/page/1784/serverove-certifikaty/.
11. **SSLS.** Typy certifikátů. *SSLS.* [Online] [Citace: 9. Srpen 2023.] https://www.ssls.cz/typy-ssl-certifikatu.html.
12. **Sectigo Group, Inc.** What Is a Multi Domain SSL Certificate? *Sectigo Store.* [Online] 2018. [Citace: 10. Srpen 2023.] https://sectigostore.com/page/what-is-a-multi-domain-ssl-certificate/#:~:text=A%20multi%20domain%20SSL%20certificate%20is%20a%20single%20certificate%20that,party%20certificate%20authority%20(CA)..
13. **Yackel, Ryan.** What are extended validation certificates? And are they dead? *KEYFACTOR.* [Online] 14. Duben 2021. [Citace: 19. Srpen 2023.] https://www.keyfactor.com/blog/what-are-extended-validation-certificates-and-are-they-dead/#:~:text=An%20EV%20certificate%20is%20the,identity%20of%20the%20website%20owner..
14. **Gitlan, Dionisie.** Are Self-Signed Certificates Secure? What Are the Risks? *SSL Dragon.* [Online] 2024. [Citace: 10. Březen 2024.] https://www.ssldragon.com/blog/dangers-self-signed-certificates/.
15. **Borges, Esteban.** Dangers of Using Self-Signed Certificates. *SecurityTrails.* [Online] 2023. [Citace: 9. Březen 2024.] https://securitytrails.com/blog/dangers-of-using-self-signed-certificates.
16. **Dobry, Jason.** What is a self-signed SSL certificate? *Nexcess.* [Online] 9. Září 2019. [Citace: 16. Srpen 2023.] https://www.nexcess.net/help/what-is-a-self-signed-ssl-certificate/.
17. **Garakh, Iliya.** 7 ways to create self-signed certificates on Windows . *Passwork.* [Online] 23. Prosinec 2021. [Citace: 22. Srpen 2023.] https://blog.passwork.pro/7-ways-to-create-self-signed-certificates-on-windows/.
18. **devopscube.** How to Create Self-Signed Certificates using OpenSSL. *devopscube.* [Online] 1. Srpen 2022. [Citace: 25. Srpen 2023.] https://devopscube.com/create-self-signed-certificates-openssl/.

19. **Pospíšil, Vojtěch.** Co jsou a k čemu slouží certifikační autority? *interval.cz.* [Online] 16. Listopad 2021. [Citace: 12. Srpen 2023.] https://www.interval.cz/clanky/co-jsou-a-k-cemu-slouzi-certifikacni-autority/.
20. **KOMAR, Brian.** *Windows Server® 2008 PKI and Certificate Security.* Washington : Microsoft Press, 2008. stránky 29-33. ISBN 9780735625167.
21. **SSL Suport Team.** What is SSL? *SSL.com.* [Online] 28. Září 2021. [Citace: 24. Srpen 2023.] https://www.ssl.com/faqs/faq-what-is-ssl/.
22. **F., Domantas G. & Brian.** What Is SSL? Understanding Secure Sockets Layer and How It Works. *Hostinger.* [Online] 23. Březen 2023. [Citace: 25. Srpen 2023.] https://www.hostinger.com/tutorials/what-is-ssl.
23. **Sopha, M.** What Is TLS? Understanding Transport Layer Security and How It Works. *Hostinger.* [Online] 7. Květen 2023. [Citace: 25. Srpen 2023.] https://www.hostinger.com/tutorials/what-is-tls.
24. **Chipeta, Catherine.** What is HTTPS? How it Works and Why It's So Important. *UpGuard.* [Online] 7. Únor 2023. [Citace: 21. Srpen 2023.] https://www.upguard.com/blog/what-is-https.
25. **Šubrt, Tomáš.** *Ekonomicko-matematické metody.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2011. ISBN 978-80-7380-345-2.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů

8.4 Seznam použitých zkratek

CA	Certifikační autorita