Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Digitální certifikáty

Bc. Ondřej Svačina

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Ondřej Svačina

Informatika

Název práce

Digitální certifikáty

Název anglicky

Digital certificates

Cíle práce

Diplomová práce je tematicky zaměřena na problematiku digitálních certifikátů pro zabezpečenou komunikaci v informačních systémech. Hlavním cílem práce je analyzovat digitální certifikáty jako takové. Dílčími cíli diplomové práce je také analyzovat certifikační autority, realizovat vlastní certifikační autoritu a certifikáty, analyzovat vědomosti o bezpečnosti certifikátů na vybraném vzorku osob.

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýze odborných informačních zdrojů. Dále autor realizuje případovou studii a provede dotazníkové šetření. Na základě syntézy teoretických poznatků budou formulovány závěry diplomové práce.

Doporučený rozsah práce

60

Klíčová slova

Digitální certifikát, certifikační autorita, certifikace, kryptografie, klíče, bezpečnost

---

Doporučené zdroje informací

DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.

KUROSE, James F a Keith W ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.

OPPLIGER, Rolf. SSL and TLS theory and practice. Boston: Artech House, 2009. ISBN 978-15-969344-8-1.

PETERKA, Jiří. Báječný svět elektronického podpisu. Praha: CZ.NIC, c2011, 430 s. CZ.NIC. ISBN 978-80-904248-3-8.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 19. 11. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 20. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 29. 03. 2016

Čestné prohlášení

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

V Praze dne 31.03.2016 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Tomášovi Vokounovi za poskytnutí cenných rad a připomínek při psaní této práce, dále paní Ing. Zuzaně Novotné, Ph.D. za konzultace s dotazníkovým šetřením a mým rodičům, kteří mi umožnili studovat a tedy i psát tuto práci. Poděkování patří také přátelům za poskytnutou pomoc při studiu, přítelkyni za podporu při psaní a v neposlední řadě respondentům za jejich čas.

Digitální certifikáty

Digital certificates

Souhrn

Práce představuje problematiku digitálních certifikátů pro zabezpečenou komunikaci. Nejprve byly zjištěny metody autentifikace a kryptografie. Dále se práce věnuje komunikačním protokolům pro zabezpečené připojení HTTPS a SSL/TLS, významu certifikačních autorit, jejich vlastnostem a analýze samotných digitálních certifikátů.

Praktická část představuje dostupné certifikační autority včetně praktické realizace vlastní certifikační autority a vystavení certifikátu. Tento vytvořený nedůvěryhodný certifikát se stal klíčovým prvkem dotazníkového šetření, které zjišťuje stupeň informovanosti uživatelů o bezpečnosti připojení prostřednictvím důvěryhodných digitálních certifikátů. Po analýze, interpretaci získaných dat a ověření vybraných hypotéz byly stanoveny doporučení pro majitele domén plánující přechod na HTTPS.

Summary

This thesis is focused on the topic of digital certificates for secure communication. First of all, methods of authentication and cryptography are analyzed as a starting point. Furthermore, the thesis describes communication protocols for secure connection HTTPS and SSL/TLS, the importance of certification authorities and their characteristics. It devotes the biggest part of attention to digital certificates as such.

Practical part introduces available certification authorities, including practical creation of the new certification authority and certificate. This untrusted certificate has become the key element of the questionnaire survey, which aim is to analyze knowledge level of users about secure connection through trusted certificates. After the analysis, interpretation of obtained data and verification of selected hypothesis, recommendations for domain owners, who are planning to use HTTPS, were proposed.

Klíčová slova: Digitální certifikát, certifikační autorita, certifikace, důvěryhodnost, kryptografie, párové klíče, zabezpečené připojení, HTTPS, SSL/TLS, bezpečnost.

Keywords: Digital certificate, certification authority, certification, trustworthiness, cryptography, pair of keys, secure connection, HTTPS, SSL/TLS, security.

Obsah

Seznam obrázků

Seznam grafů

Seznam tabulek

1 Úvod

Rostoucí počet osob využívajících moderních komunikačních technologií a současný přechod z papírových dokumentů na elektronické vyžaduje i rozšiřování autentizačních metod. Za pomoci kvalifikovaných certifikátů je možné komunikovat se státními orgány, podávat žádosti či daňová přiznání, atd. S využitím komerčních certifikátů je možné šifrovat, autentizovat a přistupovat zabezpečeným protokolem HTTPS na webové servery.

K ověření identity účastníka digitální komunikace slouží systém digitálních certifikátů a certifikačních autorit, označovaný jako infrastruktura veřejného klíče. Celý proces je postaven na asymetrické kryptografii se soukromým a veřejným klíčem.

Práce bude nejprve zaměřena na základní východiska, jako je autentizace a kryptografie, kde budou popsány jednotlivé možnosti šifrování. Další důležitou kapitolou budou komunikační protokoly využívané k zabezpečenému připojení. Poté již bude přiblížena činnost certifikačních autorit, včetně důležité subkapitoly zaměřující se na jejich důvěryhodnost a možnost vytvořit vlastní certifikační autoritu. Poslední kapitola teoretické části bude věnována samotným digitálním certifikátům, jejich struktuře, druhům i životnímu cyklu.

V praktické části budou analyzovány certifikační autority dostupné na českém trhu. Nejprve bude práce zaměřena na akreditované autority, dále budou vybráni poskytovatelé bezplatných důvěryhodných autorit a v neposlední řadě bude realizována vlastní certifikační autorita. Díky ní bude vystaven vlastní certifikát, který bude ovšem považován za nedůvěryhodný. Je očekáváno, že uživatelé ignorují varovné zprávy o nedůvěryhodnosti certifikátu, a nezáleží tak na jeho vystavovateli. K ověření domněnky bude využito dotazníkové šetření s praktickým příkladem. Druhý oddíl bude tedy zaměřen na zjištění stupně informovanosti uživatelů o bezpečnosti připojení prostřednictvím důvěryhodných digitálních certifikátů. Získaná data budou následně interpretována. Na základě výsledků budou stanoveny doporučení pro majitele domén, kteří plánují přechod na HTTPS.

Problematice se věnuje několik knih, ovšem problém nastává v jejich zastaralosti a neaktuálnosti. Proto bylo potřeba některé informace z tištěných publikací ověřovat pomocí elektronických zdrojů. Problematika digitálních certifikátů je tak široké téma, že je těžké jej popisovat pouze na daný rozsah diplomové práce. Některé detaily musely být proto vypuštěny či přesunuty do příloh jinak by práce dosahovala mnohem objemnější publikace.

2 Cíl práce a metodika

Cílem teoretické části diplomové práce je přiblížit problematiku zabezpečené komunikace s využitím digitálních certifikátů. Hlavním cílem práce proto byla zvolena analýza samotných digitálních certifikátů. Předtím je ale potřeba objasnit témata, jako jsou autentizace, kryptografie, zabezpečené komunikační protokoly a certifikační autority.

V praktické části budou využity poznatky a znalosti získané z teoretické části. Dílčím cílem je analyzovat certifikační autority, realizovat vlastní certifikační autoritu a certifikát. Dalším dílčím cílem je, s využitím vystaveného nedůvěryhodného certifikátu a dotazníkového šetření, analyzovat vědomosti o bezpečnosti certifikátů. Na základě získaných poznatků budou formulovány závěry šetření, následně pak stanovena doporučení pro majitele domén a pro rozšíření povědomí o této problematice mezi uživatele.

Metodika řešené problematiky diplomové práce je založena na studiu a analýze odborných informačních zdrojů. Hlavním zdrojem byla publikace Velký průvodce infrastrukturou PKI a technologií elektronického podpisu (1), kde je problematika přehledně, obsáhle a zároveň srozumitelně popisována. Problémem byla neaktuálnost některých informací, které byly ověřovány pomocí dalších knižních či elektronických zdrojů.

Následně proběhla analýza dostupných certifikačních autorit pomocí informací uvedených na jejich webových stránkách případně v jejich dokumentech týkajících se certifikačních politik. S využitím softwaru X Certificate and key management, dle přehledné příručky, byla vytvořena certifikační autorita společně s vystaveným certifikátem, který byl následně umístěn na zaregistrovaný webový hosting. Praktický příklad nedůvěryhodného certifikátu stál za vznikem a provedením dotazníkového šetření, které bylo vyhodnoceno pomocí softwaru Microsoft Excel a SAS. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány doporučení a závěry diplomové práce.

3 Teoretická východiska

V dnešní době každou vteřinou přibývá počet informací proudících na internetu. Dle statistiky webových stránek bylo k 17. 3. 2016 v databázích vyhledáčů přes 4,63 miliard stránek. Podle D. Evanse bude v roce 2020 připojeno k internetu 50 miliard zařízení (Příloha A). Mezi tato zařízení nepatří jen elektronika, jako jsou chytré telefony a tablety, ale už i další typy jako například rychlovarné konvice či bezdrátové monitory pro kardiaky. S roustoucí intenzitou digitální komunikace je tedy potřeba rozšiřovat zejména i autentizační metody. (2) (3)

3.1 Autentizace

Samotný termín „autentizace“ byl převzat z latinského původu „authenticus“. V češtině a odborné literatuře se používá několik podobných termínů jako „autentifikace“ nebo „autentikace“, které mají naprosto stejný význam. Ovšem Ústav pro jazyk český se přiklání k variantě „autentizace“, a proto bude v textu nejčastěji použit právě tento termín. Autentizace představuje proces prokázání pravosti entity, například osoby, zprávy nebo programu (kódu) atd. Pokud je autentizace úspěšná, tak se potvrdí identita ověřované entity a zajistí se ochrana před falzifikací. (4)

Pro tento proces se využívá mnoho metod různého stupně zabezpečení a úrovně spolehlivosti, mezi ně lze zařadit autentizaci:

- pomocí hesla – kdy je potřeba dbát na pravidla bezpečného hesla. (1 str. 31)
- pomocí prostředků na ukládání aktiv – kdy může být využito uložení aktiv na disk či hardwarový klíč – například čipová karta, USB token, HSM (Host security modul). Dále mezi hardwarové zařízení lze zařadit autentizační kalkulátor. Bezpečnostní požadavky hardwarových nástrojů jsou specifikovány ve standardu FIPS 140-2 vydaným Národním institutem standardů a technologií Spojených států.[1] (1 stránky 37–51)
- pomocí biometriky – kam se řadí ověření identity otiskem prstu, snímáním duhovky či sítnice, geometrie ruky, rozpoznávání obličeje a další metody. (1 str. 36)

[1] National Institute of Standarts and Technology. *FIPS Publications* [online]. [cit. 2016-03-16]. Dostupné z WWW: <http://csrc.nist.gov/publications/PubsFIPS.html>.

- pomocí vícefaktorové autentizace – tato možnost je nejbezpečnější cestou, jelikož je kombinací ochrany na základě znalosti (hesla), vlastnictví (prostředek na ukládání aktiv) a biometrie (sám uživatel). V případě prozrazení jednoho z prvků není uživatel v nebezpečí, jelikož je zajištěn dalšími typy zabezpečení. Běžně je využívano dvouúrovňové zabezpečení – například při použití platební karty a ověření PINem. (5)

3.2 Kryptografie

Kryptografie neboli šifrování, je matematický vědní obor, který se zabývá utajováním zpráv před nežádoucím zobrazením jinými osobami než těmi, pro které je zpráva určena. Využívají se k tomu šifrovací algoritmy, které pomocí klíče dokáží zprávu (text nebo i data) zašifrovat. Zabezpečenou zprávu je poté možné přenést i nezabezpečenou cestou cílovému adresátovi. Ten využije znalosti šifrovacího algoritmu a příšlušného klíče k dešifrování zprávy a tím se dostane k původní zprávě. (1 stránky 21–30)

Algoritmy používané k šifrování se mohou dělit podle způsobu šifrování zprávy na prodouvé a blokové šifrovače. Zatímco proudové šifrují postupně každý jednotlivý znak textu na šifru, pomocí blokových šifrovačů se zabezpečují celé bloky určité délky textu na šifru se stejnou délkou. Takto dále pro každý další blok, kdy se délka bloků pohybuje na 64 či 128 bitech. (1 stránky 21–30)

Obor, který dešifruje text z šifrované zprávy, ovšem bez znalosti klíče a někdy i bez znalosti využitého kryptografického algoritmu, se nazýva kryptoanalýza. Mezi hlavní vynalezená šifrovací schémata se řadí symetrická a asymetrická kryptografie. (1 stránky 21–30)

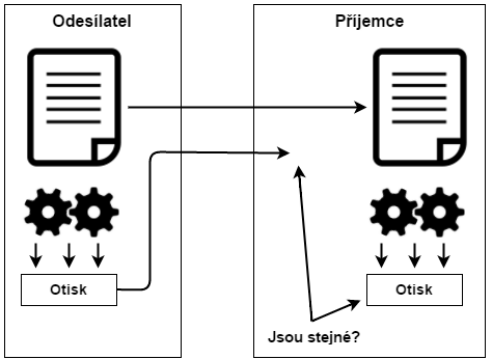
3.2.1 Hashovací funkce

Otisk (hash) je jednocestná funkce, díky níž je možné libovolně dlouhý text přetvořit na krátký řetězec s konstantní délkou. Původní text by měl být maximálně charakterizován výsledným otiskem, jelikož i drobnou změnou v původním řetězci se způsobí velká změna v otisku. Díky tomu, že se otisk tvoří z jakkoliv dlouhého řetězce, existuje tak teoreticky velice nízká pravděpodobnost nalezení původního textu k určitému otisku. (1 stránky 21–23)

Jednocestná funkce představuje algoritmus, který je výpočetně nenáročný. Ovšem velice náročným je nalezení původního textu k výsledku otisku. Konstrukce těchto funkcí

probíhá přes výpočetní operace na nízkých úrovních, například bitové operace a posuny, díky čemuž je zajištěna efektivnost a rychlost výpočtu. Tento algoritmus nepatří mezi kryptografické algoritmy, jelikož ze samotného otisku již nelze získat původní řetězec. (1 stránky 21–23)

Hashovací funkce se využívá po přenosu k ověření zprávy, zda po cestě nebyla nějakým způsobem modifikována či poškozena, tzn. je tedy používána jako důkaz integrity zprávy. Strana odesílající data (text) zprávy ji doplní o část, která obsahuje otisk této zprávy. Druhá strana po přijetí zprávy si vypočte otisk přijaté zprávy a porovná jej s přiloženým otiskem první strany (Obrázek 1). V případě shody lze usoudit, že zpráva nebyla cestou modifikována. Kontrola integrity je tímto způsobem využívána i linkovými protokoly (například Ethernet) pro zjištění chyb linek. (1 stránky 21–23)



Obrázek 1: Použití otisku k ověření integrity zprávy

Zdroj: Vlastní zpracování dle (1 stránky 21–23)

Ovšem v případě útoku má útočník možnost odposlechu zprávy přenášené od první strany. Následně pak může modifikovat její obsah a dle veřejně popsaného výpočtu otisku vytvořit nový otisk, kterým nahradí ten původní. Přijímající strana následně považuje tuto modifikovanou zprávu za původní. (1 stránky 21–23)

Z tohoto důvodu se využívá způsob označený jako MAC (Message Authetication Code), který používá sdílené tajemství (například pouhé slovo nebo věta) zahrnuté do výpočtu otisku. Útočník, který nezná tajemství, pak není schopen vygenerovat stejný otisk a nemůže tak editovat zprávu. (1 stránky 21–23)

Hashovací algoritmus, který byl pojmenován jako MD5 (Message-Digest) vznikl v roce 1991. Roku 1996 byla objevena nepříliš vážná chyba, avšak již v roce 2004 byly objeveny zásadní chyby – jeho použití se tak nedoporučuje. (1 stránky 21–23) (6)

Národní bezpečnostní agentura v USA vyvinula algorimus SHA (Secure Hash Algorithm), který slučuje skupinu pěti různých algoritmů odlišujících se délkou

vystupujících klíčů v bitech. Algoritmus nalezl využití také v aplikacích či v komunikačních protokolech jako SSH (Secure Shell), SSL (Secure Sockets Layer) či při kontrole integrity komunikace a souborů. Rozdíl mezi SHA-0 a SHA-1 je pouze v jedno bitové rotaci, která byla provedena využitím jednocestné funkce. Algoritmy z originálního řetězce vytvářejí 160 bitový otisk. Bylo ovšem nalezeno několik závažný chyb a Ministerstvo vnitra České republiky vydalo pokyn, aby od 1. 1. 2010 české certifikační autority vydávaly ověřené certifikáty pouze s podepisovacím algoritmem, který používá hashovací funkci SHA-2. Microsoft se rozhodl taktéž omezovat podporu certifikátu s SHA-1. Od 1. 1. 2016 by všechny certifikační autority měli vystavovat certifikáty pouze s SHA-2. Od 1. 1. 2017 nebude Microsoft důvěřovat žádným certifikátům podepsaným SHA-1. (1 stránky 21–23) (7) (8)

Společným označením SHA-2 jsou myšleny čtyři hashovací funkce, které nesou číselné označení podle velikosti generovaného otisku v bitech – SHA-224, SHA-256, SHA-384, SHA-512. Tyto verze hashovacích funkcí byly publikovány již v roce 2001, ale jejich rozšíření mezi širokou veřejnost bránila zejména nedostačující podpora od systému Windows XP. Velikost otisku tedy vzrostla až na 512 bitů. (1 stránky 21–23)

Dne 2. 11. 2007 byla americkým institutem NIST (National Institute of Standards and Technology) vyhlášená veřejná soutěž, jejímž cílem bylo vyvinout novou hashovací funkci, která bude označena jako SHA-3. Do soutěže byli přihlášeni i čeští odborníci, kteří spolupracovali na vývoji nové hashovací funkce. Byly to RNDr. Vlastimil Klíma (Blue Midnight Wish, EDON-R) a prof. Aleš Drápal (hashovací algoritmus EDON-R), ovšem ani jeden z nich nedosáhl finálového umístění. Dne 2. 10. 2012 byl oznámen vítěz této pětileté soutěže, kterým se stal algoritmus Keccak a porazil tak 63 ostatních algoritmů. Tým odborníků NIST ocenil na algoritmu především jeho možnost běhu na různých počítačových zařízeních, rychlost při implementaci hardwaru, elegantní design a přehlednou konstrukci. Jak prohlásil počítačový expert Tim Polk, algoritmus Keccak odlišuje jiný způsob výpočtu otisku od SHA-2 a poskytuje tak důležitou pojistku v případě, že bude algoritmus SHA-2 prolomen. V srpnu 2015 již NIST vydal standard pro SHA-3 (FIPS – 202[2]). (9) (10) (11)

[2] National Institute of Standards and Technology. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* [online]. In: Gaithersburg: Information Technology Laboratory, 2015, s. 37 [cit. 2016-03-15]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

3.2.2 Replay attack, nonce

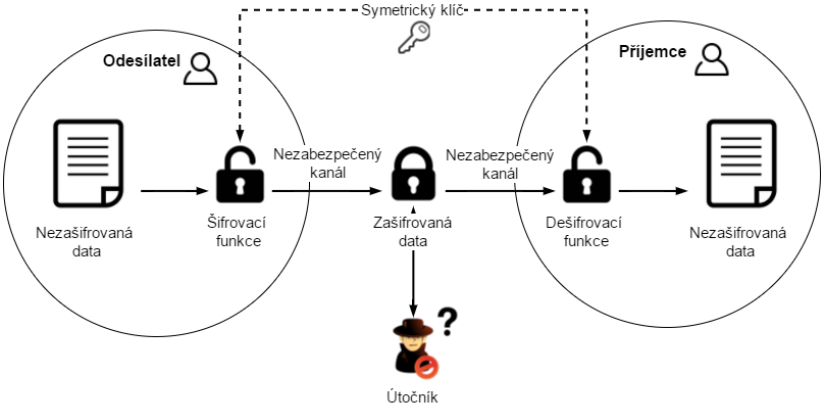
Útok označovaný jako replay attack využívá otisku a jeho nedostatku. Ten spočívá v tom, že útočník může zaznamenat a odposlechnout celou přenášenou zprávu včetně MAC a po určitém čase ji poslat přijímací straně znovu. Tento způsob lze využít například při zadávání platebního příkazu bance. Příkaz bude poté zaplacen dvakrát, banky tento krok označují jako dual spend attack. (1 str. 23)

Obranou proti takovému útoku je například vzestupné číslování zpráv. Pokud druhá strana obdrží nižší číslo zprávy, než které očekávala, bude jí jasné, že se jedná o zopakovanou starou zprávu. Stejně tak banky nezpracují dva příkazy se stejným číslem. (1 str. 23)

Jiný způsob obrany se nazývá nonce – označuje dostatečně dlouhé náhodné číslo přidávané do zprávy. Tím je zajištěno, že s velmi nízkou pravděpodobností by mohly být vygenerovány dvě stejné MAC a tím pádem odeslány dvě stejné zprávy. Pro ještě větší snížení této pravděpodobnosti se často náhodné číslo skládá ze dvou částí, kdy jedna obsahuje samotné náhodné číslo a druhá je složena z neopakovatelné položky – datum a čas. (1 str. 23)

3.2.3 Symetrické šifra

Symetrické šifrování a dešifrování je takový způsob zabezpečení komunikace, kdy je pro obě činnosti použit stejný klíč označovaný jako tajný klíč. Klíč je sdílen mezi oběma komunikujícími stranami a je nutno jej chránit před nežádoucí třetí stranou, která by v případě jeho zjištění mohla jednoduše šifru dešifrovat. Symetrické šifrování má také autorizační smysl, jelikož zprávu mohla zašifrovat pouze druhá strana znající společný tajný klíč. (1 str. 24)



Obrázek 2: Princip symetrického šifrování
Zdroj: Vlastní zpracování dle (12 str. 270)

Důležitým prvkem silného zabezpečení je použítá délka klíče. Krátké klíče je možné prolomit útokem hrubou silou neboli zkoušením všech možných kombinací klíčů. Tabulka 1 představuje nejběžnější symetrické šifrovací algoritmy společně se základními vlastnostmi. (1 str. 24)

Šífrovací algoritmus	Typ	Délka klíče	Autor	Standard z roku	Status
DES (Data Encryption Standard)	Blokový 64 bitů	56 bitů	IBM	1977	**Nebezpečný, odstraněn z TLS 1.2**
3DES (Triple Data Encryption Standard)	Blokový 64 bitů	112 nebo 168 bitů	IBM	1978	**Nebezpečný, součástí TLS 1.2**
RC4 (Rivest's Cipher 4)	Proudový	40 – 256 bitů	RSA Security	1987	**Dlouhodobě slabý, prohlížeči zakázán**
IDEA (International Data Encryption Algorithm)	Blokový 64 bitů	128 bitů	ETH Zurich	1991	**Nebezpečný, odstraněn z TLS 1.2.**
AES (Advanced Enryption Standard)	Blokový 128 bitů	128, 192 či 256 bitů	Rijmen, Daemen	2002	**Doporučovaný**

Tabulka 1: Přehled symetrických šifrovacích algoritmů

Zdroj: Vlastní zpracování dle (13 stránky 34–36), (14)

3.2.4 Asymetrické šifrování

Asymetrické šifrování na rozdíl od symetrického používá dva klíče – jeden k šifrování a druhý k dešifrování. (1 stránky 25–26)

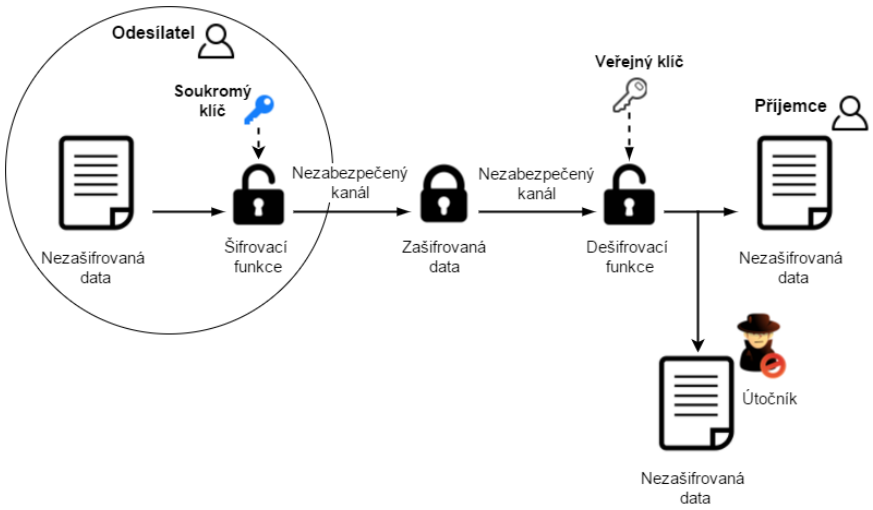
Mezi základní vlastnosti těchto klíčů patří to, že data, která jsou zašifrována jedním klíčem, je možné dešifrovat pouze klíčem druhým z této dvojice a také, že v případě znalosti jednoho klíče není možné (za krátký čas) odvodit klíč druhý. (1 stránky 25–26)

Data je možné zašifrovat jakýmkoliv z dvojice těchto klíčů, proto je označení šifrovací a dešifrovací zavádějící. Častějším pojmenováním se uvádí soukromý a veřejný

klíč, které označují funkci těchto klíčů. Zatímco soukromý je určen pouze pro vlastníka a nesmí se dostat k někomu jinému, veřejný klíč je dostupný komukoliv. Utajení soukromého klíče je základem bezpečnosti a principů asymetrického šifrování. (1 stránky 25–26)

Pomocí výše uvedených pravidel je možné v asymetrickém šifrování odvodit samotný průbeh šifrování. K dispozici jsou čtyři klíče – jednak soukromý a veřejný klíč odesílající strany a jednak soukromý a veřejný klíč přijimací strany. Odesílající strana má na zašifrování zprávy čtyři možnosti použití klíčů: (1 stránky 25–26)

1. **Zašifrování dat svým veřejným klíčem** – dešifrovat data pak může pouze ten, kdo vlastní odpovídající soukromý klíč, tedy pouze odesílající strana. Odesílatel si tímto způsobem zašifruje data pouze sám pro sebe, jelikož příjemce není schopen dešifrovat tato data.
2. **Zašifrování dat svým soukromým klíčem** (Obrázek 3) – dešifovat data může vlastník odpovídajícího veřejného klíče, což může být jak příjemce, útočník, tak vlastně kdokoliv. Pro šifrování dat je proto tato varianta nevhodná, avšak využívá se pro ověření vlastnictví soukromého klíče.

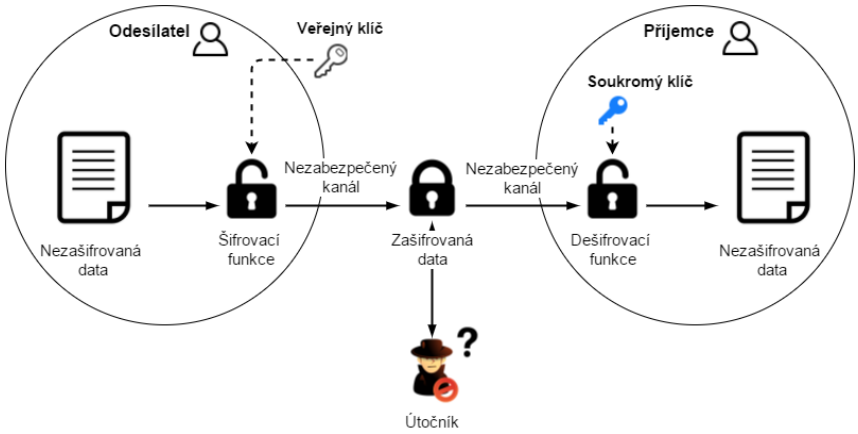


Obrázek 3: Přenos neadresovaných šifrovaných dat soukromým klíčem

Zdroj: Vlastní zpracování dle (12 str. 270)

3. **Zašifrování dat příjemcovým soukromým klíčem** – v této variantě by bylo porušeno základní pravidlo, že nikdo by neměl poskytnout svůj soukromý klíč další straně. Odesílatel by tedy neměl mít možnost získat cizí soukromý klíč.

4. **Zašifrování dat příjemcovým veřejným klíčem** (Obrázek 4) – dešifrovat data může ten, kdo vlastní odpovídající soukromý klíč, tedy pouze přijímací strana. Tato varianta je tak jedinou správnou možností.



Obrázek 4: Přenos adresovaných šifrovaných dat veřejným klíčem
Zdroj: Vlastní zpracování dle (12 str. 270)

Pomocí asymetrického šifrování odpadá starost z bezpečného předání tajného klíče druhé straně jako v případě symetrické kryptografie, jelikož příjemce poskytuje komukoliv přístup k veřejnému klíči. Mezi slabé stránky algoritmů pro asymetrické šifrování patří, že jsou náročné na výpočetní zpracování a samotné šifrování zprávy by tak mohlo být pomalé. V běžné praxi se proto používá kombinace asymetrického a symetrického šifrování. (1 stránky 25–26)

Nepoužívanějším algoritmem pro asymetrické šifrování je RSA (příjmení autorů Rivest, Shamir, Adleman), který byl poprvé zveřejněn v roce 1978. RSA klíče mohou být libovolně veliké, ale v současnosti je doporučováno používat velikost 2048 bitů. Algoritmus RSA vychází z problému rozložení velkých čísel na prvočísla, kdy je jednoduché vypočítat ze dvou velkých prvočísel p a q jejich součin n, jako n = p *q. Ovšem je velice výpočetně náročné zjistit hodnotu prvočísel p a q při znalosti jejich součinu n. (1 stránky 25–26)

Alternativou je algoritmus EC (Elliptic Curve), který je založen na výpočetní operaci s eliptickými křivkami. Klíče tohoto algoritmu jsou mnohem menší než RSA klíče. Jako příklad se uvádí, že 160 bitový klíč EC je srovnatelně zabezpečený jako klíč RSA s 1024 bity. Jeho výhodou je i menší výpočetní zatížení, i přesto je málo rozšířený. (1 stránky 25–26)

Algoritmus DH (Diffie-Hellman) je navržený pro zabezpečenou výměnu tajných klíču mezi dvěmi stranami v symetrickém šifrování nebo i jiných sdílených tajemstvích.

Princip je založen na vygenerování soukromých a veřejných DH čísel, kde si obě komunikující strany navzájem vymění veřejná čísla DH. S pomocí předaných a vlastních dat si následně nezávisle na sobě vygenerují stejná sdílená tajemství, používána v dalších částech šifrované komunikace. (1 stránky 25–26)

3.2.5 Kombinace symetrického a asymetrického šifrování

Jelikož symetrické šifrování není příliš bezpečné a asymetrické šifrování je poměrně náročné, využívá se proto jejich kombinace (Obrázek 5). Prvním krokem je zašifrování dat symetrickým klíčem, který je poté zašifrován veřejným klíčem příjemce. Příjemce si zprávu dešifuje pomocí soukromého klíče, čímž získá symetrický klíč a následně jej použije pro dešifrování samotných dat. Tento způsob kombinace šifrování se používá i u protokolu TLS, kdy je veřejným klíčem serveru zašifrován klíč symetrický používaný pro šifrování dat. (15)

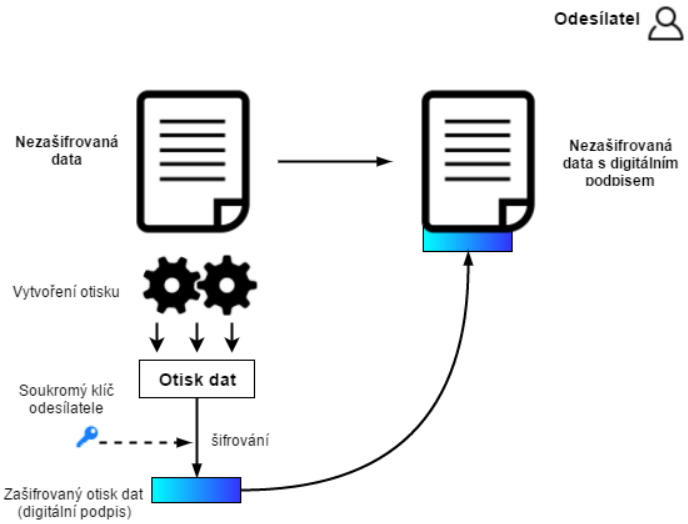
Obrázek 5: Komunikace pomocí kombinace symetrického a asymetrického šifrování
Zdroj: Vlastní zpracování dle (15)

3.2.6 Elektronický podpis

Nejprve je důležité představit samotný termín „elektronický podpis“, jelikož podle terminologie zákona č. 227/200 Sb. o elektronickém podpisu se ve skutečnosti jedná o „zaručený elektronický podpis“. (4 stránky 533–538)

Potřeba podepisování dat vznikla z toho důvodu, že se tímto způsobem dokáží data propojit s příslušnou podepisující osobou, což samotné šifrování neumí zajistit. Jak již bylo popsáno, při asymetrickém šifrování se k šifrování dat pro příjemce používá přijemcův veřejný klíč. Z toho vyplývá, že klíč je veřejně dostupný a šifrovanou zprávu může tedy poslat kdokoliv. (4 stránky 533–538)

Ovšem kombinací vlastností asymetrického šifrování a hashovací funkce vzniklo podepisování dat, které zobrazuje Obrázek 6.

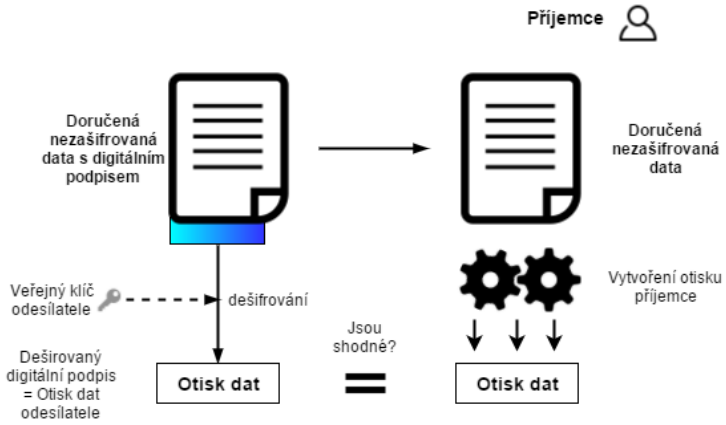


Obrázek 6: Vytvoření digitálního podpisu odesílatele

Zdroj: Vlastní zpracování dle (1 str. 27)

Dohodnutá hashovací funkce je využita na výpočet otisku ze vstupních dat. Otisk je následně zašifrován soukromým klíčem odesílatele. Nyní již lze hovořit o elektronickém podpisu, jelikož tím se stal právě zašifrovaný otisk, který se domluveným způsobem připojí k odesílanému dokumentu. Poté je celý soubor odeslán příjemci. (1 str. 27)

Na druhé straně, u přijemce, pak dochází k ověření podpisu dat, které probíhá dle schématu viz Obrázek 7.



Obrázek 7: Ověření digitálního podpisu příjemcem

Zdroj: Vlastní zpracování dle (1 str. 28)

Dešifrování u přijemce začíná přiloženým elektronickým podpisem pomocí dostupného veřejného klíče odesílatele, čímž je získán původní otisk vstupních dat

vypočtený na odesílatelově straně. Následně si přijemce vypočítá dle dokumentu svůj otisk za použití stejné hashovací funkce. Posledním krokem je porovnání otisků. V případě, že se otisky shodují, může být příjemce ujištěn o tom, že: (1 str. 27)

- dokument byl odeslán skutečně odesílatelem, jelikož nikdo jiný nemá přístup k soukromému kliči, který je příslušný k odesílatelově veřejnému klíči.
- dokument zároveň nikdo nemohl modifikovat, což dokazuje shoda vypočtených otisků.

Díky elektronickému podpisu je možné nejen identifikovat osobu podepisující dokument, ale i zjistit, zda byl dokument po podepsání modifikován. Další výhodou je, že pro jiný dokument se vygeneruje vždy jiný elektronický podpis, jelikož se pokaždé vypočte různý otisk. Není proto možné elektronický podpis na jednom dokumentu přenést do druhého dokumentu, jelikož zde by byl při ověřování označen jako neplatný. (1 str. 27)

Podpisové algoritmy se označují názvy ve tvaru například SHA256withRSA. Příklad je založený na kryptografickém algoritmu RSA, kde je na otisk využita hashovací funkce s označením SHA-256. (1 str. 27)

3.3 Komunikační protokoly

Komunikační protokoly definují jasná pravidla probíhající elektronické komunikace. Mezi základní parametry protokolů patří: (4 str. 85)

- používáné šifrování,
- samotný proces navázání a ukončení komunikace,
- nalezení a případná oprava chyb během komunikace,
- vlastnosti hardwaru pro fyzické spojení.

Nejvíce využívaným komunikačním protokolem na internetu je skupina protokolů TCP/IP a taktéž aplikační protokoly, jako například HTTP, POP3, FTP, SMTP, IMAP, atd. Většina z uvedených protokolů taktéž umí komunikovat zabezpečeným šifrovaným spojením. (4 str. 85)

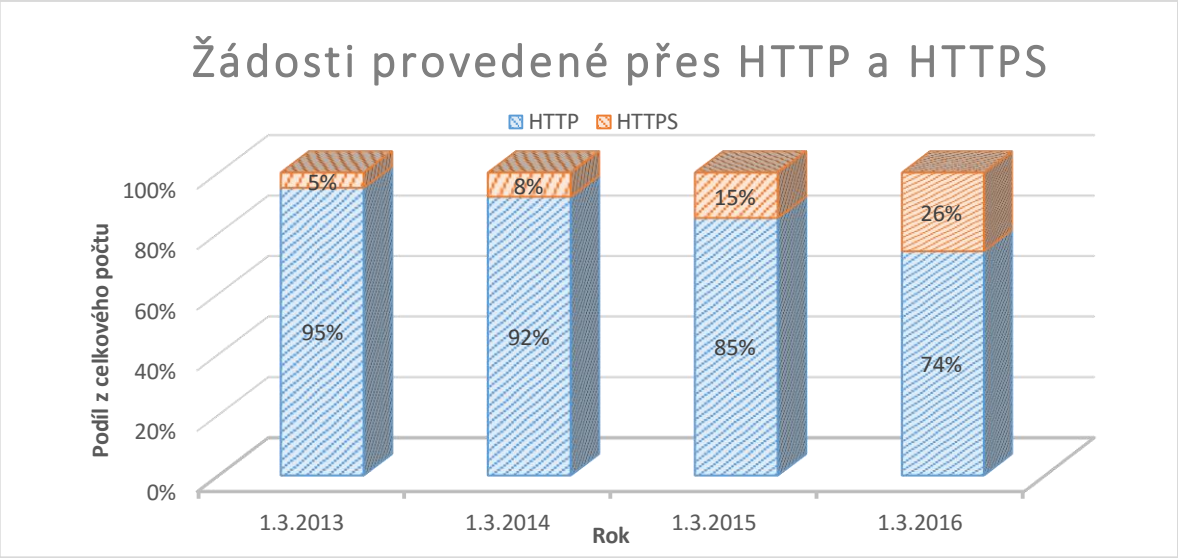
3.3.1 HTTPS

Pod tímto názvem se skrývá protokol HTTP (Hypertext Transfer Protocol), který je však zabezpečen pomocí TLS. HTTPS (Hypertext Transfer Protocol Secure) je tedy označení pro „HTTP over TLS“ a je synonem pro „bezpečný web“. Síťový port serveru 443 se všeobecně využívá pro HTTPS. (1 str. 411)

Samotné HTTP není totiž chráněné před sledováním, odposloucháváním či změnou obsahu, proto se tyto problémy řeší pomocí HTTPS, který šifruje data mezi klientem a serverem. Před zahájením spojení si obě strany vygenerují klíče a navzájem si prohodí své veřejné klíče, které následně ověřují. Ověření probíhá díky otisku veřejného klíče, který ovšem digitálně podepsala důvěryhodná certifikační autorita. (1 str. 411)

Existují útoky na HTTPS, které se snaží komunikaci degradovat na HTTP. Tento problém se řeší HTTP hlavičkami HSTS (HTTP Strict Transport Security) a HPKP (HTTP Public Key Pinning). HSTS je bezpečnostní funkce, která webové stránce umožňuje oznámit prohlížeči, na kterých místech webové stránky musí být použita komunikace výhradě protokolem HTTPS. HPKP je bezpečnostní mechanismus, který určuje, jaký certifikát musí být v cestě a kterému tak lze důvěřovat. (16) (17)

Dle stránky httparchive.org, která sbírá data z nejlepšího milionu webových stránek, bylo k 1. 3. 2015 (Graf 1) provedeno celkem 15 % žádostí přes protokol HTTPS. V letošním roce 2016 je udávaný počet 26 %, což je oproti minulému roku nárůst o více než 70 %. (18)



Graf 1: Procento provedených žádostí přes HTTP a HTTPS

Zdroj: Vlastní zpracování dle (18)

3.3.2 SSL/TLS

Verze SSL/TLS

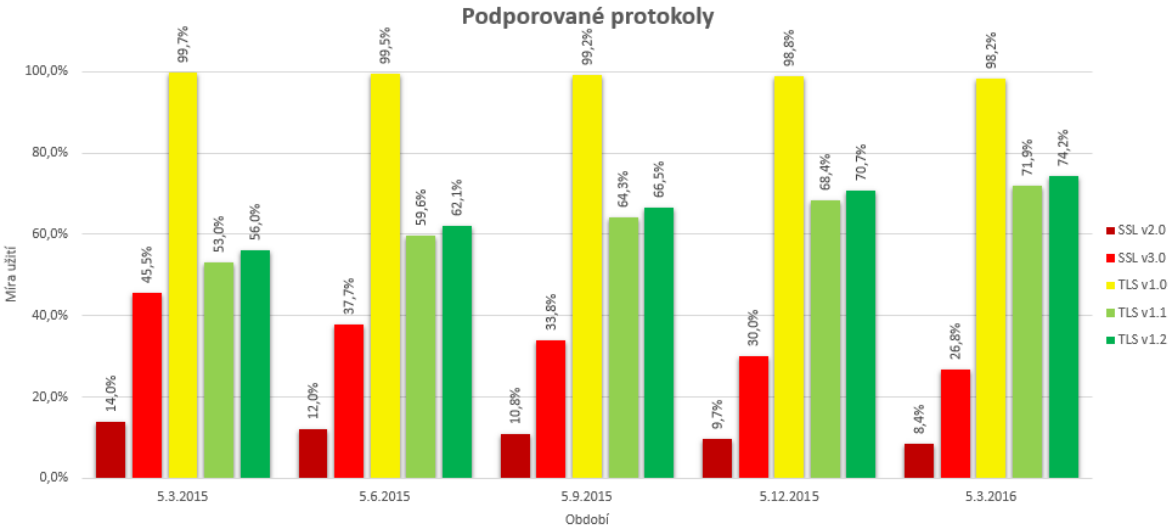
SSL (Secure Sockets Layer) byl vytvořen společností Netscape s cílem zabezpečit komunikaci mezi dvěma stranami. Verze SSL 1.0 nebyla nikdy veřejně představena. Až v roce 1995 byla uvolněna verze SSL 2.0 obsahující mnoho chyb a proto v roce 2011 byla zakázaná (RFC 6176). Protokol čekalo kompletní přepracování a tak v roce 1996 vzniklo SSL 3.0. Od roku 2014 byla tato verze považována za nespolehlivou, jelikož byla bezbranná vůči některým útokům, a od června 2015 je již považována za zastaralou (RFC 7568). (14)

V roce 1999 se jako zdokonalení verze SSL 3.0 měla objevit verze SSL 3.1, jenže vývojáři Christopher Allen a Tim Dierks požadovali, aby byl protokol šířen jako „otevřený a volný“, čímž by se dostali do právnických sporů se společností Netscape. Proto přejmenovali protokol na TLS 1.0 (Transport Layer Security). TLS zajišťuje šifrování, autentizaci a i tedy bezpečný tunel pro přenos dat. Protokol se také využívá nejen u komunikace využívající spojované služby (například TCP protokol), ale i v rámci zabezpečení linkové vrstvy (protokol EAP-TLS – využívaný pro autentizaci v bezdrátové síti). Existují však některé útoky využívající kompatibility tohoto protokolu se SSL, které degradují protokol TLS na SSL a tím se dostávají na zastaralý SSL. (1 str. 381) (14)

V dubnu 2006 byl definován TLS 1.1, který přinesl další vylepšení například proti útoku řetězení šifrových bloků. V sprnu 2008 byl vydán TLS 1.2, který je aktuální, ruší

kompatibilitu se SSL a zároveň z verze byly odstraněny některé nebezpečné šifrovací algoritmy. V lednu 2016 byl navržen TLS 1.3, jehož hlavním účelem bude odstranit zastaralé standardy. (14)

Dle dat z projektu SSL Pulse, který zkoumá technické informace z nejlepšího milionu webových stránek, získané 5. 3. 2016 (Graf 2) je nejčastěji podporován protokol TLS 1.0 (98,2 %). Zarážejícím je ale fakt, že některé stránky ještě stále podporují i zastaralé a nebezpečné SSL 2.0 (8,4 %) a SSL 3.0 (26,8 %). (19)



Graf 2: Podporované protokoly v top miliónu webových stránek

Zdroj: Vlastní zpracování dle (19)

Princip TLS

Protokol TLS je mezivrstva, která je vložena mezi protokol TCP (Transmission Control Protocol) a aplikační protokol (Obrázek 8). Vrstva TLS nemá na starosti rozpoznání, o jaké data se jedná, jejím úkolem je zabezpečení a zaslání dat dále protokolu TCP. Protokol TLS je otevřený pro možné využití jakýmkoliv protokolem vyšší vrstvy. (1 str. 381)

Obrázek 8: Vložení TLS mezi aplikační protokol a protokol TCP

Zdroj: Vlastní zpracování dle (1)

Mezi hlavní úkoly protokolů TLS patří: (1 str. 381)

- autentizovat server i klienta pomocí jejich certifikátů.

- šifrovat přenášená data – počáteční výměna kryptografického materiálu proběhne za pomocí asymetrického šifrování, následný přenos dat probíhá přes symetrické šifrování.
- zajistit integritu přenášených dat – dle kryptografického kontrolního součtu.

Na začátku komunikace serveru s klientem probíhá tzv. TLS dialog, kdy se strany domluví na použitých kryptografických algoritmech, materiálu a proběhne autentizace. Následně se mezi nimi vytvoří tzv. TLS relace, kdy probíhá již zabezpečený přenos aplikačních dat. V případě obnovování relace je již úvodní dialog mezi oběma stranami jednodušší a méně naročný. (1 str. 382)

Jelikož je protokol TCP duplexním spojením, vytváří dva kanály pro spojení – jeden pro tok dat mezi klientem a serverem a druhý naopak, mezi serverem a klientem. Protokol TLS proto musí zabezpečovat každý komunikační kanál zvlášť s pomocí jiného kryptografického materiálu. TLS protokol je složen ze dvou subprotokolů (Příloha B): (1 str. 383)

Record Layer Protocol (RLP) – má na starosti převzetí dat z aplikačních protokolů a jejich zašifrování, dále z nich počítá kontrolní kryptografický součet. Druhá strana komunikace použitím stejného protokolu uskuteční dešifrování dat, ověření kontrolního kryptografického součinu a následné odeslání dat aplikačnímu protokolu. (1 str. 383) (20 str. 87)

Handshake Protocol (HP) – protokol se aktivuje bezprostředně po navázání TCP komunikace, případně dle potřeby i během komunikace, a má na starosti navázat šifrovanou a autentizovanou komunikaci mezi oběma stranami. Obě strany se tak domlouvají na použití kryptografických algoritmů i na kryptografickém materiálu (sdílená tajemství a šifrovací klíče). Protokol dále využívá další dva protokoly: (1 str. 383) (20 str. 94)

- **Change Cipher Specification Protocol (CCSP)** – jeho úkolem je pouze odesílání zprávy z protokolu HP do protokolu RLP s informací o nastavení nových kryptografických parametrů. (20 str. 117)
- **Alert Protocol (AP)** – v případě problému v komunikaci podává informace s varováním či chybami. (20 str. 118)

Podrobný popis využití protokolů je uveden viz Příloha C.

3.4 Certifikační autority

Certifikační autorita patří mezi nezávislou třetí stranu, jejíž úkolem je vydávat certifikáty. Toto pojmenování lze použít buď pro označení aplikace vydávající certifikáty anebo pro pojmenování samotné instituce, která proces vydávání zajišťuje. V případě instituce se pak může jednat o celou firmu, která se tímto zabývá, nebo pouze o její část, tedy nějaké samostatné oddělení společnosti. V zákonech a vyhláškách se ovšem používá termín poskytovatel certifikačních služeb. Jejím největším bohatstvím je privátní klíč. V případě jeho zcizení je kompromitován celý strom podřízených autorit a vydaných certifikátů. (1 str. 76) (21 str. 42)

Certifikační autoritu jako instituci lze rozdělit na dvě části: (1 str. 76)

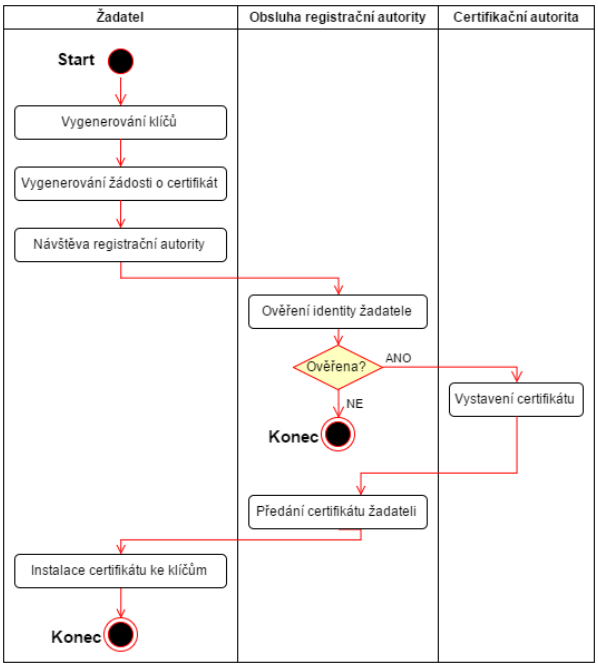
- **registrační autoritu** – jedná se o místo, kam žadatelé přicházejí se svými žádostmi o certifikát a poté se dostavují pro vydaný certifikát. Toto pracoviště si lze představit jako bankovní přepážku s lidskou obsluhou.
- **certifikační autoritu** – vnímána jako aplikace, která běží na serveru a jejímž úkolem je přijímat žádosti o vydání certifikátů z registračních autorit a vydávat certifikáty elektronicky podepsané soukromým klíčem certifikační autority.

3.4.1 Činnost certifikační autority

Certifikační autorita má za úkol vydávat digitální certifikáty představující digitálně podepsaný veřejný šifrovací klíč, jehož obsahem jsou samotné identifikační údaje držitele. Vystavením certifikátu držiteli se certifikační autorita zaručila, že ověřila správnost uvedených údajů. Díky principu přenosu důvěry tak lze důvěřovat informacím uvedených na digitálním certifikátu, ovšem za podmínky, že lze věřit samotné certifikační autoritě. (1 str. 77)

Zároveň certifikační autorita má na starosti udržovat databázi držitelů, auditní záznamy její činnosti, archív vystavených certifikátů a seznam odvolaných certifikátů. Zároveň autority vydávají pro jednotlivé typy certifikátů dokument certifikační politiky. V dokumentu lze nálezt informace o způsobu vydání certifikátu, použití, další správu, akceptaci, zneplatnění, ukončení platnosti a další činnosti s párovými daty. (1 str. 77)

3.4.2 Proces vydání a použití certifikátu



Obrázek 9: Diagram aktivit procesu žádosti o certifikát

Zdroj: Vlastní zpracování dle (22)

Jak lze vidět z diagramu aktivit (Obrázek 9), proces začíná tím, že si žadatel vygeneruje RSA klíče, tzn. vytvoří si soukromý a veřejný klíč. Následně vyplní žádost o certifikát, se kterou se musí dostavit na registrační autoritu, kde je poté ověřována jeho identita. (22)

Pokud se jedná o právnickou osobu, je potřeba předložit:

- občanský průkaz či cestovní pas,
- dokument dokládající existenci společnosti,
- dokument opravňující k jednání za společnost.

Fyzickým nepodnikajícím osobám postačuje k ověření pouze občanský průkaz nebo cestovní pas. Dle doložených dokladů se ověřuje správnost uvedených údajů na žádosti a předání žádosti certifikační autoritě. Ta na základě informací z žádosti vydá samotný certifikát a registrační autorita jej žadateli předá. Posledním krokem je samotná žadatelova instalace vystaveného certifikátu k vygenerovaným klíčům. (1) (22)

3.4.3 Hierarchie certifikačních autorit

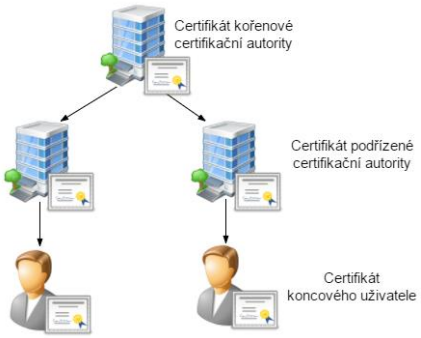
Certifikát koncového uživatele je ověřen soukromým klíčem certifikační autority, tedy uživatelský certifikát je podřízen certifikátu autority. V tomto případě si autorita vystavila certifikát sama sobě a jedná se o tzv. self-signed certifikát, tedy že podepsání

certifikátu lze ověřit veřejným klíčem té samé autority. V hierarchii (Obrázek 10) tedy neexistuje již žádný nadřazený certifikát, a proto se certifikát autority označuje jako kořenový. Z údajů uvedených na uživatelském certifikátu lze určit samotnou certifikační cestu přímo ke kořenovému certifikátu. (1 stránky 95–105) (21 stránky 44–46)

Obrázek 10: Jednoúrovňová hierarchie certifikační autority

Zdroj: Vlastní zpracování dle (1 str. 95)

Ve skutečnosti jsou certifikační autority vnitřně členěny a vznikají tak složitější struktury. Používá se proto členění na kořenové a podřízené certifikační autority, kdy kořenové mohou vydávat certifikáty i více podřízeným a teprve samotná podřízená autorita vystavuje různé druhy certifikátů koncovým uživatelům. Tím vzniká strom certifikačních autorit (Obrázek 11). (1 stránky 95–105) (21 stránky 44–46)



Obrázek 11: Strom certifikačních autorit

Zdroj: Vlastní zpracování dle (1 str. 98)

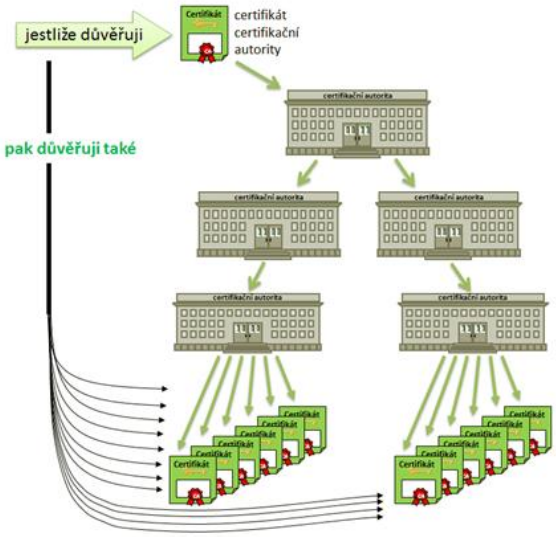
3.4.4 Důvěryhodnost certifikátu a certifikační autority

Mezi nejvýznamnější atributy digitálního certifikátu patří jeho důvěryhodnost, neboli jak moc lze věřit informacím na něm uvedeným. Důvěryhodnost lze posuzovat pro každý certifikát zvlášť na základě informací, kterém o něm uživatel má. Ovšem v praxi by tento postup nebyl přiliš účinný, jelikož lze těžko lze získat důvěryhodné informace o všech certifikátech. (1 stránky 95–105) (21 stránky 46–53)

Je proto potřeba důvěryhodný prostředník, od kterého by uživatel přebíral různé certifikáty a zároveň by ručil za jejich pravost. Prostředníkem by měla být samotná

certikační autorita. Mezi certifikáty a certifikačními autority zároveň platí tzv. přenos důvěry. Jakmile uživatel důvěřuje konkrétní certifikační autoritě, zároveň může důvěřovat i veškerým certifikátům, které byly vydány touto autoritou. Důvěryhodnost se nevztahuje přímo na certifikační autoritu, ale na její certifikát, kterým podepisuje vydané certifikáty konečným uživatelům. (1 stránky 95–105) (21 stránky 46–53)

Důvěru je možné dále předávat. V případě, že uživatel vyjádří důvěryhodnost v jednu certifikační autoritu, která vyjádřila důvěru v další certifikační autority, znamená to, že i uživatel může důvěřovat i těmto dalším certifikačním autoritám. Celá situace se dá představit jako strom důvěry (Obrázek 12), kdy jeho kořenem je právě jeden kořenový certifikát certifikační autority a od něj postupuje důvěra mezi další podřízené certifikáty autorit až k samotným certifikátům koncových uživatelů. Hlavním cílem přenosu důvěry je zjednodušení vyjádření důvěryhodnosti. Uživateli tedy stačí označit kořenový certifikát jako důvěryhodný a tím vyjadřuje svou důvěru i celému stromu. (1 stránky 95–105) (21 stránky 46–53)



Obrázek 12: Strom důvěry

Zdroj: (21 str. 49)

Ve skutečnosti, při existenci několika různých certifikačních autorit, vzniká i několik stromů důvěry, kde každý vlastní svůj kořenový certifikát. Celý systém se pak označuje jako infrastruktura veřejného klíče (PKI – Public Key Infrastructure), jejímž úkolem je zajištění důvěryhodného systému pro distribuci veřejných klíčů, které jsou obsaženy v certifikátech. (1 stránky 95–105) (21 stránky 46–53)

Vyjádření důvěry celým stromům či pouze jednomu certifikátu je vždy na samotném uživateli, a pokud se dopustí omylu, pak pouze on nese následky za svou chybu. Při vyjadřování důvěry certifikátu uživatel pracuje s třemi možnostmi: (21 str. 50)

- důvěryhodný certifikát,
- nedůvěryhodný certifikát,
- nedostatek informací k posouzení důvěryhodnosti certifikátu.

Způsob vyjádření důvěry jakémukoliv certifikátu vychází z konkrétního programu, který využívá daný certifikát. Každý program využívající certifikáty pracuje s úložištěm certifikátů. Některé aplikace mají přímo své úložiště, jiné zas využívají sdíleného. Úložiště má určitou vnitřní strukturu složek s daným významem. Důvěryhodnost certifikátu je určena právě jeho umístěním či nainstalováním do složky určitého významu. Pokud je tedy nějaký kořenový certifikát umístěn do složky pro důvěryhodné kořenové certifikační autority (Příloha D) je vyjádřena důvěra pro celý příslušný strom certifikátů. V případě, že certifikát není umístěn ani v jedné ze složek, program tak nemá podle čeho posoudit jeho důvěryhodnost a rozhodnutí nechá přímo na uživateli. (21 stránky 50–51)

Uživatel by měl vědět, kde nalezne úložiště k jednotlivým programům. Úložiště aplikací bývá autory předvyplněno takovými certifikáty, které považují za důvěryhodné. Uživatel má tak usnadněnou práci a hlavní důvěryhodné kořenové certifikační autority již má v úložišti obsažené. Ovšem seznam nemusí odpovídat jeho představám a mohou mu chybět další certifikáty, které on považuje za důvěryhodné. Proto by měl mít znalost, kam další důvěryhodné certifikáty umístit. (21 stránky 50–51)

3.4.5 Vlastní certifikační autorita

Pokud si uživatel nevybral z nabízených služeb certifikační autorit a nepotřebuje kvalifikovaný certifikát, naskytuje se mu možnost vytvořit si vlastní certifikační autoritu, díky níž si následně může vydávat vlastní certifikáty. Na trhu je k nalezení několik dostupných možností: (1 str. 139)

- nechat si zřídit od kvalifikované certifikační autority vlastní registrační autoritu dle svých představ,
- využít některý z komerčních produktů,
- využít open source řešení.

Zřízení klientské registrační autority dle vlastních požadavků má ovšem význam pouze u firem, kde se vydávají certifikáty ve větším měřítku a je potřeba flexibility při

samotném vydávání. Zřízenou autoritu pak má uživatel sám ve správě a množství vydaných certifikátů není omezené. Řešení je spíše určené pro obchodní společnosti, školství či bankovní instituce. (22)

Vlastní kořenová certifikační autorita

Vytvoření vlastní kořenové certifikační autority vychází z kořenového certifikátu, který je podepsán sám sebou (self-signed). Mezi výhody tohoto řešení lze zařadit hlavně nezávislost na nadřízených certifikačních autoritách, jelikož není potřeba podpisu nadřízené autority. Avšak mezi její hlavní nevýhody patří nedůvěryhodnost, jelikož samostatně vytvořená kořenová certifikační autorita nemá možnost se dostat do důvěryhodných úložišť operačních systémů či webových prohlížečů pro kořenové certifikáty autorit. Každý uživatel, který bude využívat některý z vydaných certifikátů této autority, tak nejprve musí kořenový certifikát zdůvěryhodnit. Avšak v situaci, kdy přijde cizí uživatel, který kořenovou autoritu nezná a nebude ji důvěřovat, se pak nedostane k obsahu šifrované komunikace. (1)

Vlastní podřízená certifikační autorita

Podřízená autorita vychází z předpokladu, že nadřízená autorita ji ověřila a svým certifikátem podepsala. Pokud je nadřízená autorita zařazená do seznamu důvěryhodných autorit, pak je i podřízená autorita důvěryhodná. Mezi další výhody lze zařadit, že nadřízená autorita je zodpovědná za vydání chybného certifikátu a případně i vzniku škody. Avšak podřízená autorita musí dodržovat podmínky stanovené nadřízenou autoritou, mezi které se řadí například technická bezpečnost, proces ověření identity žadatele, atd. Řešení je podmíněno pořizovací cenou, kterou požaduje vydávající nadřízená certifikační autorita. (1)

Klientská certifikační autorita

Služba je vhodná pro zákazníky, kteří nedisponují příslušnými znalostmi a potřebují certifikační autoritu dle svých požadavků. Řešení většinou obsahuje jak technické, tak softwarové prostředky. Jakmile je řešení nasazené a řádně otestováné je předáno zákazníkovi, který již může spravovat certifikační autoritu. Může tedy přijímat žádosti o certifikáty, ověřovat údaje na žádosti, kontrolovat identitu žadatele, vydávat certifikáty, udržovat seznam vystavených certifikátu, zneplatňovat certifikáty a také udržovat databázi zneplatněných certifikátů. (22)

Řešení umožňuje i uvedená První certifikační autorita, a.s., která poskytuje jak speciální software z vlastní produkce, tak i technické prostředky – server. V jejich ceníku

není uvedená částka, ovšem po dotázání jejich podpory bylo uvedeno, že cena za pronájem této služby činí od 3 000 Kč/měsíc, v případě přímé koupě se cena pohybuje od 61 200 Kč. (22)

Využití komerčního produktu

Realizace certifikační autority je možná i pomocí některých komerčních produktů například od společnosti Entrust, VeriSign, SimpleAuthority atd. Jelikož se jedná o finančně nákladné řešení, je určeno spíše pro velké společnosti, které upřednostňují zabezpečení a vysokou úrovní spolehlivosti před samotnou cenou. (1) (23)

Komerční produkty poskytují moduly, které umožňují spravovat digitální identity uživatelů, životní cyklus certifikátu, automatizovat správu párových klíču, řidit proces registrování, ověřovat žádosti o certifikát, archivovat a obnovovat uživatelské klíče. (1)

Využití řešení od Microsoftu

Operační systém Windows Server 2008 od společnosti Microsoft nabízí certifikační autoritu, která je označena jako Active Directory Certificate Services (AD CS). Kromě standardních funkcí, které poskytuje každá vlastní certifikační autorita jako je vydávání certifikátů, jejich odvolání, atd., nabízí toto řešení i další možnosti. Mezi ně lze zařadit archivaci privátních klíčů v databázi autority, automatické vydávání certifikátů pro počítače a uživatele, definování šablon certifikátů či pomocí jednoduché webové stránky vytváření žádostí o certifikáty, které jsou následně odeslány do správce certifikační autority. (24)

Využití open source řešení

OpenSSL je výsledkem společného úsílí, jehož cílem bylo vyvinout silný a plně vybavený open source nástroj. Řešení tak nabízí implementaci protokolů SSL a TLS pomocí knihoven naprogramovaných jazykem C, které lze využívat i v jiných programovacích jazycích, a jejichž obsahem jsou základní šifrovací funkce. Projekt je spravován celosvětovou komunitou dobrovolníků, kteří vzájemně komunikují, plánují rozvoj tohoto nástroje a vydávají související dokumentaci. Za předpokladu splnění podmínek uvedených v licenci lze nástroj využít jak ke komerčním, tak k nekomerčním účelům a to na všech dostupných operačních systémech. (25)

Nástroj lze používat jednak v příkazové řádce jako utilitu, anebo jako knihovnu do další aplikace. Takový je například volně dostupný program XCA (X Certificate and Key

Management), jehož jádrem je právě kryptografická knihovna OpenSSL. Aplikace se ovládá pomocí přehledného uživatelského grafického rozhraní. (26)

3.5 Digitální certifikát

Certifikát bývá často přirovnáván k občanskéhu průkazu či pasu, který je vydáván v tištěné podobě. Zatímco digitální certifikát je podepsaná datová struktura s veřejným klíčem držitele certifikátu, kde právě veřejný klíč je jeho základní součástí. (1 str. 58)

3.5.1 Účel certifikátů

Asymetrická kryptografie vytváří jednu závažnou překážku – jakou použít bezpečnou cestu pro předání svého veřejného klíče druhé straně, aniž by měla obavy o jeho nepravosti. Když útočník napadne komunikační cestu a podaří se mu ji ovládnout, pak toho může snadno využít a zaměnit svůj klíč za původní předávaný veřejný klíč a tím vlastně změnit svoji identitu. Tento útok se nazývá „man in the middle“, kdy si oběť útoku myslí, že má k dispozici veřejný klíč od protistrany a chce s ním zašifrovat data, ovšem útočník veřejné klíče zaměnil, takže data jsou šifrována jeho klíčem. Následně útočník snadno odchytí zašifrovaná odeslaná data a pomocí svého soukromého klíče je jednoduše dešifruje, přečte si je a poté data opět zašifruje, ale tentokrát původním veřejným klíčem a odešle je té straně, které byla data určená. Ta tak nemá žádné podezření. Útočník dokonce v některých případech může data jakkoliv modifikovat, pokud zašifrovaná data nejsou podepsána. (1 stránky 53–58) (12 str. 266)

Veřejný klíč může být předáván důvěryhodným způsobem. Za tímto účelem zde existují certifikáty, které ve své datové struktuře obsahují identifikační údaje o vlastníkovi spolu s veřejným klíčem. Ovšem takové údaje na certifikát by si mohl každý vymyslet, a proto je nutné, aby o vydání certifikátu zažádal vlastník veřejného klíče třetí stranu, certifikační autoritu, která z něj dělá důvěryhodný způsob předávání informací. (1 stránky 53–58)

3.5.2 Obsah certifikátu

Jednotlivé údaje certifikátu lze připodobnit k občanskému průkazu (viz Tabulka 2). Toto porovnání je i součástí pracovních úkolů zaměstnanců registrační autority, kteří musí ověřovat totožnost žadatele o certifikát. (1 str. 58)

Údaj na certifikátu	Údaj na občanském průkazu
Verze (Version)	Verze občanského průkazu
Pořadové číslo (Serial number)	Číslo občanského průkazu
Podpisový algoritmus (Signature algorithm)	Typy ochranných prvků, způsob podpisu úředníka
Vydavatel (Issuer)	Vydal
Platnost (Validity)	Platnost
Předmět: jméno, adresa, … (Subject)	Jméno a adresa
Veřejný klíč (Public key)	–
–	Fotografie
Rozšíření certifikátu (Extension)	Nepovinné údaje
Digitální podpis (Digital signature)	Vlastnoruční podpis, aplikace ochranných prvků

Tabulka 2: Srovnání obsahu certifikátu a občanského průkazu

Zdroj: Vlastní zpracování dle (1 str. 59)

Norma X.509

Existuje několik norem, které definují samotnou strukturu certifikátu, jsou to X.509, WAP, EDI, atd. Na internetu se ovšem vychází ze standardu vydaném ITU (International Telecommunication Union) a to X.509 verze 3, kdy je vytvořen i internetový profil standardu X.509 v příslušném RFC (Request for Comments), který je dnes standardem RFC-5280. Byl vydán v roce 1988 a postupem času je vývojem doplňován. (1 str. 59)

Norma má také na starosti formát uloženého certifikátu, a jaké konkrétní položky budou tvořit jeho strukturu, apod. Nejfrekventovanějšími příponami pro certifikáty jsou: (1)

- .PEM – certifikát je zakódovaný base64, jeho obsahem můžou být i privátní klíče,
- .DER – certifikát je zakódovaný,
- .P12, .PFX – obsahem jsou privátní, veřejné klíče a certifikáty jsou pod ochranou hesla,
- .P7B, .P7C – obsahem jsou listy odvolaných certifikátů nebo samotné certifikáty.

V následujících subkapitolách jsou uvedeny základní položky struktury digitálního certifikátu. U každé položky je taktéž naznačen příklad exportovaný z reálného certifikátu staženého dne 22. 1. 2016 ze školních stránek is.czu.cz, který byl zobrazen pomocí příkazu `certutil -dump certifikat_is_czu.cer` v příkazové řádce operačního systému Windows 7. Snímek výpisu příkazové řádky zobrazuje Příloha E.

Verze certifikátu je uváděná jako číselná hodnota snížená o 1, tzn. pro verzi 1 se uvádí 0, či pro verzi 2 pak 1. V případě, že je certifikát ve verzi 1, je možné pole vynechat. Jako aktuální verze se používá číslo 3, což dokazuje i školní certifikát: (1 str. 60)

```
Verze: 3
```

Sériovým číslem musí být celé číslo, které je kladné a unikátní pro každý certifikát vydaný totožnou certifikační autoritou. Kombinace sériového čísla a jména certifikační autory slouží k jednoznačné identifikaci každého certifikátu. Číslo může být velice obsáhlé, ovšem nesmí překročit velikost 20 bajtů a může být zadáno v decimálním, ale i hexadecimálním tvaru, jak dokazuje skutečný příklad: (1 str. 60)

```
Sériové číslo: b85c4fa5e16b4809a09f34ce984933c5
```

Subjekt obsahuje jméno toho, komu byl certifikán vystaven a zároveň jednoznačně identifikuje držitele tohoto certifikátu. V případě, že držitel vlastní více certifikátů od stejné certifikační autority, pak se jednotlivé certifikáty, pro dodržení unikátnosti, odlišují právě sériovým číslem. Pole je vyplněno podle podané žádosti o certifikát. Pole Subjekt a Vystavitel využívají pro uložení informací datový formát, který se označuje jako jedinečné jméno (Distinguished Name), viz Tabulka 3. (1 str. 63)

Zkratka	Atribut	Význam
C	Country	Zkratka státu podle ISO 3166. Stejná norma se využívá pro top level domény DNS (Česká republika = CZ, atd.)
CN	Common Name	Název objektu, pod kterým je v místě znám. U osob se může jednat o jméno a příjmení, u serverů pak o jméno DNS.
E	Email Address	E-mailová adresa
L	Locality	Místo (například město)
O	Organization	Název organizace
OU	Organization Unit	Název části organizace
SP	State or Province	Nižší organizační jednotka státu, například kraj

Tabulka 3: Vybrané položky u jedinečných jmén

Zdroj: (1 str. 62)

```
Subjekt:
    CN=is.czu.cz
    OU=Domain Control Validated
```

Položka Vystavitel obsahuje informaci o jméně vydavatelské ceritifikační autority. Jméno by mělo splňovat podmínku unikátnosti v rámci všech společností, zabývající se stejnými požadavky. Certifikační autorita by své jméno měla důkladně zvážit, aby později nevznikla nutnost ho změnit, jelikož tím by se vytvořila nová nezávislá autorita. (1 str. 63)

```
Vystavitel:
    CN=TERENA SSL CA 2
    O=TERENA
    L=Amsterdam
    S=Noord-Holland
    C=NL
```

Pole Algoritmus podpisu obsahuje informaci o identifikátoru kryptografického algoritmu a jeho parametru použitém jako podpis daného certifikátu. Položka obsahuje dvě části – identifikátor algoritmu a jeho parametry. (1 str. 60)

```
Algoritmus podpisu:
    OID algoritmu: 1.2.840.113549.1.1.11 sha256RSA
    Parametry algoritmu: 05 00
```

Položka doba platnosti obsahuje informaci o časovém intervalu, po který je certifikát platný a certifikační autorita se tudíž zaručuje za jeho obsah. V položce lze najít datum a čas, před kterým certifikát není platný pod názvem „Neplatí před“ a dále datum a čas, po kterém certifikát již není taktéž platný pod označením „Neplatí po“. Data jsou uvedená v UTC (Coordinated Universal Time). (1 str. 60)

Doba platnosti certifikátu je omezena ze dvou důvodů, jednak z organizační stránky – kdy aplikace má taky pouze určitou životnost a jednak z bezpečnostní stránky – životnost certifikátu by neměla být delší, než doba, za kterou je možné prolomit certifikovaný veřejný klíč. (1 str. 60)

```
Neplatí před: 16.6.2015 1:00
Neplatí po: 16.6.2018 0:59
```

Položka Použití klíče určuje, k jakému způsobu je možné využít certifikovaný veřejný klíč a tím omezit jeho použití. Každý způsob použití obsahuje bit a v případě, že hodnota bitu v bitovém řetězci je 1, pak je klíč možné použít pro konkrétní způsob využití. Mezi způsoby patří: (1 str. 64)

- verifikace digitálně podepsaných dat,

- digitální podpis,
- šifrování klíče,
- šifrování jiných uživatelských dat,
- algoritmy na výměnu klíčů,
- podepisování certifikátů,
- podepisování seznamu odvolaných certifikátů,
- šifrování,
- dešifrování.

```
Použití klíče
```

```
    Digitální podpis, Šifrování klíče (a0)
```

Pole Veřejný klíč obsahuje informace o identifikátoru algoritmu určeného pro veřejný klíč a také konkrétní veřejný klíč, který je s certifikátem spojen. Bitová velikost veřejného klíče je závislá na typu zvoleného šifrování. Příklad z existujícího certifikátu zobrazuje snímek příkazové řádky, viz Příloha E. (1 str. 64)

3.5.3 Rozšíření certifikátu

Informace, které se nevejdou do předchozích položek certifikátu, jsou uloženy v některém z rozšíření. Certifikát by ovšem neměl na druhou stranu obsahovat příliš mnoho informací, které pak mohou být i zbytečnými. Mezi hlavní zásady proto patří, že certifikát by měl obsahovat pouze údaje týkající se identifikace držitele certifikátu. (1 str. 64)

Rozšíření certifikátu je definováno zcela obecně. Vyskytuje se problém, že některým položkám v rozšíření nemusí aplikace rozumět. Proto u každého rozšíření existuje atribut závažnosti a v případě, že její hodnota je rovna 1, pak je označená jako závažná. (1 str. 64)

Aplikace, která využívá certifikáty, pak musí rozumět všem závažným rozšířením certifikátu a musí si být vědoma, že v těchto místech jsou uloženy závažné informace. Pokud je některá z položek označená jako závažná a aplikace neví, k čemu takovouto informaci využít, je povinna celý certifikát odmítnout. (1 str. 64)

Standard RFC-5280 definuje seznam rozšíření, který zobrazuje Příloha F. Některé položky rozšíření jsou k nalezení i na výpisu certifikátu is.czu.cz z příkazové řádky, viz Příloha E.

3.5.4 Druhy certifikátů

Hlavní rozdělení certifikátů je na komerční a kvalifikované. Zatímco komerční nejsou zákonem nijak upraveny, kvalifikované mohou být vydávány pouze akreditovanými certifikačními autoritami. Dále se využívají komerční serverové certifikáty a kvalifikované osobní certifikáty. Komerční je možné rozlišit dle úrovně ověření certifikátu. (21 str. 124)

Komerční

Komerční certifikáty se řadí mezi ty nejrozšířenější, jelikož na tento druh není kladen žádný požadavek ze strany zákona o elektronickém podpisu. Certifikáty vystavuje certifikační autorita, a jelikož nemusí být dodržovány požadavky ze zákona, autorita si sama stanovuje požadavky a ověřuje tak držitele s využitím svých směrnic. Pro využití komerčních certifikátů není omezena oblast, a proto nalézají velmi široké uplatnění. Mezi nejčastější účely se řadí: (21 str. 125)

- ověřování elektronického podpisu,
- šifrování komunikace,
- autentizace uživatelů do informačního systému.

Jelikož komerční certifikáty neposkytují legislativní záruky, mezi důležité součásti patří důvěryhodnost komunikující strany certifikátu, který byl vydán konkrétní certifikační autoritou. Tento druh certifikátu může být poskytnut jednak osobám, ale i technologicky zaměřeným celkům, mezi které se řadí aplikace, servery a ostatní zařízení. (21 str. 125)

Kvalifikovaný osobní certifikát

Tento druh certifikátů mohou vystavovat pouze akreditované kvalifikované certifikační autority, které se musí řídit zákonem o elektronickém podpisu § 12 zákona č. 227/2000 Sb. a jsou často kontrolovány jejich bezpečnostní pravidla i samotná důvěryhodnost. Dle uvedeného zákona nalezly certifikáty využití i v prostředí komunikace se samotnými státními institucemi České republiky. Měly by tedy být akceptovány stejným způsobem, jako například občanské průkazy a vydávány pouze fyzickým osobám, ovšem v současné době je jejich využití značně omezeno na: (21 stránky 128–130)

- komunikaci se státní správou elektronickým způsobem,
- zajištění neodmítnutelnosti odpovědnosti,
- bezpečné ověření elektronických podpisů.

Kvalifikované certifikáty jsou určené pouze pro elektronické podepisování (tzn. držitel certifikátu by svůj soukromý klíč měl využít pouze pro podepisování dat) neboli kvalifikovaný certifikát zajišťuje autenticitu a integritu dat v rámci komunikace se subjekty státních institucí. Seznam certifikačních autorit, kterým byla udělena akreditace od Ministerstva vnitra ČR a staly se tak akreditovanými poskytovately certifikačních služeb, je dostupný na jejich webových stránkách[3]. (21 stránky 128–130)

Komerční serverový certifikát

Tento typ certifikátů je vystavován serverům a jeho úkolem je prokazovat, že organizace spravující daný server má skutečně právo jej provozovat. Certifikáty se ukládájí přímo na webové servery a dávají klientovi možnost ověřit identitu serveru. Klient tím získává pocit bezpečí, že komunikace probíhá s ověřeným serverem. Klient může být taktéž požádán webovým serverem o předložení certifikátu, kterým následně pomocí procesu autentizace ověří identitu dané strany. Tento sled kroků je možný díky existenci prokolu TLS. (21 stránky 123–124) (22)

O vydání serverového certifikátu mohou prostřednictvím elektronické žádosti, vytvořené většinou přímo konkrétním serverem, požádat nejen fyzické, ale i právnické osoby. U registrační autority je důležitý následný proces ověření totožnosti pomocí příslušných dokladů a poté samotné vydání certifikátu. (21 stránky 123–124) (22)

Kvalifikovaný systémový certifikát

Na rozdíl od kvalifikovaného osobního certifikátu si o tento druh certifikátu mohou žádat nejen fyzické osoby (nepodnikající i podnikající), ale i právnické osoby a organizační složky státu. Tento druh certifikátu má povolení vydávat dle zákona o elektronickém podpisu pouze kvalifikovaný poskytovatel certifikačních služeb – musí při tom splňovat požadavky dle § 12a tohoto zákona. Náležitosti v této části zákona se velice podobají těm uvedeným v § 12, které jsou určené pro kvalifikované certifikáty, ovšem podle prvního požadavku musí být certifikát označen, že je vydáván jako kvalifikovaný systémový certifikát. (22) (27)

Kvalifikované systémové certifikáty vznikly z potřeby elektronicky podepisovat velké množství zpráv, na které již nestačí schopnost člověka a navíc dle zákona by se

[3] Přehled udělených akreditací. *Ministerstvo vnitra České republiky* [online]. Odbor Hlavního architekta eGovernment, 2012 [cit. 2016-03-26]. Dostupné z: http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx

podepisující osoba vždy měla seznámit s obsahem, který podepisuje. Proto je vhodné tento proces zautomatizovat. Využívat se k tomu začalo místo elektronického podepisování elektronické označování. S tím souvisí i potřeba odlišit právní terminologii. Místo podepisování se používá termín označování a termín podepsané osoby se nahradil jako označující osoba. Jelikož označování se používá strojově, bez součinnosti fyzické osoby, je odstraněn i předpoklad, že označující osoba se seznámila s obsahem, který je právě označován. Značka je obsažena na elektronických fakturacích, hromadně zasílaných e-mailech či na výstupech z informačních systémů například z oblasti veřejné správy. (27) (28)

Doménové ověření (Domain Validation – DV)

Certifikát DV je cenově nejdostupnějším, jelikož samotné ověření probíhá pouze přes e-mail provozovaný na ověřované doméně. Certifikační autorita po dokončené objednávce odešle na uvedený e-mail odkaz pro ověření, který směřuje na portál autority. Žadatel po kliknutí na odkaz ověří vlastnictví domény a tím je proces ověřování dokončen. Velkou výhodou je proto rychlost získání certifikátu, která se pohybuje od 2 minut. (29)

Jedná se o základní stupeň ověření, kdy v detailu certifikátu není možnost zkontrolovat údaje o majiteli. Uvedená je pouze informace o doméně, pro kterou byl certifikát vydán a která byla e-mailem ověřena. Certifikát je proto využíván na projektech, kde je známý jeho provozovatel – například firemní systémy, intranet či menší webové projekty. (29)

Ověření organizace (Organization Validation – OV)

Tento druh ověření patří mezi nejpoužívanější stupeň, označuje se proto jako standardní. O ověření může žádat firma nebo organizace a ověření probíhá v několika krocích. Nejprve je ověřeno samotné vlastnictví domény stejně jako u certifikátu DV. Následně je potřeba ověřit existenci a registraci organice či podnikatele, a poté ještě pomocí krátkého telefonického hovoru ověřit žadatele. (29)

Vystavení certifikátu se většinou pohybuje od 2 pracovních dnů. Ve vydaném certifikátu OV jsou v detailu uvedeny ověřené údaje o majiteli. Certifikát je vhodný pro webové projekty, na které přicházejí návštěvníci z internetu, například firemní stránky, internetové obchody, atd. (29)

Rozšířené ověření (Extended Validation – EV)

Nejvyšší důvěryhodnost a úroveň ověření provozovatele představují certifikáty EV, které se od ostatních odlišují tím, že v prohlížeči se v adresním řádku navíc zobrazuje zelený pruh certifikátu EV (Obrázek 13) s informací o názvu ověřené společnosti. Ověření je složeno ze stejných kroků jako v případě certifikátu OV s tím rozdílem, že je přísnější a informace je potřeba doložit z více zdrojů. Nutné je také ověření osoby zastupující organizaci, která tento typ certifikátu požaduje. Mezi výhody tohoto řešení patří, že uživatelé více důvěřují takovým webovým stránkám, kde dokáží na první pohled identifikovat důvěryhodnost provozovatele. (29)

Obrázek 13: Zbarvení URL řádky v Firefox (vlevo) a Internet Explorer (vpravo)

Zdroj: Autor

Vystavení certifikátu se pohybuje od 5 pracovních dnů. Certifikáty EV v detailu obsahují ověřené informace o provozovateli a jsou vhodné například pro webové stránky bank, finančních instuticí, platebních bran a u dalších projektů, kde je kladen důraz na nejvyšší stupeň bezpečnosti. (29)

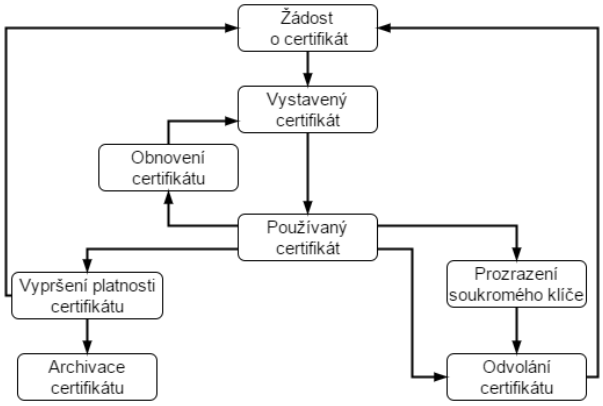
3.5.5 Kvalita certifikátů

Samotnou kvalitu certifikátů lze určit dle několika hledisek: (1 str. 107)

- **certifikační autorita** – její důvěryhodnost, dodržování zákona o elektronickém podpisu, zpětná vazba od zákazníků, atd.
- **chování a manipulace uživatele** – mezi nejslabší místa ověření certifikátu patří nedostačné proškolení uživatele, který může svou nedbalostí například vložit chybný kořenový certifikát, čímž se znehodnotí princip přenosu důvěry.
- **kryptografický algoritmus** – kvalitní a bezpečný algoritmus, jelikož se vzrůstajícím výkonem výpočetní techniky se snižuje odolnost používaných šifrovacích algoritmů. Je proto nutné stále zdokonalovat šifrovací způsoby a také nastavovat časově omezenou platnost digitálním certifikátům.

3.5.6 Životní cyklus

Životní cyklus certifikátu se skládá z několika stavů, které zobrazuje Obrázek 14, a poté jsou popsány v jednotlivých subkapitolách.



Obrázek 14: Životní cyklus certifikátu

Zdroj: Vlastní zpracování dle (30)

Žádost o certifikát

Vystavení certifikátu certifikační autoritou předchází podání žádosti o certifikát, do které by žadatel měl úvést následující náležitosti: (1 str. 79)

- své identifikační údaje – budou umístěny na vydaném certifikátu v položce předmět nebo jako alternativní jméno v možnosti rozšíření certifikátu.
- veřejný klíč – společně s identifikací asymetrického algoritmu, ke kterému je veřejný klíč určen.
- důkaz o držení soukromého klíče.
- některé další údaje, které chce mít v certifikátu uvedené (například použití klíče, rozšířené použití klíče atd.).
- v případě placeného vydání certifikátu je potřeba uvést údaje určené pro fakturaci.
- hesla důležitá pro autentizaci v případě spojení s certifikační autoritou – například v případě odcizení soukromého klíče a zadání jednorázového hesla pro odvolání certifikátu.

Důkaz o držení příslušného soukromého klíče je nejčastěji prováděn tak, že je proveden digitální podpis ze struktury obsahující veřejný klíč. Žádost o certifikát, která obsahuje důkaz o vlastnictví soukromého klíče s pomocí digitálního podpisu, se označuje jako CSR (Certfication Signing Request). (1 str. 80)

Nejpoužívanějším formátem pro žádost o certifikát je norma PKCS#10, která vychází z kořenového certifikátu, ovšem obsahem zůstala jen potřebná pole pro žádost o certifikát, a to: (1 str. 83)

- verze,
- předmět,
- veřejný klíč,
- atributy,
- elektronický podpis vykonaný soukromým klíčem žadatele.

V položce atributy jsou obsahem jednotlivé atributy anebo rozšíření, které chce žadatel mít uvedené na vydaném certifikátu. Ovšem záleží, jakou má certifikační autorita nastavenou certifikační politiku a jak s chtěnými rozšířenými údaji naloží. Jedním z atributů je také jednorázové heslo pro odvolání certifikátu, které se ve vydaném certifikátu neobjevuje. Formát PKCS#10 nelze využít v případech, kdy veřejný klíč nedovoluje ověřit digitální podpis anebo v situaci, kdy párová data generuje až oslovená certifikační autorita, tzn., že žadatel při podávání žádosti nemá párová data k dispozici. (1 str. 84)

Problémy formátu PKCS#10 řeší podstatně bohatší žádost označená jako CRMF (Certificate Request Message Format), která dovoluje k žádosti přidat i další údaje, jako třeba informace určené pro fakturaci. (1 str. 84)

Atypická žádost, která byla vytvořená firmou Netscape, je typ SPK. Formát byl určen pro vytvoření žádosti o certifikát s pomocí webové stránky. Byl proto zaveden i speciální HTML tag <KEYGEN>, který je součástí webového formuláře. Po jeho odeslání prohlížeč vygeneruje párové klíče, vytvoří digitální podpis veřejného klíče příslušným soukromým klíčem a vloží kódovaný veřejný klíč společně s digitálním podpisem jako obsah pole HTML stránky, která obsahuje tag KEYGEN. (1 str. 85)

CMC protokol je využíván v případě, kdy je potřeba, aby na žádosti o certifikát bylo uvedeno více podpisů, například jeden vytvořen klíčem žadatele a druhý podpis klíčem registrační autority. (1 str. 86)

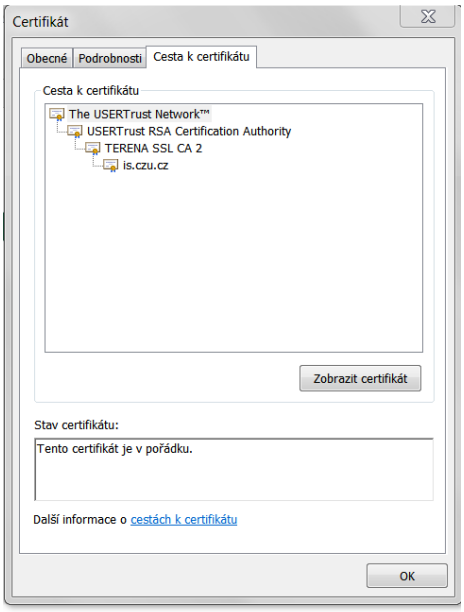
Vyplněná žádost o certifikát je následně poskytnuta certifikační autoritě, která má na starost ověřit vyplněné údaje a vydat samotný certifikát, který je obvykle vystavován ve formátech PEM, DER nebo TXT. Pokud je žádost schválena a certifikát úspěšně vydaný, certifikační autorita jej umístí do veřejného seznamu vydaných certifikátů, kde jsou k nalezení informace: (1 str. 79)

- sériové číslo certifikátu,
- obecné jméno (CN),
- platnost od,

- platnost do,
- certifikát ke stažení ve formátech DER, PEM a TXT,
- stav.

Ověřování platnosti certifikátu

Certifikát se musí ověřovat z toho důvodu, aby bylo možné zjistit, že uvedený platný veřejný klíč certifikátu je skutečně vlastněn držitelem uvedeným v předmětu certifikátu a že klíč je určen k uvedenému účelu. Pro ověření je nejprve nutné vytvořit certifikační cestu (viz Obrázek 15). Ta se vytváří od důvěryhodné kotvy, která bývá ve tvaru kořenového certifikátu a značí se jako certifikát číslo nula, až k samotnému ověřovanému certifikátu. Certifikát vystavený důvěryhodnou kotvou se nazývá jako první certifikát certifikační cesty, a dále certifikát vystavený prvním certifikátem se označuje jako druhý certifikát certifikační cesty, atd. (1 str. 107)



Obrázek 15: Certifikační cesta v případě certifikátu pro is.czu.cz

Zdroj: Vlastní zpracování

Z důvěryhodné kotvy se v rámci ověřování vezmou informace o jméně vydavatele a veřejném klíči společně s použitým algoritmem. Následně se při ověřování postupuje po certifikační cestě od prvního certifikátu až po ověřovaný a u každého se kontroluje: (1 str. 108)

- vydavatel daného certifikátu je předmětem předchozího certifikátu.
- daný certifikát je digitálně podepsán předchozím certifikátem.
- aktuální čas je v rozmezí platnosti certifikátu.

- certifikát nebyl odvolaný a nelze ho dohledat v seznamu odvolaných certifikátů.
- splněný účel použití certifikátu.

Ověření se také uskutečňuje použitím párování položek ze za sebou jdoucích certifikátů v certifikační cestě. Používá se buď shoda jedinečných jmen, kdy je z nadřízeného certifikátu porovnáván obsah položky Subjekt s obsahem položky Vystavitel z ověřovaného certifikátu. Avšak mezi významnější identifikátory se řadí tzv. shoda klíčů. V tomto případě se kontroluje otisk (nebo pouze část) veřejného klíče. U nadřízeného certifikátu se jedná o obsah položky Identifikátor klíče předmětu a u ověřovaného certifikátu pak o obsah položky Identifikátor klíče autority (viz Příloha G). Pokud v certifikační cestě neselhal ani jeden z kroků ověřování, pak může být ověřovaný certifikát prohlášený za platný. (1 str. 111)

Vytvoření a ověřování certifikační cesty se řadí mezi složitější procedury, které provádí k tomu určený software. I samotné ověření se uskutečňuje automatizovaně bez součinnosti osoby. (1 str. 112)

Odvolávání certifikátu

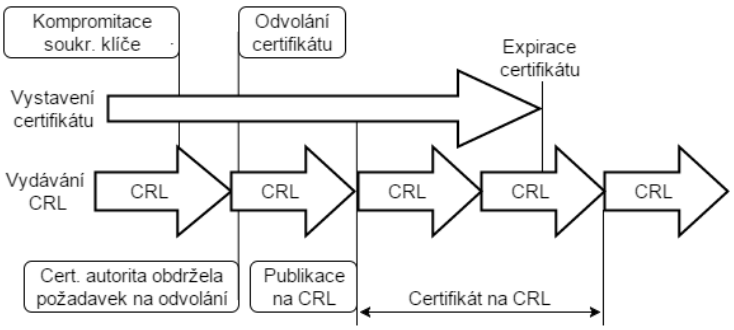
Platnost certifikátu se ukončí v době, kdy vyprší deklarovaná doba platnosti uvedená na certifikátu. Ovšem před vypršením doby platnosti může nastat situace, že certifikát byl z nějakých důvodů odvolán či může dojít k pozastavení platnosti. V případě, že nastane odvolání ceritifikátu, dojde k jeho zařazení do CRL (Certificate Revocation List – seznam odvolaných certifikátů). Ze seznamu bude odstraněn až po uplynutí původně prohlášené platnosti. Certifikační autority rozlišují několik typů seznamů odvolaných certifikátů: (1 str. 87)

- **přímý seznam** – je vydáván přímo autoritou, která odvolala certifikáty.
- **nepřímý seznam** – je vydáván jinou certifikační autoritou, než tou, která odvolala certifikáty. Označuje se jako autorita pro vydávání CRL.
- **úplný seznam** – obsahem jsou všechny odvolané certifikáty, kterým ještě nevypršela původní platnost.
- **rozdílový seznam** – obsahem jsou pouze odvolané certifikáty, které byly prohlášeny neplatnými až po vydání úplného seznamu.
- **částečný seznam** – obsahem jsou odvolané certifikáty dle vybraného kritéria.

Požadavek na odvolání certifikátu může být předán několika možnostmi. Jedním ze způsobů je přímá návštěva držitele odvolávaného certifikátu u certifikační autority.

Rychlejší možností je elektronická cesta, kdy se žádost o odvolání podepíše soukromým klíčem odvolávaného certifikátu a tím certifikační autorita ověří identitu držitele. Další způsob odvolání odkazuje na využití jednorázového hesla, které držitel zadával při žádosti o vydání certifikátu. (1 str. 89)

Proces odvolání certifikátu začíná ve chvíli, kdy došlo k odcizení soukromého klíče. Jakmile to držitel certifikátu zjistil, náhlasil událost příslušné certifikační autoritě. Poté certifikační autorita posoudí žádost o odvolání, a pokud ji schválí, zařadí identifikační údaje odvolávaného certifikátu do nejbližšího vydání seznamu CRL (viz Obrázek 16). Zde ještě záleží na pravidlech konkrétní certifikační autority a na periodě aktualizování seznamu CRL. (1 str. 88)



Obrázek 16: Průběh odvolávání certifikátu

Zdroj: Vlastní zpracování dle (1 str. 88)

Nejčastějším důvodem odvolání certifikátu však nepatří odcizení soukromého klíče, ale běžnější je žádost například v situaci, když zaměstnanci byl ukončen pracovní poměr, který ovšem vlastnil firemní certifikát. Certifikační autorita má také možnost odvolat certifikát ze své vlastní iniciativy. Situace nastává v případech, kdy autorita obdržela žádost o vydání nového certifikátu ovšem s již certifikovaným veřejným klíčem anebo pokud jsou v žádosti uvedené neplatné údaje. (1 str. 90)

Seznam zneplatněných certifikátů

Seznam zneplatněných certifikátů si lze jednoduše představit jako úřední desku, kam jsou certifikační autoritou pravidelně zvěřejňovány odvolané certifikáty. Seznam zpravidla vystavují přímo certifikační autority anebo mohou pověřit jinou autoritu pro vydávání CRL. Certifikáty, které byly odvolané, jsou v seznamu uvedeny se svým sériovým číslem a datem odvolání. Struktura CRL je přímo specifikována normou X.509 a je obdobná se strukturou certifikátu, tzn. obsahuje: (1 str. 91)

- verze – specifikace uvádí položku jako povinnou s hodnotou 1 (podle normy X.509 tedy verze 2),
- vystavitel – identifikace vydavatele CRL,
- datum začátku platnosti – udává přesný čas, ve který byl seznam vystaven,
- příští aktualizace – udává předpokládaný nejpozdější čas, kdy bude následující seznam vydán, ovšem může být vydán i dříve,
- algorimus podpisu – specifikuje algoritmus použitý pro podepsání CRL,
- podpisový algoritmus hash – Otisk podpisového algoritmu,
- rozšíření CRL – je nepovinné, ale často se uvádějí informace jako Identifikátor klíče autority, Číslo seznamu CRL či o jaký druh seznamu se jedná,
- záložka Seznam odvolání – obsahující soupis odvolaných certifikátů, kdy je pro každý uvedeno sériové číslo, datum a čas odvolání, případné rozšíření konkrétního certifikátu.

Certifikát pro is.czu.cz taktéž obsahuje seznam CRL, který zobrazuje Příloha H.

Protokol pro on-line zjištění stavu certifikátu

Tato online služba je využívána k rychlému informování uživatele o změně statusu daného certifikátu. Její provoz má na starosti certifikační autorita. Používá se tak, že pokud chce uživatel použít certifikát, prohlížeč se nejdříve online zeptá serveru na jeho status. V případě, že je platný, prohlížeč ho bezproblému použije. Ovšem v situaci, kdy je certifikát odvolán, prohlížeč jej zamítne. Taktéž může nastat situace, kdy server odpoví, že status certifikátu je neznámý a rozhodnutí o použití je tedy na samotném uživateli. (31)

Tento způsob informování využívá protokolu OCSP (Online Certificate Status Protocol) a online status je poskytován z OCSP serveru certifikační autority. Protokol je k nalezení i na certifikátu is.czu.cz (viz Příloha I). Protokol řeší zároveň některé problémy, jako je rychlost informace o odvolání certifikátu. Není tak nutné čekat, až certifikační autorita vydá další seznam CRL, jelikož protokol OCSP vždy online informuje o stavu konkrétního certifikátu. Zároveň není do prohlížeče přenášen takový objem dat jako u seznamu CRL, který obsahuje veškeré odvolané certifikáty konkrétní certifikační autority. U protokolu OCSP prohlížeč položí dotaz serveru na status pouze jednoho konkrétního certifikátu a tím je zaručená rychlost a aktuálnost poskytnuté informace. (31)

Obnova certifikátu

V případě, že se blíží konec platnosti certifikátu, je nutné, aby uživatel zažádal o obnovení tohoto certifikátu. Platnost je určena informacemi na certifikatu, které lze dohledat, jako položky Neplatí před a Neplatí po. Pokud byl certifikát platný, ale z nějakého důvodu byl odvolán, tak ho již nelze obnovit a k uživateli certifikační autorita přistupuje stejně, jako kdyby žádal o svůj první certifikát. (1 str. 116) (22)

Proces lze opět přirovnat k občanskému průkazu. Pokud občan dojde před koncem platnosti občanského průkazu zažádat o nový, prokáže se starým průkazem. Ovšem pokud je starý průkaz již neplatný, musí prokázat svou totožnost jinými doklady. Je snahou, aby obnova certifikátu probíhala elektronickou cestou bez nutné osobní návštěvy autority. To lze ovšem jen za situace, pokud žadatel disponuje platným certikátem. (1 str. 116) (22)

Dobu platnosti certifikátu určuje kompromis mezi častou obnovou certifikátu a bezpečností. Pro certifikační autority by bylo nejjednoduší stanovit co nejdelší dobu, ovšem pak hrozí riziko určitých kryptografických nedostatků párových dat. Bezpečnějším by tedy bylo stanovit dobu co nejkratší, avšak to by způsobilo zatížení certifikační autorit, které by byly nuceny často obnovovovat certifikáty. Rozhodnutí se odvíjí od používaných technologií a deklarované bezpečnosti certifikační autority. Zároveň se pro komerční a kvalifikované certifikáty stanovuje odlišná doba platnosti. (1 str. 119)

Obnova certifikátu koncového uživatele

Obnova certifikátu určeného koncovému uživateli, který disponuje platným certifikátem, probíhá elektronickou cestou. Osobní identifikace držitele byla provedena již při vydání prvního certifikátu. Ovšem je nutné uživatele autentizovat. Z tohoto důvodu se použije starý certifikát, a to tak, že se jim digitálně podepíše žádost o obnovu certifikátu a odešle se na příslušnou certifikační autoritu. Pokud si uživatel vygeneroval nová párová data, pak musí dokázat, že má v držení nový soukromý klíč. Důkaz provede například digitálním podpisem, který vytvořil pomocí nového soukromého klíče. (1 str. 117)

V situaci, kdy uživatel již nemá platný certifikát, musí provést stejné kroky, jako když žádal o vystavení prvního certifikátu. Musí se tedy osobně dostavit na registrační autoritu a poskytnout dokumenty k prověření totožnosti. Autority se snaží těmto situacím vyhýbat, a proto mají nastavené upomínaní. Držitelé jsou tak upozorněni na blížící se konec platnosti jejich certifikátů a mohou si je pohodlně obnovit elektronickou cestou. (1 str. 117)

Obnova certifikátu certifikační autority

Období platnosti certifikátu neplatí jen pro koncové uživatele, ale i pro certifikáty certifikačních autorit. Autorita by nikdy neměla vystavit uživateli certifikát, který bude mít delší platnost, než certifikát samotné autority. Nastala by tak situace, kdy by uživatel vlastnil platný certifikát, ovšem podepsaný neplatným certifikátem autority. (1 str. 118)

Řešením pro certifikační autority je křížová certifikace, kdy autorita si nějakou dobu drží dva certifikáty, které se platností vzájemné překrývají. Oba mají stejnou hodnotu v položce předmět a liší se hodnotou pořadového čísla a veřejného klíče. Někteří držitelé tak mají certifikát podepsaný starým certifikátem autority a ostatní už novým certifikátem autority. Vystavené certifikáty pro koncové uživatele ovšem v položce vydavatel obsahují informace z předmětu certifikátu autority, která je podepsala. A tato položka je právě shodná, jak pro starý, tak pro nový certifikát certifikační autority. (1 str. 118)

4 Praktická část

Praktická část je rozdělena na dva oddíly, kde první je zaměřen na analýzu certifikačních autorit včetně způsobu vytvoření vlastní autority. Druhá sekce obsahuje dotazníkové šetření s využitím vystaveného certifikátu, který byl považován za nedůvěryhodný. Průzkum byl sestaven takovým způsobem, aby zároveň zjistil informovanost mezi uživateli internetu o zabezpečeném připojení i o samotných digitálních certifikátech.

4.1 Certifikační autority

V této kapitole jsou uvedeny informace o třech českých akreditovaných certifikačních autoritách a dále pak o autoritách, kde je možné bezplatně získat důvěryhodný certifikát. Poslední subkapitola obsahuje vytvoření vlastní autority a vystavení certifikátu.

4.1.1 Akreditované certifikační autority v ČR

4.1.1.1 První certifikační autorita, a.s. (I.CA)

První certifikační autorita získala v roce 2002 jako první v České republice akreditaci pro poskytování certifikačních služeb dle zákona č. 227/2000 Sb., o elektronickém podpisu. Tímto začala poskytovat kvalifikované a komerční certifikáty. V roce 2006 si autorita vyžádala rozšíření akreditace, aby mohla vydávat i kvalifikované systémové certifikáty a kvalifikovaná časová razítka. Autorita má své kořenové certifikáty zařazené mezi důvěryhodné kořenové certifikační autority společnosti Microsoft. (22)

Dne 1. 9. 2015 změnila autorita svou hierarchii na dvouúrovňovou strukturu. V první úrovni je umístěn samotný kořenový certfikát certifikační autority (I.CA Root CA/RSA) a ve druhé úrovni jsou pak dvě podřazené certifikační autority. Jedna podřazená autorita (I.CA Qualified CA/RSA) má na starosti kvalifikované certifikační služby a druhá (I.CA SSL CA/RSA) pak nekvalifikované služby – komerční, serverové, SSL certifikáty. (22)

Žadatelé o certifikát si mohou vybrat ze třiceti registračních autorit umístěných většinou v krajských městech České republiky. Dle informací uvedených na stránkách autority je pro bezproblémové odbavení vhodné si domluvit termín návštěvy. Autorita také nabízí své služby na Slovensku. Pomocí mobilního pracoviště již také autorita vystavila certifikáty v zemích jako je Německo, Velká Británie, Rakousko či Švýcarsko. (22)

Získání certifikátu

Pomocí webové aplikace si žadatel vytvoří elektronickou žádost, ve které si vygeneruje i pár klíčů. Vytvořenou žádost si je možné uložit na přenosné médium nebo si uschovat šestimístný číselný kód a nechat si žádost uložit na server autority. Dalším krokem je dostavení se na vybranou registrační autoritu i s příslušnými doklady totožnosti. Počet dokladů a případných dokumentů je závislý na druhu certifikátu a pro koho je určen. (22)

Registrační autorita ověří údaje uvedené na žádosti dle dokladu, uloží žádost do systému a následně odešle požadavek o vydání certifikátu. Vystavení certifikátu trvá několik minut. Vydaný certifikát je následně odeslán do e-mailové schránky žadatele a zároveň může být požádáno o uložení certifikátu na USB flash paměť či čipovou kartu. (22)

Žadateli nezbývá nic jiného, než si certifikát nainstalovat do svého počítače. K samotné instalaci může využít webovou stránku, jejíž adresu obdržel do e-mailové schránky spolu s certifikátem. (22)

Ceník

Z ceníku dostupného na webových stránkách I.CA byly vyjmuty pouze ceny základních produktů ke dni 9. 3. 2016 (viz Tabulka 4). Cena prodloužení certifikátu, tedy následného certifikátu, je stanovena shodně jako vydání prvotního certifikátu. (22)

Certifikát	Platnost	Cena včetně DPH
Komerční certifikát	1 rok	395,00 Kč
Komerční serverový certifikát	1 rok	1170,00 Kč
Kvalifikovaný certifikát	1 rok	495,00 Kč
Kvalifikovaný systémový certifikát	1 rok	780,00 Kč
Zneplatnění certifikátu		Zdarma
Výjezd mobilní registrační autority I.CA		6 050,00 Kč

Tabulka 4: Ceník vybraných produktů První certifikační autority, a.s.

Zdroj: (22)

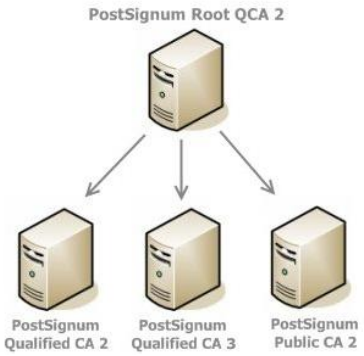
4.1.1.2 PostSignum

PostSignum je provozováno společností Česká pošta, s. p. Ta byla dne 15. 7. 2005 zařazena na seznam akreditovaných poskytovatelů certifikačních služeb dle zákona č. 227/2000 Sb., o elektronickém podpisu. Autorita nabízí jak kvalifikované, tak komerční certifikáty. Od roku 2009 pak nabízí i zřízení kvalifikovaného časového razítka. Kořenový

certifikát této autority je zařazen do seznamu důvěryhodných autorit v operačním systému Windows. (32)

Certifikační autorita má stanovenou dvouúrovňovou stromovou strukturu (viz Obrázek 17). Kořenová autorita je označena jako PostSignum Root QCA2 (SHA 256), která vystavila třem podřízeným autoritám kvalifikované systémové certifikáty: (32)

- PostSignum Qualified CA 2 (SHA 256) – se zaměřuje na vydávání kvalifikovaných certifikátů,
- PostSignum Qualified CA 3 (SHA 256) – má na starosti kvalifikované certifikáty pro časová razítka,
- PostSignum Public CA 2 (SHA 256) – vydává komerční certifikáty.



Obrázek 17: Hierarchie PostSignum

Zdroj: (32)

Žadatelé se pro vydání certifikátu musí dostavit osobně – na výběr mají z 976 poboček České pošty se službou Czech POINT. Další možností je za poplatek objednání mobilní registrační autority. (32)

Získání certifikátu

Získání certifikátu u certifikační autority PostSignum lze rozdělit na dva hlavní procesy. Prvním důležitým procesem je uzavření smlouvy s Českou poštou o poskytnutí certifikační služby, která se většinou uzavírá na dobu neurčitou a je možné na ní vystavit libovolné množství certifikátů. Následně je potřeba vyplnit dokument Údaje pro vydávání certifikátu, který specifikuje druh certifikátu a informace na něm uvedené. Právnické osoby musí navíc vyplnit i Seznam žadatelů, který autoritě předává pověřená osoba stanovená ve smlouvě. Smlouvu může žadatel uzavřít na některé z poboček České pošty s označením Czech POINT nebo využit obchodní místa certifikační autority. (32)

Žadatele o certifikát ještě čeká druhý proces. V tomto kroku si žadatel musí vygenerovat párové klíče a samotnou žádost o certifikát. Může si vybrat z možnosti online či offline. V případě první jmenované možnosti je podpora pro operační systém Windows a internetový prohlížeč Internet Explorer. Pokud nelze splnit tyto podmínky, pak nezbývá jiná volba než offline, která požaduje nainstalování aplikace s podporou všech operačních systémů. Po vygenerování je potřeba uložit žádost na USB flash paměť nebo si uložit identifikační číslo žádosti uložené na serveru PostSignum. (32)

Následuje žadatelova návštěva u registrační autority s dvěma osobními doklady, vyplněnými dokumenty a vygenerovanou žádostí. Po ověření identity obsluha odešle žádost do systému certifikační autority. Jakmile dojde k vystavení certifikátu, obsluha jej předá žadateli na přinesenou USB flash paměť a také odešle webovou adresu ke stažení kopie do jeho e-mailové schránky. Žadatel už jen vydaný certifikát nainstaluje do svého počítače. (32)

Ceník

Z ceníku dostupného na webových stránkách PostSignum byly vybrány pouze ceny základních produktů ke dni 9. 3. 2016 (viz Tabulka 5). Cena prodloužení certifikátu, tedy následného certifikátu, je stanovena shodně jako vydání prvotního certifikátu. Následný certifikát má prodlouženou platnost na 385 dní. (32)

Certifikát	Platnost	Cena včetně DPH
Komerční certifikát	1 rok	348,00 Kč
Komerční serverový certifikát	1 rok	800,00 Kč
Kvalifikovaný certifikát	1 rok	396,00 Kč
Kvalifikovaný systémový certifikát	1 rok	780,00 Kč
Zneplatnění certifikátu		Zdarma
Výjezd mobilní registrační autority		1 680,00 Kč + dopravné

Tabulka 5: Ceník vybraných produktů PostSignum

Zdroj: (32)

4.1.1.3 Akreditovaná certifikační autorita eIdentity, a.s. (ACAeID)

Společnost eIdentity, jež se stala akreditovaným poskytovatelem certifikačních služeb dle zákona č. 227/2000 Sb., o elektronickém podpisu 12. 9. 2005, vznikla v roce 2004 se zaměřením na oblast správy elektronické identity. Autorita nabízí komerční a kvalifikované certifikáty. Od července 2010 je také možné požádat o kvalifikované časové razítko. Kořenový certifikát autority není předinstalován v úložišti pro operační systém

Windows. Před použitím je proto nutné v každém prostředí, kde má být vydaný certifikát využíván, zdůvěryhodnit tuto certifikační autoritu. (33)

Společnost má opět stanovenou dvouúrovňovou stromovou strukturu (viz Obrázek 18), kde kořenová certifikační autorita je označena jako RCA (Root Certificate Authority) a vystavila kvalifikované systémové certifikáty pro tři podřízené autority: (33)

- TSA (Time Stamping Authority) – autorita vydávající kvalifikovaná časová razítka,
- QCA (Qualified Certificate Authority) – autorita vystavující kvalifikované certifikáty a kvalifikované systémové certifikáty
- CCA (Commercial Certificate Authority) – autorita vystavující komerční certifikáty a komerční serverové certifikáty

Obrázek 18: Stromová struktura eIdentity

Zdroj: (33)

Žadatelé si o své certifikáty mohou žádat na třech registračních místech, které jsou umístěné pouze v Praze. K dispozici je také využití služby mobilní registrační autoritou. (33)

Získání certifikátu

Prvním krokem pro získání certifikátu je registrace žadatele do systému a zřízení uživatelského účtu. Do účtu se následně lze přihlásit pomocí jména a hesla zaslaného na registrovanou e-mailovou adresu. Po přihlášení do účtu si již lze vybrat z nabízených služeb. V případě organizace je nutné si ještě vytvořit organizační zařazení, kam se vyplňují informace o organizaci, jejím sídle a pracovní pozici žadatele. Dále je krok společný i pro fyzickou osobu, kdy následuje vybrání údajů umístěných na požadovaném certifikátu a určení osobních dokladů k předložení registrační autoritě. Krok je ukončený vygenerovanou žádostí o platbu za vydání certifikátu, kdy je potřeba předem tuto částku uhradit. (33)

Potvrzení přijetí platby je eIdentitou zasláno žadateli e-mailem a může tak pokračovat dalším krokem, kdy je potřeba provést výběr registrační autority a termínu

plánované návštěvy. Následuje samotné vygenerování párových klíču a žádosti o certifikát, jejíž odeslání proběhlo automaticky do certifikační autority. (33)

Na registrační autoritě je potřeba doložit osobní doklad pro ověření identity. V případě žádosti o kvalifikovaný certifikáty jsou potřeba dva osobní doklady. Následně proběhne samotné vystavení certifikátu certifikační autoritou, ovšem žadatel jej nedostane na žádné přenosné médium. Svůj certifikát získá až po přihlášení do systému a zobrazení webové stránky s vystavenými certifikáty. Poté po stisknutí tlačítka pro instalování certifikátu, kde je potřeba ještě uvedené údaje potvrdit, proběhne samotné nainstalování certifikátu do jeho počítače. (33)

Ceník

Z ceníku dostupného na webových stránkách eIdentity byly vybrány pouze ceny základních produktů ke dni 9. 3. 2016 (viz Tabulka 6). Cena prodloužení certifikátu, tedy následného certifikátu, je stanovena shodně jako vydání prvotního certifikátu. (33)

Certifikát	Platnost	Cena včetně DPH
Komerční certifikát	1 rok	357,00 Kč
Komerční serverový certifikát	1 rok	1 083,00 Kč
Kvalifikovaný certifikát	1 rok	478,00 Kč
Kvalifikovaný systémový certifikát	1 rok	1 113,00 Kč
Zneplatnění certifikátu		Zdarma
Výjezd mobilní registrační autority		Na vyžádání – dle lokality a počtu vydaných certifikátů

Tabulka 6: Ceník vybraných produktů ACAeID

Zdroj: (33)

4.1.2 Bezplatné způsoby získání důvěryhodného certifikátu

Na trhu se lze setkat s několika společnostmi, které nabízejí získání certifikátu zdarma. Jedná se například o společnost CAcert.org[4], která je spravována komunitou uživatelů, ale její vydávané certifikáty nejsou důvěryhodné. Další možností je využití certifikační autority StartSSL[5] od společnosti StartCom, která nabízí základní certifikát

[4] *CAcert* [online]. 2016 [cit. 2016-03-09]. Dostupné z: http://www.cacert.org/

[5] *StartSSL™ Certificates; Public Key Infrastructure* [online]. 2016 [cit. 2016-03-09]. Dostupné z: https://www.startssl.com/

ověřující doménu zdarma. Vystavené certifikáty jsou důvěryhodné, jelikož kořenovou certifikační autoriou je StartCom, která je standardně uložená v úložišti důvěryhodných kořenových certifikátů autorit. V následujících subkapitole bude detailněji popsána česká certifikační autorita, která začala poskytovat důvěryhodný certifikát zdarma. Do druhé subkapitoly byla zvolena certifikační autorita, za jejímž vznikem stála zajímavá myšlenka a poskytuje důvěryhodné certifikáty také zcela zdarma.

4.1.2.1 Zoner software

Zoner software provozuje SSLmarket, kde jsou nabízeny již od roku 2005 důvěryhodné komerční certifikáty. Jako první společnost v ČR zprostředkovala vydání EV certifikátu na českém trhu. Mezi nabízenými službami není pouze přeprodej certifikátů, ale i zákaznická podpora na vysoké úrovni. Společnost uzavřela partnertví s největší certifikační autoritou na světě – Symantec, ovšem nabízí i produkty ostatních certifikační autorit, jako je RapidSSL, Thawte či GeoTrust. Hierarchii této společnosti nelze určit, jelikož není certifikační autoritou, ale pouze přeprodejcem certifikátů od světových certifikační autorit. (34)

Získání certifikátu

Získání certifikátu je velmi jednoduché, jelikož společnost nabízí pouze komerční certifikáty a nepodléhá tak zákonu o elektronickém podpisu, musí pouze dodržovat pravidla nastavená certifikačními autoritami. Mezi produkty lze najít certifikáty dle ověření DV, OV a EV. Zatímco u DV probíhá ověření pouze přes odeslaný e-mail z ověřované domény a certifikát je vystaven již od 2 minut, tak v případě OV je potřeba provést ověření domény, ověření existence a registrace firmy a také pomocí telefonického hovoru ověření samotného žadatele. Vystavení certifikátu se tak pohybuje od 2 dnů. V případě požadavku na EV vychází ověření z předchozí úrovně, ovšem je přísnější, informace jsou potvrzovány z více zdrojů a proto vydání certifikátu trvá minimálně 5 dní. (34)

Ceník

Z ceníku dostupného na webových stránkách SSLmarket byly vyjmuty pouze ceny nejlevnějších produktů dle typu ověření ke dni 9. 3. 2016 (viz Tabulka 7). Cena prodloužení certifikátu, tedy následného certifikátu, je cenově ohodnocena shodně jako vydání prvotního certifikátu. (34)

Ovšem Zoner přišel na český trh v březnu 2016 se zajímavou nabídkou, která je zatím pouze ve zkušebním provozu a spuštění ostré verze je naplánováno na 1. 4. 2016. Pokud uživatel převede nebo zaregistruje svou doménu pod Zoner, dostane zdarma, na celou dobu její platnosti, certifikát Basic DV od Symantec – největší certifikační autority světa. (34)

Certifikát	Platnost	Cena včetně DPH
Certifikát Basic DV	dle platnosti domény	zdarma
Ověření domény (DV)	1 – 3 roky	od 349,00 Kč
Ověření společnosti (OV)	1 – 3 roky	od 2 463,00 Kč
Rozšíření ověření (EV)	1 – 2 roky	od 4 795,00 Kč
Přeregenerování certifikátu		Zdarma

Tabulka 7: Ceník vybraných produktů SSLmarket

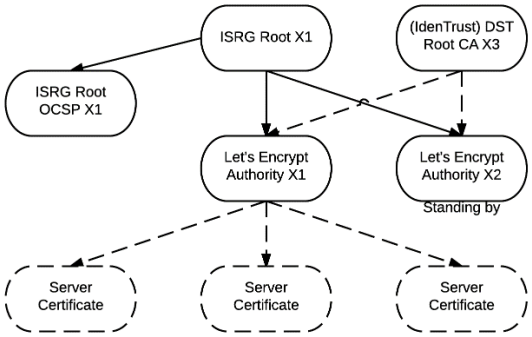
Zdroj: (34)

4.1.2.2 Let‘s encrypt

Let’s encrypt je zdarma dostupná, automatizovaná a otevřená certifikační autorita, fungující ve prospěch veřejnosti. Služba je poskytovaná skupinou Internet Security Research Group (ISRG) a financovaná Mozillou, Akamai, Cisco Systems, Chrome a dalšími. Myšlenkou vzniku bylo, že pokud má být HTTPS rozšířeno na další webové stránky, nemělo by být jeho nasazování zpoplatněno a plné překážek. Klíčovými zásadami služby jsou: (35)

- **bezplatnost** – jakýkoliv vlastník domény může získat důvěryhodný certifikát zdarma.
- **automatičnost** – software je spuštěn na webovém serveru, díky němuž je získán správně nakonfigurovaný certifikát, a automaticky se stará o jeho obnovování.
- **bezpečnost** – služba funguje jako platforma pro nasazení šifrovaného připojení, zároveň autorita pomáhá provozovatelům se zabezpečením jejich webových stránek.
- **transparentnost** – všechny vydané a odvolané certifikáty jsou zveřejněny a tedy zpřístupněny každému ke kontrole.
- **otevřenost** – protokol pro automatické vydávání a prodlužování je zveřejněn jako otevřený standard.
- **součinnost** – služba chce být součástí spolupráce internetové komunity, nikoliv být ovládána pouze jednou organizací.

Dne 8. března 2016 autorita uvedla, že již vydala svůj miliontý certifikát během svého 16 měsíčního působení. Důvěryhodnost vystaveného certifikátu je zajištěna pomocí křížového podepisování mezi autoritami, kdy mezilehlý certifikát Let's Encrypt byl podepsán autoritou IdenTrust (Obrázek 19), jejíž kořenový certifikát se standardně vyskytuje v důvěryhodných úložištích. (35)



Obrázek 19: Stromová struktura Let's Encrypt

Zdroj: (35)

Získání certifikátu

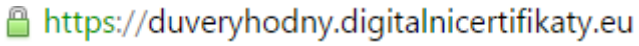
Získání certifikátu se provádí využitím automatické utility letsencrypt, kterou si vlastník domény nainstaluje na server. Ta následně komunikuje se serverem služby. Po instalaci se vygeneruje pár klíčů, se kterým se uživatel představuje serveru, probíhá tak zabezpečená komunikace, kde je autorita požádána o vydání certifikátu. Pokud server prohlásí žádost za oprávněnou, dojde k vydání certifikátu, který se uloží do předem určeného úložiště. Certifikát je vystavený pouze na jeden měsíc, ale utilita automaticky hlídá platnost certifikátu a sama si pak požádá o vystavení nového. (35)

Ceník

Ceník na stránkách této autority není k dohledání, jelikož nabízené služby jsou poskytovány zdarma. Jako poděkování za služby je možné přispět libovolným finančním obnosem. Organizace mají navíc možnost se stát sponzory, kdy nejnižším možným příspěvkem je 10 000 dolarů za rok. (35)

Praktická aplikace

Společnost COX Intelligent Applications vytvořila přehledný návod[6] na implementaci Let's Encrypt u webového hostingu Wedos. Součástí je poupravený lescript, který je volně dostupný, a po jeho správné konfiguraci a spuštění, je požádáno o vystavení certifikátu. V případě potvrzení od autority jsou za několik málo minut stažené certifikáty v nastaveném úložišti. Poté již stačí překopírovat jejich obsah do konfigurace zabezpečeného připojení webové hostingu. Návod byl prakticky otestován na doméně duveryhodny.digitalnicertifikaty.eu (viz Obrázek 20) a díky němu byl získán důvěryhodný certifikát (viz Příloha J) zcela zdarma. Správné zabezpečení webové stránky je možné otestovat na SSL Labs[7], kde s takto vystaveným certifikátem lze získat nejvyšší ohodnocení A+ (Příloha K).



Obrázek 20: Zobrazení URL řádky s důvěryhodným certifikátem

Zdroj: Autor

4.1.3 Vlastní certifikační autorita

Vytvoření certifikační autority

K vytvoření certifikační autority a následnému vystavení certifikátu bylo využito open source řešení – aplikace XCA, jejímž jádrem je kryptografická knihovna OpenSSL. Aplikace je uživatelsky přívětivá, jelikož nabízí přehledné grafické rozhraní, podrobný popis[8] a je také dostupná na operační systémy Linux, Mac OS a Windows.

Prvním krokem po stažení instalační balíku, provedení instalace a spuštění aplikace, bylo vytvoření nové databáze. Pro databázi se určilo místo úložiště v systému, její název a také heslo, kterým jsou zašifrovány privátní klíče v ní uložené.

Před samotným vytvořením certifikační autority bylo nejprve nutné vygenerovat její privátní klíč. V aplikace je tato možnost pod záložkou Private Keys, kde bylo potřeba privátní klíč pojmenovat, zvolit jeho algoritmus šifrování a velikost (viz Příloha L).

---

[6] *Nasazení Let's Encrypt u Wedos* [online]. Brno: COX Intelligent Applications, 2016 [cit. 2016-03-16]. Dostupné z: http://www.cox.cz/public/le/wedos_navod.zip

[7] *Qualys SSL Labs* [online]. Qualys, 2016 [cit. 2016-03-16]. Dostupné z: https://www.ssllabs.com

[8] *XCA - X Certificate and key management* [online]. Christian Hohnstädt, 2015 [cit. 2016-02-21]. Dostupné z: http://xca.sourceforge.net/xca.html

Dále bylo potřeba vytvořit certifikát samotné certifikační autority, který byl tvořen na záložce Certificates. Poté na záložce Source (viz Příloha M) bylo možné zvolit z několika šablon, pro certifikační autoritu byla tedy zvolena šablona CA. Následně bylo potřeba zkontrolovat, že certifikát bude podepsaný sám sebou (self signed), uvést jeho pořadí a podpisový algoritmus, který by měl být dle doporučení ze skupiny SHA-2.

Na následující záložce Subject bylo potřeba vyplnit informace, které mají být uvedené na certifikátu. Kromě základních položek bylo možné přidat i další doplňující informace z rozbalovacího menu. Ve spodní části bylo ještě nutné vybrat privátní klíč, který má být použit. Pro účely vytvoření certifikační autority byly základní položky vyplněny takto:

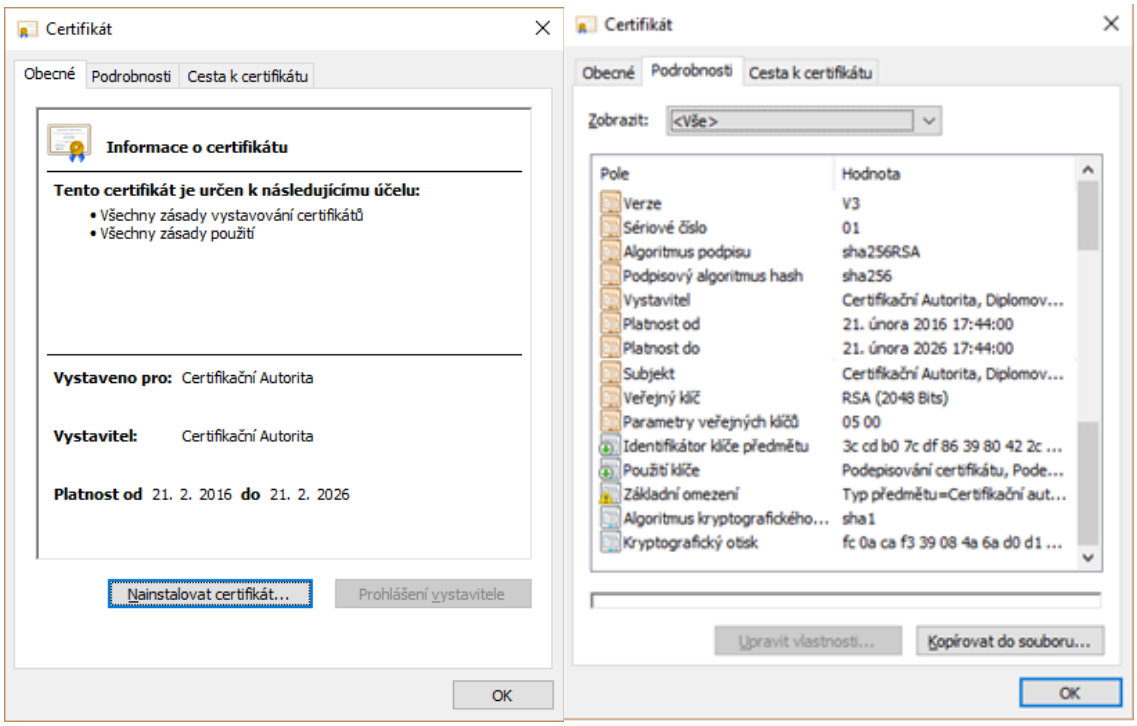
- **countryName** – CZ
- **localityName** – Praha
- **organizationName** – Česká zemědělská univerzita
- **organizationalUnitName** – Diplomová práce
- **commonName** – Certifikační autorita

Další záložka Extension obsahovala část se základními omezeními, kde pro autoritu byla zvolena možnost Certification Authority. Ve vedlejší části pro identifikátor klíče byla zvolena varianta pro předmět, tedy Subject Key Identifier. Dále zde bylo možné definovat platnost certifikátu položkami Not before, Not after či možností Time range. Pro šablonu CA je standardním nastavením 10 let. Ve spodní části okna bylo možné doplnit alternativní název předmětu, alternativní jméno vydavatele, odkaz na CRL či využití přístupu k informacím pomocí OCSP.

Záložka Key usage stanovovala použití klíče, pro CA byla standardně nastavená možnost podepisování certifikátů (Certificate Sign) a podepisování CRL (CRL Sign).

Záložka Advanced představovala shrnutí nakonfigurovaných parametrů. V případě, že by bylo potřeba přidat ještě některé položky, které nejsou pokryty aplikací, bylo možné je ručně nakonfigurovat pomocí příkazů definovanými OpenSSL.

Posledním krokem bylo potvrzení certifikátu autority, čímž došlo k jejímu vytvoření. Certifikát je také zobrazen v seznamu certifikátů a od ostatních je rozeznatelný tím, že má v položce CA zobrazené zelené zatržítko. Aplikace také nabízela možnost exportování vystaveného certifikátu (Obrázek 21) do formátů PEM, PKCS #7, PKCS #12, DER a dalších možností vzniklých kombinováním.



Obrázek 21: Zobrazení informací na vyexportovaném certifikátu certifikační autority

Zdroj: Autor

Vytvoření certifikátu

Vytvoření samotného certifikátu začíná stejným krokem jako v případě certifikační autority – vygenerováním privátního klíče. Následujícím krokem je vytvoření žádosti o certifikát, která se předává certifikační autoritě ke schválení. To bylo uskutečněno na záložce Certificate signing requests. Záložky jsou obdobné jako při vytváření certifikátu.

Na první záložce Source bylo možné v části Signing request vyplnit nestrukturovaný název a heslo k ověření, zvolit podpisový algoritmus a taktéž si vybrat z vytvořených šablon.

Záložku Subject bylo nutné vyplnit údaji, které mají být uvedené na vydaném certifikátu. Bylo možné vyplnit základní i rozšířené údaje, ale nutností bylo vybrat ve spodní části vygenerovaný privátní klíč. Základní položky pro účel vytvoření žádosti o certifikát byly vyplněny následovně:

- **countryName** – CZ
- **stateOrProvinceName** - Praha
- **localityName** – Praha
- **organizationName** – Ondřej Svačina
- **organizationalUnitName** – Diplomová práce
- **commonName** – www.digitalnicertifikaty.eu

Další záložka Extensions obsahuje opět části pro základní omezení, identifikátor klíče a možnosti doplnění alternativních jmen a odkazů na CRL či OCSP. V žádosti ovšem není možné stanovit období platnosti, jelikož toto rozhodnutí zůstává na certifikační autoritě.

Na následující záložce Key usage bylo možné navolit potřebné možnosti pro použití klíče. Pro účely tohoto certifikátu byly vybrány možnosti Digitální podpis, Šifrování klíče a v části Použití rozšířeného klíče pak Ověření serveru a Ověření klienta.

Poslední záložka Advanced opět poskytovala shrnutí nakonfigurovaných parametrů a dávala možnost upravit či přidat další parametry, které aplikace nepokrývá.

Závěrečným krokem bylo potvrzení žádosti, kdy byla žádost vytvořena a zařadila se do seznamu tomu určenému. Následně bylo možné žádost exportovat do formátu PEM či DER a odnést na certifikační autoritu, kde by proběhl proces ověření identity a vystavení certifikátu.

Schválení žádosti o certifikát

Jelikož byla vytvořena jak certifikační autorita, tak žádost o certifikát, bylo nutné využít autoritu ke schválení žádosti. Na záložce se žádostmi bylo potřeba vybrat žádost připravenou k posouzení a zvolit možnost Sign, kdy se zobrazilo již předvyplněné okno Create x509 Certificate.

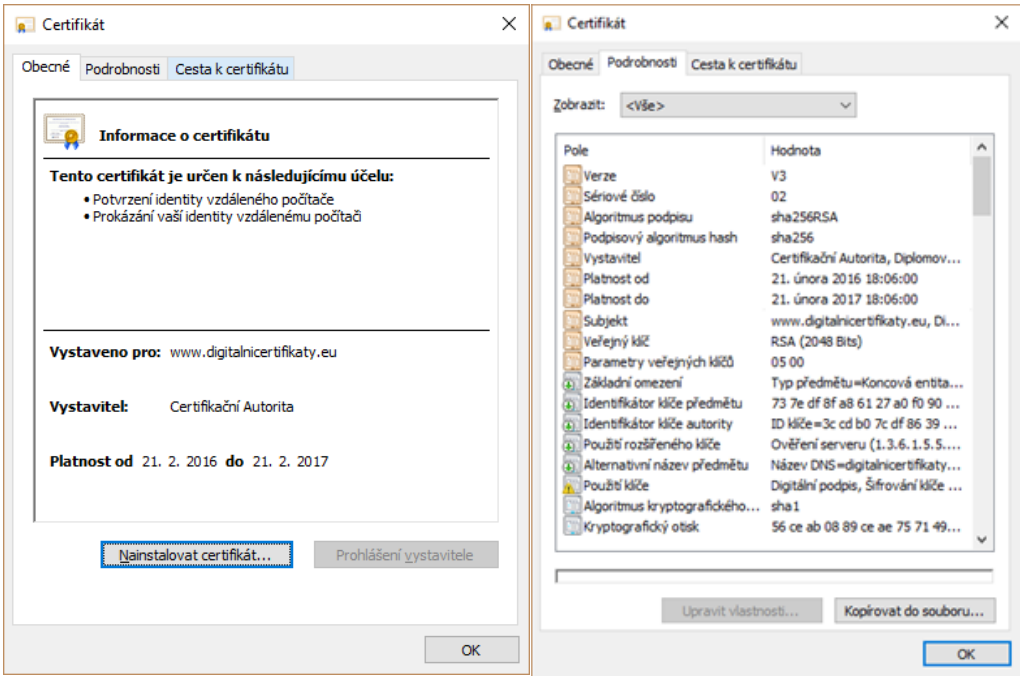
Na záložce Source bylo potřeba zkontrolovat, zda je vybrána správná žádost o certifikát. Dále byla možnost zkopírovat rozšíření uvedené na žádosti a možnost upravení předmětu ze žádosti. Při zvolení druhé možnosti přibyla záložka Subject s předvyplněnými údaji, které bylo možné editovat. Také byla vybrána položka, že pro podepsání bude použit certifikát certifikační autority a konkrétní podpisový algoritmus.

Následující záložka Extension (viz

Příloha N) uvádí základní omezení, kde byla vybrána koncová entita. V části Validity bylo nastaveno období na 1 rok platnosti a jako identifikátor klíče byl zvolen jak identifikátor klíče předmětu, který je vždy povinný, tak identifikátor klíče autority, který je povinný pro všechny nekořenové certifikáty. Do pole Alternativní název předmětu byly doplněny doménová jména digitalnicertifikaty.eu a www.digitalnicertifikaty.eu.

Záložka Key Usage zobrazovala již označené použití ze žádosti o certifikát, ovšem dle normy X.509 bylo nutné základní použití označit jako kritické. Poslední záložkou byla opět Advanced se stejným významem jako v předchozích případech. Následně již stačilo

schválení potvrdit, čímž se vytvořil certifikát. Ten se zobrazil v seznamu na záložce Certificates a bylo možné jej exportovat (viz Obrázek 22) a poté uložit na webový server.



Obrázek 22: Zobrazení údajů na vystaveném certifikátu

Zdroj: Autor

Webový server

Pro umístění vystaveného certifikátu, který má být jedním z prvků dotazníkového šetření, byla zvolena varianta webového hostingu s registrací domény zdarma od společnosti WEDOS Internet, a.s.[9] Doména byla zaregistrována pod označením digitalnicertifikaty.eu s platností do 21. 02. 2017 a webový hosting byl nakonfigurován na možnost důvěryhodného a šifrovaného přístupu pomocí protokolu HTTPS s vlastním certifikátem. Dále bylo potřeba vložit privátní klíč a certifikát ve formátu PEM. Po uložení změn, které se projevily do 30 minut, se již webová stránka zobrazuje pomocí HTTPS.

Vyskytuje se zde ale záměrný problém, který se stal základem dotazníkového šetření. Jelikož byla certifikační autorita vytvořena svépomocí a není standardně obsažena v úložišti pro důvěryhodné kořenové certifikáty certifikačních autorit a také neobsahuje v cestě žádnou důvěryhodnou certifikační autoritu, prohlašují ji webové prohlížeče za nedůvěryhodnou (viz Příloha O).

[9] *WEDOS hosting* [online]. WEDOS Internet, a.s., 2016 [cit. 2016-02-21]. Dostupné z: http://hosting.wedos.com/cs/

4.2 Dotazníkové šetření

4.2.1 Cíle a hypotézy

Hlavní cíl: Analyzovat na praktickém příkladu stupeň informovanosti uživatelů o bezpečnosti připojení prostřednictvím důvěryhodných digitálních certifikátů.

Dílčí cíl č. 1: Zjistit míru informovanosti uživatelů o bezpečném připojení

$1H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi používaným internetovým prohlížečem a povšimnutím si zbarvení řádky adresy webové stránky.

$1H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi používaným internetovým prohlížečem a povšimnutím si zbarvení řádky adresy webové stránky.

$2H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi povšimnutím si zbarvení řádky adresy webové stránky a zájmem uživatele o bezpečnost svých dat.

$2H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi povšimnutím si zbarvení řádky adresy webové stránky a zájmem uživatele o bezpečnost svých dat.

$3H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi zabezpečeně připojeným uživatelem a jím ověřeným digitálním certifikátem.

$3H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi zabezpečeně připojeným uživatelem a jím ověřeným digitálním certifikátem.

$4H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi věkem uživatele a jeho zájmem o bezpečnost svých dat.

$4H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi věkem uživatele a jeho zájmem o bezpečnost svých dat.

Dílčí cíl č. 2: Zjistit míru informovanosti uživatelů o digitálních certifikátech

$5H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a jím ověřeným digitálním certifikátem.

$5H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a jím ověřeným digitálním certifikátem.

$6H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a schopností obejít varovnou zprávu.

$6H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a schopností obejít varovnou zprávu.

$7H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi používaným prohlížečem a schopností obejít varovnou zprávu.

$7H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi používaným prohlížečem a schopností obejít varovnou zprávu.

$8H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a schopností spravovat uložené digitální certifikáty.

$8H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a schopností spravovat uložené digitální certifikáty.

$9H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a znalostmi informačních technologií.

$9H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a znalostmi informačních technologií.

$10H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a chápáním významu varovné zprávy.

$10H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a chápáním významu varovné zprávy.

4.2.2 Volba a charakteristika průzkumné metody

Pomocí prostudované literatury a se záměrem získání vyššího počtu dat, byla k průzkumnému šetření zvolena metoda dotazování cílící na získání kvalitativních dat. Ta byla následně zpracována pro potřeby práce do kvantitativních údajů. Dále jako technika pro získání dat byla dle literatury vybrána forma dotazníkového šetření. (36)

Dotazník (viz Příloha Q) je pojmenován jako „Digitální certifikáty“ a je rozdělen do pěti základních částí. Celkem je dotazník složen z 22 otázek, jejichž vyplnění netrvalo respondentům více než 5 minut. Jednotlivé části dotazníků jsou:

- **I. Část** – je složena z jednoduchých pěti uzavřených otázek, které se zaměřují na využívání softwaru, internetu a různých internetových služeb.
- **II. Část** – obsahuje jednu zajímavou uzavřenou filtrační otázku, která se dotazuje na vnímání bezproblémovosti zobrazení webové stránky s nedůvěryhodným certifikátem. Po odpovědi „Ano“ jsou respondenti přesměrováni na část II. B, kde se nachází uzavřená otázka s obsahem webové prezentace. V případě odpovědi „Ne“ se zobrazí část II. A, jejímž obsahem je otevřená otázka, kde respondenti měli uvést vnímaný problém webové prezentace.
- **III. Část** – je složena z pěti středně těžkých uzavřených otázek, týkající se vnímání a znalostí o bezpečném připojení.

- **IV. Část** – obsahuje pět těžších uzavřených otázek zaměřených na znalosti digitálních certifikátů.
- **V. Část** – se skládá ze čtyř segmentačních otázek typu věk, pohlaví, dosažené vzdělání a obor vzdělání. Pro věk byla použita otevřená otázka a pro ostatní byla využita možnost uzavřených otázek.

4.2.3 Charakteristika souboru respondentů

Pro průzkumné šetření bylo potřeba najít takové respondenty, kteří alespoň někdy využili internetové připojení. Proto bylo zvoleno sestavení dotazníku pomocí online formuláře Google a následné šíření mezi respondenty probíhalo pouze přes internet.

4.2.4 Pilotní studie

Před realizací průzkumného šetření bylo potřeba ověřit srozumitelnost jednotlivých otázek. K tomuto účelu byla vytvořena pilotní studie, která byla distribuovaná 20 respondentům s následným dotazováním o srozumitelnosti otázek. Bylo zjištěno několik nesrovnalostí a proběhlo tak přeformulování otázek:

- z „Jaký používáte internetový prohlížeč?“ na „V jakém prohlížeči máte otevřený tento dotazník?“.
- z „Jaká je Vaše znalost ICT?“ na „Jaká je Vaše znalost informačních technologií?“.
- z „Zobrazí se Vám webová prezentace odkaz?“ na „Zobrazí se Vám bez problému webová prezentace po kliknutí na odkaz?“.
- z „Všiml/a jste si někdy zbarvení v URL řádce?“ na „Všiml/a jste si někdy zbarvení v řádce s adresou webové stránky?“ a zároveň byly k této otázce přidány ilustrativní obrázky.

4.2.5 Realizace dotazníkového šetření

Nejprve proběhlo stanovení potřebného množství vyplněných dotazníků, které z důvodu krátkého časového intervalu sběru, bylo stanoveno na minimálně 300 dotazníků. Náhodný výběr respondentů byl prováděn pomocí internetových diskuzí a skupin s žádostí o další šíření, čímž se dosah dotazníku rozšířil.

Sběr dat probíhal v časovém intervalu od 6. března 2016 do 13. března 2016. Pro zkrácení odkazu na dotazník byla využita internetová aplikace goo.gl[10], která umožňuje měřit počet přístupů přes zkrácený odkaz. Bylo tak změřeno, že přes odkaz si dotazník otevřelo 549 (100 %) internetových uživatelů, ovšem vyplněno a odesláno bylo 383 (69,8 %) dotazníků. Z tohoto počtu byly dále vyřazeny 2 (0,5 %) dotazníky, jelikož odpovědi u otevřené otázky byly nesmyslné. Konečný soubor byl tedy tvořen z celkem 381 vyplněných dotazníků, který byl použit k průzkumnému šetření a byl považován za 100 %.

4.2.6 Statistické zpracování získaných dat

Data byla nejdříve exportována z online dotazníku do Microsoft Excel 2013, kde proběhlo čištění a příprava dat do statistického softwaru SAS 9.4. Pomocí Excelu také byla provedena základní statistická charakteristika, ale samotné testování a zhodnocení stanovených hypotéz bylo realizováno v aplikaci SAS. K ověřování hypotéz byl používán Pearsonův chí-kvadrát test (test dobré shody), který také ověřuje, zda má náhodná veličina předem dané rozdělení pravděpodobnosti. Hladina významnosti byla stanovena na hodnotu 0,05 a pro každou stanovenou hypotézu byla sestavena kontingenční tabulka a následně byl uskutečněn Pearsonův chí-kvadrát test, jehož výsledek je vždy uveden v tabulce, kde:

- **DF** – určuje počet stupňů volnosti,
- **P** – určuje vypočtenou hladinu testu.

V případě, že byla nalezena závislost ve vztahu dvou proměnných, byla dopočítána hodnota Cramerova koeficientu, která sleduje sílu závislosti.

4.2.7 Analýza a interpetace získaných dat

Základní statistická charakteristika jednotlivých otázek je složena z tabulek, jejichž obsahem jsou absolutní hodnoty, relativní četnosti, v určitých případech validní či kumulativní četnosti. Některé otázky byly doplněny grafickým zpracováním dat. Nejprve jsou uvedeny charakteristiky segmentačních otázek a poté otázky postupně dle číslování.

[10] *Google URL shortener* [online]. Google, 2016 [cit. 2016-03-05]. Dostupné z: https://goo.gl/

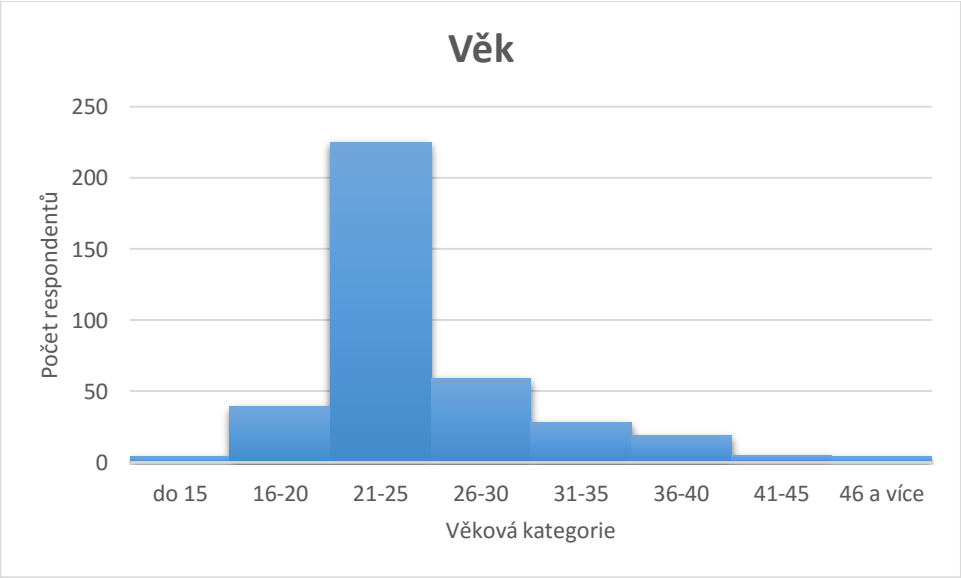
Otázka č. 19: Jaký je Váš Věk?

Kategorie	Absolutní hodnota	Relativní četnost	Kumulativní četnost
do 15 let	4	1,04%	1,04%
16–20 let	39	10,18%	11,23%
21–25 let	225	58,75%	69,97%
26–30 let	59	15,40%	85,38%
31–35 let	28	7,31%	92,69%
36–40 let	19	4,96%	97,65%
41–45 let	5	1,31%	98,96%
46 a více let	4	1,04%	**100,00%**
Celkem	**383**	**100,00%**	

Tabulka 8: Věkové kategorie

Zdroj: Vlastní zpracování

Respondenti měli zapsat svůj věk do pole, které bylo omezeno na celá numerická čísla od 10–99. Pro přehlednost byl věk rozdělen do jednotlivých intervalů dle Sturgesova pravidla. Největší počet respondentů 225 (58,75 %) byl ve věkové kategorii 21–25 let a celkově respondentů do 30 let bylo 85,38 %, což si lze vysvětlit větší internetovou aktivitou u mladších ročníků a také cestou, jakou byl dotazník distribuován. Nejnižší věk byl zaznamenaný 12 let, naopak nejvyšším byla hodnota 48 let. Průměrný věk dosáhl hodnoty 25,4 let. Nejvyšší relativní četnost (modus) se shoduje s mírou centrální tendence (medián) a to na hodnotě 24 let.



Graf 3: Histogram věkových kategorií

Zdroj: Vlastní zpracování

Otázka č. 20: Jaké je Vaše pohlaví?

Kategorie	Absolutní hodnota	Relativní četnost	Kumulativní četnost
Muž	148	38,85%	38,85%
Žena	233	61,15%	**100,00%**
Celkem	**381**	**100,00%**	

Tabulka 9: Pohlaví respondentů

Zdroj: Vlastní zpracování

Celkem bylo do dotazníkového šetření zařazeno 381 respondentů, z čehož bylo 233 (61,15 %) žen a 148 (38,85 %) mužů. Mírnou převahu žen si lze vysvětlit tím, že se více snaží být nápomocné druhým.

Otázka č. 21: Jaké je Vaše nejvyšší dosažené vzdělání?

Kategorie	Absolutní hodnota	Relativní četnost	Kumulativní četnost
Základní	16	4,20%	4,20%
Středoškolské bez maturity	7	1,84%	6,04%
Středoškolské s maturitou	189	49,61%	55,64%
Vyšší odborné	9	2,36%	58,01%
Vysokoškolské	160	41,99%	**100,00%**
Celkem	**381**	**100,00%**	

Tabulka 10: Nejvyšší dosažené vzdělání

Zdroj: Vlastní zpracování

Skoro polovina respondentů 189 (49,61 %) uvedla, že nejvyšší dosažené vzdělání je středoškolské s maturitou, což odpovídá faktu, že převažující množství populace v ČR má právě středoškolské vzdělání. Vzdělání bez maturity uvedlo pouze 6,04 % respondentů, naopak dosažené vyšší vzdělání než maturita uvedlo 44,35 %. Velký počet vysokoškolsky vzdělaných respondentů lze odůvodnit tím, že primárně byli osloveni studenti vysokých škol technického a ekonomického zaměření. (37)

Otázka č. 22: Jaký je Váš obor vzdělání?

Kategorie	Absolutní hodnota	Relativní četnost	Kumulativní četnost
Humanitní	79	20,73%	20,73%
Informatický	50	13,12%	33,86%
Jiný	158	41,47%	75,33%
Lékařský	27	7,09%	82,41%
Technický	67	17,59%	**100,00%**
Celkem	**381**	**100,00%**	

Tabulka 11: Obor vzdělání

Zdroj: Vlastní zpracování

Nejvíce respondentů 158 (41,47 %) uvedlo, že jejich obor vzdělání je Jiný. Takto vysoký podíl může být způsoben tím, že ekonomický obor byl cíleně zařazen mezi humanitní, ovšem většina respondentů měla jiné mínění. Humanitní obor vzdělání uvedlo

79 (20,73 %) respondentů, technický 67 (17,59 %) respondentů, informatický 50 (13,12 %) odpovídajících a nejméně bylo respondentů s oborem lékařským – 27 (7,09 %).

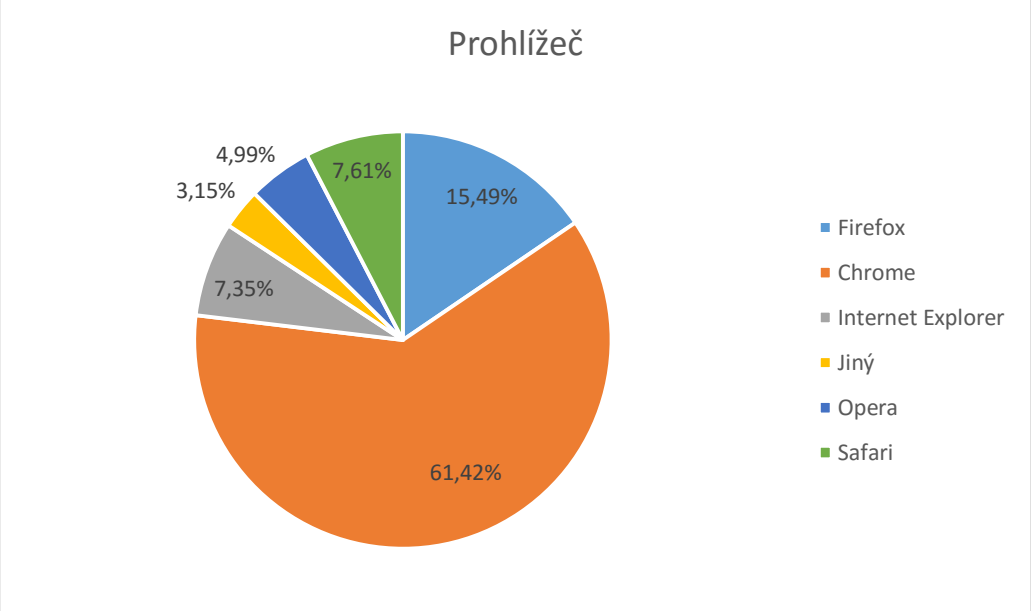
Otázka č. 1: V jakém prohlížeči máte otevřený tento dotazník?

Kategorie	Absolutní hodnota	Relativní četnost	Kumulativní četnost
Firefox	59	15,49%	15,49%
Chrome	234	61,42%	76,90%
Internet Explorer	28	7,35%	84,25%
Jiný	12	3,15%	87,40%
Opera	19	4,99%	92,39%
Safari	29	7,61%	**100,00%**
Celkem	**381**	**100,00%**	

Tabulka 12: Používaný prohlížeč

Zdroj: Vlastní zpracování

Nejpoužívanějším prohlížečem mezi respondenty byl jednoznačně Chrome s 234 (61,42 %) odpověďmi, což dokazují i statistiky o používanosti prohlížečů.[11] Dalším prohlížečem byl Firefox, který používá 59 (15,49 %) respondentů. Safari používalo 29 (7,61 %) odpovídajících, Operu pak 19 (4,99 %) respondentů. Možnost jiný prohlížeč využilo 12 (3,15 %) odpovídajících.



Graf 4: Používaný prohlížeč

Zdroj: Vlastní zpracování

[11] *StatCounter Global Stats - Browser, OS, Search Engine including Mobile Usage Share*[online]. StatCounter, 2016 [cit. 2016-03-20]. Dostupné z: http://gs.statcounter.com/

Otázka č. 2: Jaká je Vaše znalost informačních technologií?

Kategorie	Absolutní hodnota	Relativní četnost	Kumulativní četnost
Základní	52	13,65%	13,65%
Uživatelská	206	54,07%	67,72%
Nadstandardní uživatelská	72	18,90%	81,10%
Odborná	51	13,39%	**100,00%**
Celkem	**381**	**100,00%**	

Tabulka 13: Znalost informačních technologií

Zdroj: Vlastní zpracování

Více jak polovina respondentů 206 (54,07 %) uvádí, že jejich znalost informačních technologií je uživatelská. Nadstandardní uživatelskou znalost zvolilo 72 (18,9 %) odpovídajících. Základní znalost uvádí 52 (13,65 %) respondentů a odbornou pak 51 (13,39 %) odpovídajících. V současné době se nelze vyhnout kontaktu s chytrými zařízeními, neboť se stala běžnou součástí každodenního života. Základní znalost informačních technologií je vyučována již na základních školách a později je rozvíjena v závislosti na zájmu uživatele. Z toho lze usuzovat, že uživatelská znalost se stala všeobecným standardem.

Otázka č. 3: Jak často využíváte internetové připojení?

Kategorie	Absolutní hodnota	Relativní četnost	Kumulativní četnost
Denně	380	99,74%	99,74%
2-3x za týden	1	0,26%	**100,00%**
1x za týden	0	0,00%	
Méně než 1x za týden	0	0,00%	
Vůbec	0	0,00%	
Celkem	**381**	**100,00%**	

Tabulka 14: Používanost internetového připojení

Zdroj: Vlastní zpracování

Z dotazníkového šetření vyplynulo, že kromě jednoho odpovídajícího využívá každodenního internetového připojení 380 (99,74 %) oslovených respondentů. Tento fakt lze odůvodnit tím, že dotazník byl vyplňován právě internetově aktivními uživateli. Zároveň se internet stal nezbytnou součástí života a jeho každodenní využívání lze považovat za samozřejmost.

Otázka č. 4: Zajímáte se o bezpečnost Vašich dat?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	313	82,15%
Ne	68	17,85%
Celkem	**381**	**100,00%**

Tabulka 15: Zájem o bezpečnost dat
Zdroj: Vlastní zpracování

Z celkového množství respondentů jich 313 (82,15 %) uvedlo, že se zajímá o bezpečnost svých dat. Naopak 68 (17,85 %) odpovídajících uvedlo, že se o bezpečnost poskytnutých dat nezajímá. Toto zjištění si lze vysvětlit tak, že s přibývajícími kráděžemi osobních dat se uživatelé začínají více zajímat o jejich bezpečnost.

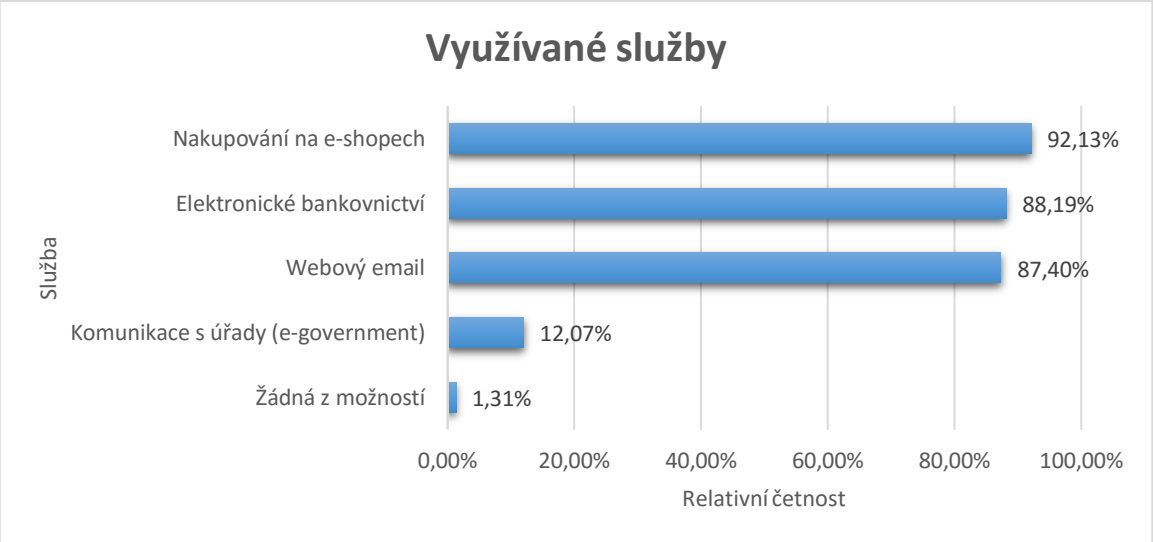
Otázka č. 5: Využíváte některé z těchto služeb?

Kategorie	Absolutní hodnota	Relativní četnost
Nakupování na e-shopech	351	92,13%
Elektronické bankovnictví	336	88,19%
Komunikace s úřady (e-government)	46	12,07%
Webový e-mail	333	87,40%
Žádná z možností	5	1,31%

Tabulka 16 : Využívanost internetových služeb

Zdroj: Vlastní zpracování

Tato otázka nabízela respondentům označení více možností a byla stanovená pro zjištění využívaných služeb mezi respondenty. Jmenované služby byly vybrány z toho důvodu, že při jejich používání se uživatelé museli setkat se zabezpečeným připojením a tudíž i s digitálním certifikátem. Nakupování na e-shopu využívá 351 (92,13 %), elektronické bankovnictví 336 (88,19 %) odpovídajících, webový e-mail 333 (87,4 %) respondentů. Komunikace s úřady není mezi uživateli ještě příliš rozšířena a preferují tedy osobní kontakt, jelikož tuto možnost označilo pouze 46 (12,07 %) respondentů. Webový e-mail je dnes považován za základní nástroj komunikace a se zrychlujícím se životním stylem zároveň roste obliba e-shopů a elektronického bankovnictví, neboť tyto služby šetří čas uživatelů. Žádnou z možností uvedlo 5 (1,31 %) respondentů.



Graf 5: Využívanost služeb

Zdroj: Vlastní zpracování

Otázka č. 6: Zobrazí se Vám bez problému webová prezentace po kliknutí na: https://goo.gl/TYFtzV ?

Filtrační a současně klíčová otázka, která sloužila k rozlišení, zda respondenti vnímají nedůvěryhodný certifikát jako problém či nikoliv. Po kliknutí na odkaz se zobrazila varovná obrazovka (viz Příloha O) a záleželo pouze na respondentovi, zda varovnou hlášku označil za problém či ji obešel. Je také nutné zmínit, že každý prohlížeč zobrazuje varovnou hlášku jiným způsobem a taktéž je požadována různá náročnost na její obejití, i proto byla v dotazníku zvolena otázka č. 1 – aktuálně používaný prohlížeč.

Kategorie	Absolutní hodnota	Relativní četnost
Ano	47	12,34%
Ne	334	87,66%
Celkem	**381**	**100,00%**

Tabulka 17: Bezproblémové zobrazení webové stránky

Zdroj: Vlastní zpracování

Z průzkumného šetření vyplynulo, že 47 (12,34 %) respondentů nenarazilo na žádný problém při zobrazování webové prezentace, a jako další krok v dotazníku je čekalo zodpovězení ověřovací otázky č. 7. Naopak 334 (87,66 %) odpovídajících zjistilo problém při zobrazení webové prezentace. Tato skupina odpovídajících měla zapsat vnímaný problém do otázky č. 8.

Otázka č. 7: Jaký obsah jste nalezl/a na webové prezentaci?

V případě, že respondent varovnou hlášku prohlížeče obešel, zobrazila se mu webová prezentace obsahující obrázek štěňátek (viz Příloha P). Účelem obrázku bylo ověřit předchozí odpověď respondenta.

Kategorie	Absolutní hodnota	Relativní četnost	Validní četnost
Obrázek koťátek	4	1,04%	8,51%
Obrázek štěňátek	30	7,83%	63,83%
Chybovou hlášku	12	3,13%	25,53%
Obrázek hříbátek	1	0,26%	2,13%
Obrázek telátek	0	0,00%	0,00%
Dílčí celek	**47**	**12,27%**	**100,00%**
Chybějící odpovědi	**336**	**87,73%**	
Celkem	**383**	**100,00%**	

Tabulka 18: Nalezený obsah na webové stránce

Zdroj: Vlastní zpracování

Ze 47 (100 %) respondentů, kteří na webové stránce nezaregistrovali problém a obešli varovnou hlášku, jich 30 (63,83 %) zvolilo správnou odpověď obrázek štěňátek. Respondenti, kteří zvolili možnost obrázek koťátek nebo hříbátek, celkem 5 (10,64 %), se

zmílili a pouze hádali. Ovšem 12 (25,53 %) odpovídajících zvolilo možnost, že na webové stránce nalezli chybovou hlášku, tzn., že varovnou hlášku nevnímají jako problém, ale jako správný obsah stránky.

Otázka č. 8: Na jaký problém jste narazil/a?

Otevřená otázka, jejíž odpovědi byly následně kategorizovány dle popsaného problému. Odpovědi se příliš nelišily, a proto vznikly pouze 4 kategorie.

Kategorie	Absolutní hodnota	Relativní četnost	Validní četnost
Nedůvěryhodný certifikát	48	12,60%	14,37%
Připojení není soukromé	246	64,57%	73,65%
Nezobrazila se	36	9,45%	10,78%
Neotvírám neznámé odkazy	4	1,05%	1,20%
Dílčí celek	**334**	**87,66%**	**100,00%**
Chybějící odpovědi	**47**	**12,34%**	
Celkem	**381**	**100,00%**	

Tabulka 19: Vnímaný problém webové stránky

Zdroj: Vlastní zpracování

Z 334 (100 %) respondentů, kteří vnímali problém na webové prezentaci, jich 246 (73,65 %) odpovědělo, že jejich připojení není soukromé či důvěryhodné, což odpovídá varovné hlášce v prohlížečích Chrome či Firefox. Vnímaný problém nedůvěryhodný či neplatný certifikát zvolilo 48 (14,37 %) odpovídajících, což odpovídá varovné hlášce v prohlížeči Opera či Internet Explorer. Dále 36 (10,78 %) respondentů uvedlo, že se jim stránka nezobrazila. Z toho lze určit, že varovnou hlášku a nedůvěryhodný certifikát nevnímali jako problém, ale zároveň ho nebrali jako správný obsah stránky. Zajímavou odpovědí u čtyř (1,2 %) respondentů bylo, že neklikají na neznámé odkazy. Toto řešení lze považovat za překvapivé, jelikož tímto způsobem uživatelé ignorují například většinu reklam, kdy je využito právě služeb zkracovačů pro zjištění, kolik zákazníků jim daný odkaz přinesl na webovou stránku.

Otázka č. 9: Byl/a jste někdy zabezpečeně přípojen?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	226	59,32%
Ne	5	1,31%
Nejsem si jistý/á	150	39,37%
Celkem	**381**	**100,00%**

Tabulka 20: Četnost zabezpečeně připojených respondentů

Zdroj: Vlastní zpracování

Z celkového počtu respondentů jich někdy bylo zabezpečeně připojeno 226 (59,32 %). Naopak 5 (1,31 %) odpovídajících uvádí, že nikdy nebyli zabezpečeně připojeni.

Z odpovědi nejsem si jistý/á, kterou zvolilo 150 (39,97 %) respondentů, lze předpokládat, že tento počet uživatelů nedokáže identifikovat zabezpečené a nezabezpečené připojení.

Otázka č. 10: Všiml/a jste si někdy zbarvení v řádce s adresou webové stránky?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	312	81,89%
Ne	38	9,97%
Nejsem si jistý/á	31	8,14%
Celkem	**381**	**100,00%**

Tabulka 21: Vnímání zbarvení v řádce s adresou webové stránky

Zdroj: Vlastní zpracování

Výsledky dotazníkového šetření ukazují, že výrazná většina respondentů si všímá zbarvení řádky s webovou adresou, téměř 312 (81,89 %) účastníků se vyjádřilo v tomto ohledu kladně. Naopak 38 (9,97 %) odpovídajících této charakteristice nevěnuje pozornost a 31 (8,14 %) uživatelů si není zbarvením jisto. Je důležité zohlednit fakt, že i zde záleží na používaném prohlížeči, jelikož některé zbarvují celou řádku adresy a jiné naopak pouze text HTTPS.

Otázka č. 11: Víte, proč se řádka s webovou adresou zbarvila?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	217	56,96%
Ne	99	25,98%
Nejsem si jistý/á	65	17,06%
Celkem	**381**	**100,00%**

Tabulka 22: Znalost důvodu zbarvení v řádce s URL adresou

Zdroj: Vlastní zpracování

V průzkumném šetření se 217 (56,96 %) respondentů vyjádřilo, že znají důvod zbarvení řádky webové adresy. Opačný názor vyjádřilo 99 odpovídajících (25,98 %) a odpověď nejsem si jistý/á označilo 65 (17,06 %) respondentů. Z počtu negativních odpovědí (Ne, Nejsem si jistý/á) lze usuzovat, že povědomí o významu zbarvení řádky s adresou není dostatečné.

Otázka č. 12: Při připojení k zabezpečenému webu se webová adresa změní na HTTPS, víte, co to znamená?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	179	46,98%
Ne	140	36,75%
Nejsem si jistý/á	62	16,27%
Celkem	**381**	**100,00%**

Tabulka 23: Znalost HTTPS

Zdroj: Vlastní zpracování

Skoro polovina, konkrétně 179 (46,98 %) odpovídajících uvedlo, že vědí, co znamená HTTPS. Avšak opačně odpovědělo 140 (36,75 %) respondentů a 62 (16,27 %) odpovídajících si není jisto významem tohoto protokolu. Jelikož protokol HTTPS slouží pro zabezpečené připojení, měly by být počty kladných odpovědí u otázky č. 9 a č. 12 podobné. Nižší počet respondentů znajících protokol HTTPS vypovídá o tom, že znalost významu této zkratky není příliš rozšířená.

Otázka č. 13: Víte, co znamená spojení SSL/TLS?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	83	21,78%
Ne	248	65,09%
Nejsem si jistý/á	50	13,12%
Celkem	**381**	**100,00%**

Tabulka 24: Znalost SSL/TLS

Zdroj: Vlastní zpracování

Výsledek této otázky v dotazníkovém šetření ukazuje, že většina 248 (65,09 %) respondentů nezná význam spojení SSL/TLS, což je pravděpodobně způsobeno nízkou znalostí informačních technologií. Významem spojení si není jisto 50 (13,12 %) odpovídajících. 83 (21,78 %) respondentů vyjádřilo, že zná význam tohoto spojení.

Otázka č. 14: Už jste někdy ověřoval/a | zkoumal/a digitalní certifikát?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	114	29,92%
Ne	242	63,52%
Nejsem si jistý/á	25	6,56%
Celkem	**381**	**100,00%**

Tabulka 25: Četnost ověřování/zkoumání certifikátu

Zdroj: Vlastní zpracování

Průzkumné šetření ukázalo, že 242 (63,52 %) respondentů nikdy neověřovalo nebo si neprohlíželo digitální certifikát. Otázkou je, zda vůbec vědí, co si pod tímto názvem

představit. Avšak 114 (29,92 %) odpovídajících již někdy zkoumalo digitální certifikát a názor nejsem si jistý/á vyjádřilo 25 (6,56 %) respondentů.

Otázka č. 15: Víte, co znamená varovná hláška "Certifikát zabezpečení předložený tímto webem nebyl vydán důvěryhodným certifikačním úřadem."?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	155	40,68%
Ne	139	36,48%
Nejsem si jistý/á	87	22,83%
Celkem	**381**	**100,00%**

Tabulka 26: Pochopení významu varovné zprávy

Zdroj: Vlastní zpracování

Otázka zkoumala význam varovné hlášky z prohlížeče Internet Explorer mezi uživateli. Z celkového počtu respondentů se jich 155 (40,68 %) vyjádřilo, že vědí, co tato hláška znamená. Naopak 139 (36,48 %) odpovídajích neví co si představit pod totou varovnou hláškou. Odpověď nejsem si jistý/á zvolilo 87 (22,83 %) respondentů.

Otázka č. 16: Víte, jak obejít varovnou zprávu v případě nedůvěryhodného či neplatného certifikátu?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	157	41,21%
Ne	173	45,41%
Nejsem si jistý/á	51	13,39%
Celkem	**381**	**100,00%**

Tabulka 27: Schopnost obejít varovnou zprávu

Zdroj: Vlastní zpracování

Skoro polovina respondentů, konkrétně 173 (45,41 %), neví, jakým způsobem se obchází varovná hláška prohlížeče, což je zajímavý fakt. Ovšem i zde záleží na typu prohlížeče, jelikož některé vyžadují větší náročnost na obejití hlášky, jiné naopak menší. Opačné znalosti mělo 157 (41,21 %) odpovídajících, kteří vědí, jak hlášku obejít. Názor nejsem si jistý/á vyjádřilo 51 (13,39 %) respondentů.

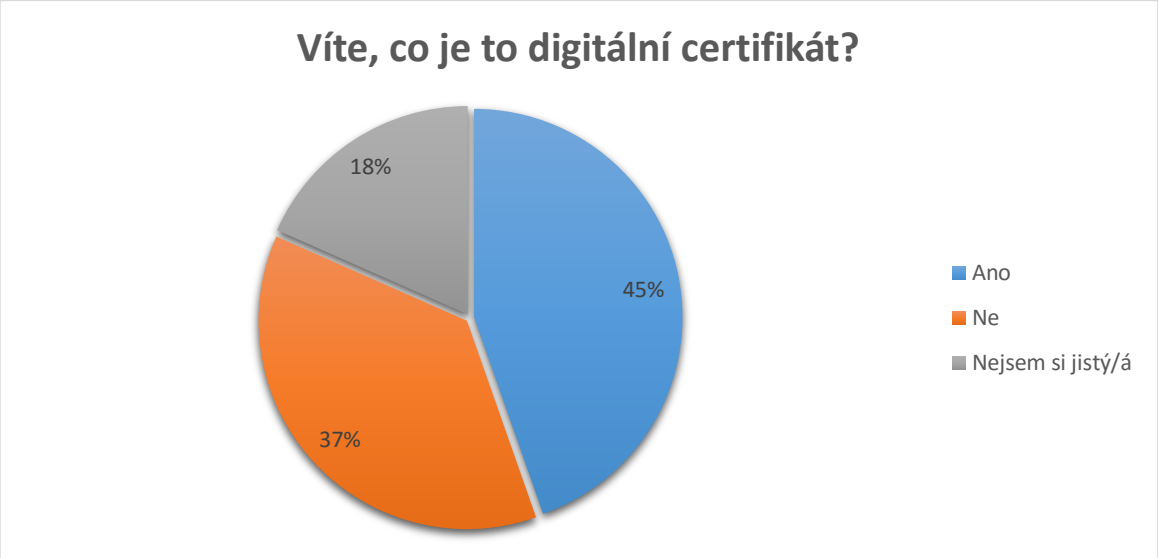
Otázka č. 17: Víte, co je to digitální certifikát?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	170	44,62%
Ne	141	37,01%
Nejsem si jistý/á	70	18,37%
Celkem	**381**	**100,00%**

Tabulka 28: Znalost významu digitálního certifikátu

Zdroj: Vlastní zpracování

Podstatná otázka zjišťující, zda vůbec respondenti vědí, co je to vlastně digitální certifikát. Dotazníkové šetření zjistilo, že 170 (44,62 %) odpovídajících zná digitální certifikát. Naopak 141 (37,01 %) respondentů označilo, že neví co si pod tímto názvem představit. Odpověď nejsem si jistý/á zvolilo 70 (18,37 %) dotázaných. Toto zjištění opět potvrzuje, že povědomí o digitálních certifikátech není dostatečné.



Graf 6: Znalost významu digitálního certifikátu

Zdroj: Vlastní zpracování

Otázka č. 18: Víte, jak spravovat digitální certifikáty?

Kategorie	Absolutní hodnota	Relativní četnost
Ano	80	21,00%
Ne	263	69,03%
Nejsem si jistý/á	38	9,97%
Celkem	**381**	**100,00%**

Tabulka 29: Znalost spravování digitálních certifikátů

Zdroj: Vlastní zpracování

Většina respondentů, konkrétně 263 (69,03 %) neví, kde nalézt úložiště důvěryhodných certifikátů a jak jej spravovat. Ovšem 80 (21 %) odpovídajících naopak ví, kde a jak spravovat certifikáty. Názor nejsem si jistý/á označilo 38 (9,97 %) respondentů.

4.2.8 Testování a ověřování hypotéz

K testování hypotéz byl zvolen Pearsonův chí-kvadrát test a hodnota 0,5 jako hladina významnosti. Jelikož tento test musí splňovat podmínku dobré aproximace (tj. alespoň 80 % teoretických četností by mělo být větší než 5), muselo dojít u několika otázek ke změnám rozložení:

- **otázka č. 10** – Všiml/a jste si někdy zbarvení v řádce s adresou webové stránky? – odpověď „nejsem si jistý/á“ byla sloučena s odpovědí „ne“, jelikož buď si uživatel někdy všiml, nebo nevšiml.
- **otázka č. 9** – Byl/a jste někdy zabezpečené připojen/a? – odpověď „Ne“ zvolilo pouze 5 respondentů, kdežto „Nejsem si jistý/á“ 150 respondentů, byly proto sloučeny do položky „Nejsem si jistý/á“.
- **otázka č. 19** – Jaký je Váš věk? – sloučení některých kategorií věku, aby obsahovaly úměrné množství respondentů (do 15, 16–20 → do 20; 36–40, 41–45, 46 a více → 36 a více)
- **otázka č. 1** – V jakém prohlížeči máte otevřený tento dotazník? – v rámci hypotézy č. 7 byl zařazen prohlížeč Opera do odpovědi Jiný, jelikož byl mezi používanými prohlížeči zvolen nejméně respondenty

Hypotéza č. 1:

$1H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi používaným internetovým prohlížečem a povšimnutím si zbarvení řádky adresy webové stránky.

$1H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi používaným internetovým prohlížečem a povšimnutím si zbarvení řádky adresy webové stránky.

Prohlížeč		Povšimnutí si zbarvení řádky		
		Ano	**Ne**	**Celkem**
Chrome	absolutní četnost	204	30	**234**
	řádková procenta	87,18 %	12,82 %	
Firefox	absolutní četnost	45	14	**59**
	řádková procenta	76,27 %	23,73 %	
Internet Explorer	absolutní četnost	20	8	**28**
	řádková procenta	71,43 %	28,57 %	
Jiný	absolutní četnost	8	4	**12**
	řádková procenta	66,67 %	33,33%	
Opera	absolutní četnost	11	8	**19**
	řádková procenta	57,89 %	42,11 %	
Safari	absolutní četnost	24	5	**29**
	řádková procenta	82,76 %	17,24 %	
Celkem	absolutní četnost	**312**	**69**	**381**
	relativní četnost	**81,89 %**	**18,11 %**	**100 %**

Tabulka 30: Kontingenční tabulka vztahu otázek č. 1 a č. 10

Zdroj: Vlastní zpracování

Ve všech prohlížečích se nejvíce projevuje zbarvení EV certifikátu. Ostatní druhy certifikátů v prohlížečích Safari, Internet Explorer a Firefox nevyvolávají žádné zbarvení, pouze umístění ikony zámečku. Přesto však poměrově si nejvíce zbarvení řádky povšimli uživatelé Chrome (87,18 %), Safari (82,76 %) a Firefoxu (76,27 %). Naopak nejméně uživatelé Opery (57,89 %).

Statistika	DF	Hodnota	P
Chi-kvadrát test	5	17,0033	0,0045
Cramerovo V		0,2113	

Tabulka 31: Statistické vyhodnocení vztahu otázek č. 1 a č. 10

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,0045, která je menší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že se zamítá nulová hypotéza a přijímá se hypotéza alternativní. Mezi používaným prohlížečem a povšimnutím si zbarvení řádky s webovou adresou existuje statisticky významný vztah se slabou závislostí 0,21.

Hypotéza č. 2:

$2H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi povšimnutím si zbarvení řádky adresy webové stránky a zájmem uživatele o bezpečnost svých dat.

$2H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi povšimnutím si zbarvení řádky adresy webové stránky a zájmem uživatele o bezpečnost svých dat.

Povšimnutí si zbarvení řádky		Zájem o bezpečnost svých dat		
		Ano	**Ne**	**Celkem**
Ano	absolutní četnost	265	47	**312**
	relativní četnost	69,55 %	12,34 %	**81,89 %**
Ne	absolutní četnost	48	21	**69**
	relativní četnost	12,60 %	5,51 %	**18,11 %**
Celkem	absolutní četnost	**313**	**68**	**381**
	relativní četnost	**82,15 %**	**17,85 %**	**100** %

Tabulka 32: Kontingenční tabulka vztahu otázek č. 10 a č. 4

Zdroj: Vlastní zpracování

Dá se očekávat, že pokud se uživatel zajímá o bezpečnost svých poskytnutých dat, měl by si všímat zbarvení řádky webové adresy. Respondentů, kteří si všimli zbarvení, bylo celkem 312 (81,89 %) a 265 z nich odpovědělo, že se zajímají o bezpečnost svých dat. Naopak 48 (12,6 %) respondentů má sice zájem o bezpečnost svých dat, ale nevšimlo si zbarvení řádky, což může být například způsobeno používaným prohlížečem.

Statistika	DF	Hodnota	P
Chi-kvadrát test	1	9,1046	0,0025
Cramerovo V		0,1546	

Tabulka 33: Statistické vyhodnocení vztahu otázek č. 10 a č. 4

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,0025, která je menší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že se zamítá nulová hypotéza a přijímá se hypotéza alternativní. Mezi povšimnutím si zbarvení řádky s webovou adresou a zájmem o bezpečnost svých poskytnutých dat existuje statisticky významný vztah se slabou závislostí 0,15.

Hypotéza č. 3:

$3H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi zabezpečeně připojeným uživatelem a jím ověřeným digitálním certifikátem.

$3H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi zabezpečeně připojeným uživatelem a jím ověřeným digitálním certifikátem.

Byl/a jste zabezpečeně připojen/a		Ověřoval/a jste někdy digitální certifikát			
		Ano	**Ne**	**Nejsem si jistý/á**	**Celkem**
Ano	absolutní četnost	97	111	18	**226**
	relativní četnost	25,46 %	29,13 %	4,72 %	**59,32** %
Nejsem si jistý/á	absolutní četnost	17	131	7	**155**
	relativní četnost	4,46 %	34,38 %	1,84 %	**40,68** %
Celkem	absolutní četnost	**114**	**242**	**25**	**381**
	relativní četnost	**29,92** %	**63,52** %	**6,56** %	**100** %

Tabulka 34: Kontingenční tabulka vztahu otázek č. 9 a č. 14

Zdroj: Vlastní zpracování

U vztahu těchto otázek se dá očekávat, že pokud někdy uživatel ověřoval či zkoumal digitální certifikát, pak byl zabezpečeně připojený. Dle průzkumného šetření certifikát ověřovalo celkem 114 (29,92 %) respondentů a z toho jich 97 označilo, že někdy byli zabezpečeně připojeni. Ostatních 17 odpovídajících nejspíše nerozezná rozdíl mezi zabezpečeným a nezabezpečeným připojením. Více odpovědí (63,52 %) zaznamenala možnost, že respondent neověřoval digitální certifikát, což může být způsobeno neznalostí významu nebo cesty k zobrazení certifikátu.

Statistika	DF	Hodnota	P
Chi-kvadrát test	2	51,1796	<0,0001
Cramerovo V		0,3665	

Tabulka 35: Statistické vyhodnocení vztahu otázek č. 9 a č. 14

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P<0,0001, která je menší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že se zamítá nulová hypotéza a přijímá se hypotéza alternativní. Mezi zabezpečeně připojeným uživatelem a jím ověřeným digitálním certifikátem existuje statisticky významný vztah se střední závislostí 0,37.

Hypotéza č. 4:

$4H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi věkem uživatele a jeho zájmem o bezpečnost svých dat.

$4H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi věkem uživatele a jeho zájmem o bezpečnost svých dat.

Věková kategorie		Zájem o bezpečnost svých dat		
		Ano	**Ne**	**Celkem**
do 20 let	absolutní četnost	31	12	**43**
	relativní četnost	8,14 %	3,15 %	**11,29 %**
	řádková procenta	72,09 %	27,91 %	
21–25 let	absolutní četnost	190	34	**224**
	relativní četnost	49,87 %	8,92 %	**58,79 %**
	řádková procenta	84,82 %	15,18 %	
26–30 let	absolutní četnost	46	13	**59**
	relativní četnost	12,07 %	3,41 %	**15,49 %**
	řádková procenta	77,97 %	22,03 %	
31–35 let	absolutní četnost	24	4	**28**
	relativní četnost	6,30 %	1,05 %	**7,35 %**
	řádková procenta	85,71 %	14,29 %	
36 a více let	absolutní četnost	22	5	**27**
	relativní četnost	5,77 %	1,31 %	**7,09 %**
	řádková procenta	81,48 %	18,52 %	
Celkem	absolutní četnost	**313**	**68**	**381**
	relativní četnost	**82,15** %	**17,85** %	**100 %**

Tabulka 36: Kontingenční tabulka vztahu otázek č. 19 a č. 4

Zdroj: Vlastní zpracování

Vztah, jehož úkolem je posoudit, zda se některá věková kategorie zajímá více o bezpečnost svých poskytnutých dat. Z průzkumného šetření vyplynulo, že o bezpečnost svých dat se zajímá celkem 313 (82,15 %) respondentů. Nejvíce dbají na bezpečnost svých dat respondenti ve věkové kategorii 31–35 let (85,71 %) a 21–25 (84,82 %) let, naopak nejméně odpovídající do 20 let (72,09 %).

Statistika	DF	Hodnota	P
Chi-kvadrát test	4	5,0117	0,2861

Tabulka 37: Statistické vyhodnocení vztahu otázek č. 19 a č. 4

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,2861, která je větší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že nulovou hypotézu nelze zamítnout. Mezi věkem uživatele a jeho zájmem o bezpečnost svých dat neexistuje statisticky významný vztah.

Hypotéza č. 5:

5H_0: Lze předpokládat, že neexistuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a jím ověřeným digitálním certifikátem.

5H_A: Lze předpokládat, že existuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a jím ověřeným digitálním certifikátem.

Zájem o bezpečnost svých dat		Ověřoval/a jste někdy digitální certifikát			
		Ano	**Ne**	**Nejsem si jistý/á**	**Celkem**
Ano	absolutní četnost	102	189	22	**313**
	relativní četnost	26,77 %	49,61 %	5,77 %	**82,15 %**
Ne	absolutní četnost	12	53	3	**68**
	relativní četnost	3,15 %	13,91 %	0,79 %	**17,85 %**
Celkem	absolutní četnost	**114**	**242**	**25**	**381**
	relativní četnost	**29,92** %	**63,52** %	**6,56** %	**100 %**

Tabulka 38: Kontingenční tabulka vztahu otázek č. 4 a č. 14

Zdroj: Vlastní zpracování

Pokud se uživatel zajímá o bezpečnost svých dat, pak se dá očekávat, že již někdy ověřoval či zkoumal digitální certifikát. Zájem o bezpečnost svých dat vyjádřilo celkem 313 (82,15 %) respondentů, avšak pouze 102 z nich již někdy ověřovalo digitální certifikát. Zbylý počet, tedy 189 odpovídajích, certifikát neověřovalo. Z tohoto faktu lze soudit, že tito respondeti mají sice zájem o bezpečnost svých poskytnutých dat, ale pouze v malé míře.

Statistika	DF	Hodnota	P
Chi-kvadrát test	2	7,4621	0,0240
Cramerovo V		0,1399	

Tabulka 39: Statistické vyhodnocení vztahu otázek č. 4 a č. 14

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,0240, která je menší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že se

zamítá nulová hypotéza a přijímá se hypotéza alternativní. Mezi zájmem uživatele o bezpečnost dat a jím ověřeným digitálním certifikátem existuje statisticky významný vztah se slabou závislostí 0,14.

Hypotéza č. 6:

$6H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a schopností obejít varovnou zprávu.

$6H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a schopností obejít varovnou zprávu.

Bezproblémové zobrazení webové prezentace		Schopnost obejít varovnou zprávu			
		Ano	Ne	Nejsem si jistý/á	Celkem
Ano	absolutní četnost	21	22	4	**47**
	relativní četnost	5,51 %	5,77 %	1,05 %	**12,34** %
	řádková procenta	44,68 %	46,81 %	8,51 %	
Ne	absolutní četnost	136	151	47	**334**
	relativní četnost	35,70 %	39,63 %	12,34 %	**87,66** %
	řádková procenta	40,72 %	45,21 %	14,07 %	
Celkem	absolutní četnost	**157**	**173**	**51**	**381**
	relativní četnost	**41,21** %	**45,41** %	**13,39** %	**100** %

Tabulka 40: Kontingenční tabulka vztahu otázek č. 6 a č. 16

Zdroj: Vlastní zpracování

Lze očekávat, že pokud respondent zvolil možnost bezproblémového zobrazení webové prezentace, pak musel obejít varovnou hlášku. Tuto kombinaci zvolilo 21 (44,68 %) respondentů z těch, kteří na problém nenarazili. Zbylý počet (55,32 %) uvedl, že neví nebo si není jist, jak hlášku obejít. Bude se tak jednat o respondenty, kteří označili v ověřovací otázce špatný obrázek či varovnou zprávu jako obsah stránky. Z 334 (87,66 %) uživatelů, kteří zaznamenali problém při zobrazení webové stránky, jich 136 (40,72 %) ví, jakým způsobem obejít varovnou zprávu a naopak 151 (39,63 %) odpovídajích postup nezná.

Statistika	DF	Hodnota	P
Chi-kvadrát test	2	1,1321	0,5678

Tabulka 41: Statistické vyhodnocení vztahu otázek č. 6 a č. 16

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,5678, která je větší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že nulovou

hypotézu nelze zamítnout. Mezi bezproblémovým zobrazením webové prezentace a schopností obejít varovnou zprávu neexistuje statisticky významný vztah.

Hypotéza č. 7:

$7H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi používaným prohlížečem a schopností obejít varovnou zprávu.

$7H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi používaným prohlížečem a schopností obejít varovnou zprávu.

Prohlížeč		Schopnost obejít varovnou zprávu			
		Ano	**Ne**	**Nejsem si jistý/á**	**Celkem**
Chrome	absolutní četnost	91	112	31	**234**
	relativní četnost	23,88 %	29,40 %	8,14 %	**61,42 %**
	řádková procenta	38,89 %	47,86 %	13,25 %	
Firefox	absolutní četnost	34	16	9	**59**
	relativní četnost	8,92 %	4,20 %	2,36 %	**15,49 %**
	řádková procenta	57,63 %	27,12 %	15,25 %	
Internet Explorer	absolutní četnost	6	18	4	**28**
	relativní četnost	1,57 %	4,72 %	1,05 %	**7,35 %**
	řádková procenta	21,43 %	64,29 %	14,29 %	
Jiný	absolutní četnost	16	15	0	**31**
	relativní četnost	4,20 %	3,94 %	0,00 %	**8,14 %**
	řádková procenta	51,61 %	48,39 %	0,00 %	
Safari	absolutní četnost	10	12	7	**29**
	relativní četnost	2,62 %	3,15 %	1,84 %	**7,61 %**
	řádková procenta	34,48 %	41,38 %	24,14 %	
Celkem	absolutní četnost	**157**	**173**	**51**	**381**
	relativní četnost	**41,21 %**	**45,41** %	**13,39** %	**100 %**

Tabulka 42: Kontingenční tabulka vztahu otázek č. 1 a č. 16

Zdroj: Vlastní zpracování

Některé prohlížeče nabízí svým uživatelům snadnější přechod přes varovnou zprávu, jako například Internet Explorer, Opera či Safari, kde stačí pouze jedno kliknutí. V Chromu

je potřeba dvojího kliknutí – nejdříve odkrýt rozšířené nastavení a poté potvrdit. Zatímco ve Firefoxu je třeba dokonce trojího kliknutí.

Přesto výsledky dotazníkového šetření ukázaly, že přechod přes varovnou zprávu nejvíce zvládají uživatelé Firefoxu (57,63 %), což může být dáno tím, že tento prohlížeč je využíván spíše uživateli s většími znalostmi informačních technologií. Překvapivým výsledkem je, že 64,29 % uživatelů Internet Exploreru nezná postup na obejití zprávy, i přes to, že principem je pouze jedno kliknutí. To může být dáno tím, že Internet Explorer je standardním prohlížečem, který není příliš oblíbený. Většina uživatelů s většími informačními znalostmi používá uživatelsky přístupnější prohlížeče. U nejvíce využívaného prohlížeče mezi respondenty (Chrome – 61,42 %) se skoro polovina (47,86 %) vyjádřila, že taktéž neovládá postup k obejití hlášky, který je zde ovšem složitější.

Statistika	DF	Hodnota	P
Chi-kvadrát test	8	21,8036	0,0053
Cramerovo V		0,1692	

Tabulka 43: Statistické vyhodnocení vztahu otázek č. 1 a č. 16

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,0053, která je menší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že se zamítá nulová hypotéza a přijímá se hypotéza alternativní. Mezi používaným prohlížečem a schopností obejít varovnou zprávu existuje statisticky významný vztah se slabou závislostí 0,17.

Hypotéza č. 8:

$8H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a schopností spravovat uložené digitální certifikáty.

$8H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi zájmem uživatele o bezpečnost svých dat a schopností spravovat uložené digitální certifikáty.

Zájem o bezpečnost svých dat		Schopnost spravovat digitální certifikáty			
		Ano	**Ne**	**Nejsem si jistý/á**	**Celkem**
Ano	absolutní četnost	75	204	34	**313**
	relativní četnost	19,69 %	53,54 %	8,92 %	**82,15 %**
	řádková procenta	23,96 %	65,18 %	10,86 %	
Ne	absolutní četnost	5	59	4	**68**
	relativní četnost	1,31 %	15,49 %	1,05 %	**17,85 %**
	řádková procenta	7,35 %	86,76 %	5,88 %	
Celkem	absolutní četnost	**80**	**263**	**38**	**381**
	relativní četnost	**21,00 %**	**69,03 %**	**9,97 %**	**100 %**

Tabulka 44: Kontingenční tabulka vztahu otázek č. 4 a č. 18

Zdroj: Vlastní zpracování

Dá se očekávat, že pokud se uživatel zajímá o bezpečnost svých poskytnutých dat, pak by si také měl umět ověřit, jakým certifikačním autoritám je standardně v úložišti vyslovena důvěra. Ovšem v průzkumném šetření 313 (82,15 %) respondentů vyjádřilo zájem o bezpečnost svých dat, avšak pouze 75 (23,96 %) z nich uvedlo, že ví, jakým způsobem spravovat uložené certifikáty. Ostatních 204 (65,18 %) odpovídajících vyjádřilo opačný názor. Z tohoto faktu lze soudit, že tito respondenti mají sice zájem o bezpečnost svých poskytnutých dat, ale pouze v malé míře.

Statistika	DF	Hodnota	P
Chi-kvadrát test	2	12,5001	0,0019
Cramerovo V		0,1811	

Tabulka 45: Statistické vyhodnocení vztahu otázek č. 4 a č. 18

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,0019, která je menší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že se zamítá nulová hypotéza a přijímá se hypotéza alternativní. Mezi zájmem uživatele o bezpečnost svých dat a schopností spravovat uložené digitální certifikáty existuje statisticky významný vztah se slabou závislostí 0,18.

Hypotéza č. 9:

$9H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a znalostmi informačních technologií.

$9H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a znalostmi informačních technologií.

Znalost informačních technologií		Bezproblémové zobrazení webové stránky		
		Ano	**Ne**	**Celkem**
Základní	absolutní četnost	5	47	**52**
	relativní četnost	1,31 %	12,34 %	**13,65** %
	řádková procenta	9,62 %	90,38 %	
Uživatelská	absolutní četnost	23	183	**206**
	relativní četnost	6,04 %	48,03 %	**54,07** %
	řádková procenta	11,17 %	88,83 %	
Nadstandardní uživatelská	absolutní četnost	10	62	**72**
	relativní četnost	2,62 %	16,27 %	**18,90** %
	řádková procenta	13,89 %	86,11 %	
Odborná	absolutní četnost	9	42	**51**
	relativní četnost	2,36 %	11,02 %	**13,39** %
	řádková procenta	17,65 %	82,35 %	
Celkem	absolutní četnost	**47**	**334**	**381**
	relativní četnost	**12,34** %	**87,66** %	**100** %

Tabulka 46: Kontingenční tabulka vztahu otázek č. 2 a č. 6

Zdroj: Vlastní zpracování

Dle dotazníkového šetření bylo nejvíce respondentů, konkrétně 206 (54,07 %) s uživatelskou znalostí informační technologií, z nichž 183 (88,83 %) nalezlo problém při zobrazování webové prezentace. Při porovnání řádkových procent je ve všech kategoriích přibližně stejně velký poměr respondentů, kteří na problém narazili či nikoliv. Překvapivým výsledkem ovšem je, že nejvíce problém vnímalo 90,38 % z uživatelů ze základní znalostí a naopak nejméně 82,35 % z uživatelů s odbornou znalostí. Tento fakt si lze vysvětlit tím, že odborníci si nedůvěryhodný certifikát ověřili a poté ho příliš nevnímali jako problém, naopak od respondentů se základní znalostí, kteří byli překvapeni varovnou zprávou.

Statistika	DF	Hodnota	P
Chi-kvadrát test	3	2,1079	0,5503

Tabulka 47: Statistické vyhodnocení vztahu otázek č. 2 a č. 6

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,5503, která je větší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že nulovou

hypotézu nelze zamítnout. Mezi bezproblémovým zobrazením webové prezentace a znalostmi informačních technologií neexistuje statisticky významný vztah.

Hypotéza č. 10:

$10H_0$: Lze předpokládat, že neexistuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a chápáním významu varovné zprávy.

$10H_A$: Lze předpokládat, že existuje statisticky významný vztah mezi bezproblémovým zobrazením webové prezentace a chápáním významu varovné zprávy.

Pochopení významu varovné zprávy		Bezproblémové zobrazení webové stránky		
		Ano	**Ne**	**Celkem**
Ano	absolutní četnost	21	134	**155**
	relativní četnost	5,51 %	35,17 %	**40,68 %**
	řádková procenta	13,55 %	86,45 %	
Ne	absolutní četnost	19	120	**139**
	relativní četnost	4,99 %	31,50 %	**36,48 %**
	řádková procenta	13,67 %	86,33 %	
Nejsem si jistý/á	absolutní četnost	7	80	**87**
	relativní četnost	1,84 %	21,00 %	**22,83 %**
	řádková procenta	8,05 %	91,95 %	
Celkem	absolutní četnost	**47**	**334**	**381**
	relativní četnost	**12,34 %**	**87,66 %**	**100 %**

Tabulka 48: Kontingenční tabulka vztahu otázek č. 15 a č. 6

Zdroj: Vlastní zpracování

Z celkového počtu odpovídajících jich 155 (40,68 %) zvolilo, že rozumí varovné zprávě, a proto jich 134 (86,45 %) z nich vnímalo problém při zobrazování webové stránky. Pouze 21 (13,55 %) respondentů z této kategorie nevnímalo žádný problém, tudíž tuto hlášku museli ve svém prohlížeči obejít. Naopak 139 (36,48 %) respondentů z celkového počtu nerozumí této varovné hlášce, avšak 120 (86,33 %) z nich ji alespoň vnímá jako problém. Zbylý počet respondentů s nepochopeným významem zprávy, tedy 19 (13,67 %), nenarazilo při zobrazování stránky na žádný problém. Názor nejsem si jist/ý, tudíž nejspíše nepochopení některé z částí varovné zprávy, zvolilo 87 (22,83 %) lidí, z nichž 80 (91,95 %) ji vnímá jako problém při zobrazování webové prezentace.

Statistika	DF	Hodnota	P
Chi-kvadrát test	2	1,9197	0,3829

Tabulka 49: Statistické vyhodnocení vztahu otázek č. 15 a č. 6

Zdroj: Vlastní zpracování

Z testovaného vztahu mezi otázkami byla vypočtena hladina významnosti testu P=0,3829, která je větší než zvolená hladina 0,05. Z tohoto důvodu lze prohlásit, že nulovou hypotézu nelze zamítnout. Mezi bezproblémovým zobrazením webové prezentace a chápáním významu varovné zprávy neexistuje statisticky významný vztah.

5 Výsledky a diskuse

Při analýze kvalifikovaných certifikačních autorit bylo zjištěno, že všechny nabízejí jak komerční, tak kvalifikované certifikáty s dobou platností vždy 1 rok a bezplatným zneplatněním certifikátu. Cenová politika je u těchto autorit podobná, ovšem nejlevnější certifikáty lze získat u PostSignum, nejdražší naopak u I.CA. Dle certifikačních politik nabízí nejrychlejší vyřízení žádosti o certifikát I.CA (jeden pracovní den), dále PostSignum (dva pracovní dny) a eIdentity tuto informaci neuvádí. Zasádní výhodou autority PostSignum je počet registračních míst, kterých je celkem 976. U I.CA si zákazníci mohou vybrat ze 30 registračních autorit a u eIdentity pouze ze tří. Autorita eIdentity není standardně systémem Windows považována jako důvěryhodná na rozdíl od ostatních. První certifikační autoritu lze také zařadit mezi nejdůvěryhodnější autority, díky nejdelšímu působení na trhu i významným zákazníkům. Záleží tedy na preferencích žadatele, ovšem dle uvedených parametrů se jako nejlepší volba jeví I.CA.

Další variantou pro majitele domén je využití bezplatného důvěryhodného certifikátu. Detailněji byla popsána služba od společnosti Zoner a autorita Let's encrypt. Zatímco služba SSLmarket je založena českou společnosti Zoner a je pouze přeprodejcem certifikátů od světových certifikačních autorit, Let's encrypt je spravován skupinou ISRG a je založen na myšlence bezplatného šíření důvěryhodných certifikátů bez zbytečných překážek. Zoner spustil zkušební verzi poskytovaných důvěryhodných certifikátů od Symantec za podmínky, že doména bude převedena pod jeho registrátora. Platnost takového certifikátu se vztahuje na celou dobu platnosti domény. Avšak Let's encrypt je samotnou certifikační autoritou, jejíž certifikát byl podepsán jinou důvěryhodnou autoritou a sama tak bezplatně vystavuje důvěryhodné certifikáty. Vše se děje pouze nahráním a spuštěním skriptu na daném serveru a certifikát je vystavený s platností pouze 1 měsíc. Z hlediska bezpečnosti je tato délka platnost nejlepším řešením, a díky automatizovanému žádání o prodloužení certifikátu odpadá i starost o obnovu certifikátu. Z uvedených hledisek se lepší volbou zdá být autorita Let's Enrypt.

Vytvoření vlastní autority bylo provedeno s využitím softwarového programu XCA, kdy byly nejprve vygenerovány privátní klíče, vytvořena žádost o vydání certifikátu a následně vlastní certifikační autorita. Díky ní byla žádost schválena a podepsána. Poté byl vystavený certifikát nahrán na webový hosting, kde se však po zadání webové adresy zobrazila varovná hláška. Ta byla způsobena tím, že autorita byla vytvořená svépomocí,

tudíž její kořenový certifikát není obsažen v úložišti pro důvěryhodné kořenové certifikační autority. Webová stránka se tak stala praktickým příkladem využitým pro dotazníkové šetření.

Průzkumné šetření formou dotazníku, který obsahoval celkem 22 otázek, probíhalo od 6. března 2016 do 13. března 2016. Bylo realizováno online formou a zúčastnilo se ho celkem 383 respondentů. Z důvodů nesmyslných odpovědí musely být 2 dotazníky z celkového počtu odstraněny. Konečný soubor byl tedy tvořen 381 respondenty.

Nejčastějšími respondenty byli uživatelé ve věkové kategorii 21–25 let, což lze odůvodnit větší internetovou aktivitou mezi touto věkovou skupinou. Dále byli respondenti složeni z mírné převahy žen, což může být způsobeno jejich snahou o nápomoc druhým lidem. Nejvyšší dosažené vzdělání bylo skoro u poloviny odpovídajících středoškolské s maturitou a u 41,99 % vysokoškolské. Vysoký podíl takto vzdělaných lidí je způsoben tím, že dotazník byl primárně šířen mezi studenty vysokých škol používající každodenní internetové připojení. Nejčastějším oborem vzdělání byla možnost Jiný. Takto vysoký podíl si lze vysvětlit tím, že cíleně nebyly jmenovány veškeré dostupné obory, ale byly zařazeny do nadskupiny a například ekonomický obor se řadí mezi humanitní, ovšem dle výsledků většina respondentů volila právě možnost jiný.

Mezi nejpoužívanější prohlížeče se jednoznačně zařadil Chrome s 61,42% četností a druhý pak Firefox s 15,49% četností. Respondenti byli složeni z různých stupňů znalostí informačních technologiích, kdy více než polovina (54,07 %) měla uživatelskou znalost. Dotazníkové šetření dále ukázalo, že absolutní vetšina respondentů využívá každodenní internetové připojení. Zájem o bezpečnost svých poskytnutých dat vyjádřilo 82,15 % uživatelů. Vysoký počet respondentů využivá i nakupování na e-shopech (92,13 %), elektronické bankovnictví (88,19 %) či webový e-mail (87,4 %). Využití e-governmentu mezi uživateli ještě zaostává, jelikož jej využívá pouze 12,07 %.

Důležitou položkou byla filtrační otázka, která se dotazovala, zda respondent bezproblému zobrazí webovou prezentaci na odkazu, kde se právě skrýval nedůvěryhodný certifikát s varovnou hláškou. Významným prvkem u této otázky je i právě používaný prohlížeč, jelikož každý nabízí jinou náročnost pro obejití varovné zprávy. Dotazníkové šetření ukázalo, že 87,66 % respondentů vnímá nějaký problém při zobrazení a byli nuceni popsat vyskytovaný problém. Odpovědi byly následně kategorizovány, kdy 64,57 % respondentů uvedlo jako problém, že připojení není soukromé, což odpovídá

i zobrazovaným varovným hláškám některých z prohlížečů. Naopak 12,34 % odpovídajících, kteří na žádný problém při zobrazování stránky nenarazili, čekala kontrolní otázka, jaký obsah na webové stránce nalezli. Z celkového počtu správně zodpovědělo 63,83 % respondentů, ovšem 25,53 % zvolilo možnost, že obsahem byla chybová zpráva. Tento počet uživatelů tak nevnímá varovnou zprávu jako problém, ale jako správný obsah webové stránky.

Následovaly otázky zjišťující informovanost o zabezpečeném připojení. V průzkumném šetření se 59,32 % respondentů vyjádřilo, že již někdy byli zabezpečeně připojeni a 39,37 % vyjádřilo nejistý názor, který je pravděpodobně způsoben neidentifikováním zabezpečeného a nezabezpečeného připojení. Tento fakt lze porovnat s již uvedenými výsledky využiváných služeb, kde například elektronické bankovnictví využívá 88,19 % oslovených. Je však třeba si uvědomit, že zabezpečené připojení je základem každého elektronického bankovnictví. Lze tedy usoudit, že téměř třetina respondentů nemá dostatečné povědomí o zabezpečeném připojení.

Dále šetření zjistilo, že 81,89 % respondentů si někdy všimlo zbarvení řádky s webovou adresou, ovšem pouze 56,96 % odpovídajících ví, za jakým účelem se barva změnila. Je nutné poznamenat, že zbarvení se odlišuje dle využívaného prohlížeče. Následně bylo zjištěno, že skoro polovina respondentů (46,98 %) ví, co znamená protokol HTTPS. Následnou otázkou, která jde více do hloubky problematiky, však 65,09 % odpovídajících vyjádřilo, že nezná spojení SSL/TLS.

Poslední část dotazníkového šetření byla zaměřena přímo na digitální certifikáty, kde 63,52 % respondentů uvedlo, že nikdy neověřovali nebo nezkoumali digitální certifikát. Srozumitelnost varovné zprávy z prohlížeče Internet Explorer byla zkoumána v další otázce, kde 40,68 % významu hlášce rozumí, avšak 36,48 % neví, co zpráva znamená. Následující otázka byla zaměřena na schopnost obejít tuto hlášku, kde 41,21 % odpovídajících ví, jakým způsobem hlášku obejít, a naopak to neví 45,41 % respondentů. Podstatnou otázkou bylo, zda vůbec respondenti vědí, co je to samotný digitální certifikát, kde 44,62 % odpovídajích uvedlo, že vědí, avšak 37,01 % respondentů nezná jeho význam. Dotazník také zjistil, že 69,03 % respondentů neví, jakým způsobem spravovat uložené certifikáty, pouze 21 % odpovídajích zná tento postup. Tento fakt lze hodnotit negativně, jelikož by každý uživatel měl vědět, jakým certifikátům autorit vyjadřuje důvěru a nenechat toto posouzení pouze na operačním systému, který již obsahuje předdefinované důvěryhodné certifikáty.

V dalším úseku praktické části proběhlo analyzování dílčích cílu pomocí testování stanovených hypotéz, kdy dílčím cílem č. 1 bylo zjistění míry informovanosti uživatelů o bezpečném připojení. Hypotézy byly stanoveny pouze u některých vztahů, jelikož se nelze zabývat veškerými možnostmi.

Hypotéza	H_0: Neexistuje statisticky významný vztah mezi		Vyhodnocení
$1H_0$	Používaným prohlížečem	Povšimnutím si zbarvení řádky	**Zamítá se**
$2H_0$	Povšimnutím si zbarvení řádky	Zájmem o bezpečnost dat	**Zamítá se**
$3H_0$	Zabezpečeně připojeným uživatelem	Jím ověřeným digitálním certifikátem	**Zamítá se**
$4H_0$	Věkem uživatele	Zájmem o bezpečnost dat	**Přijímá se**

Tabulka 50: Vyhodnocení hypotéz pro první dílčí cíl

Zdroj: Vlastní zpracování

Každý prohlížeč zobrazuje zbarvení HTTPS či celé řádky odlišně. V první hypotéze bylo zjištěno, že závisí tedy na způsobu grafického zobrazení zabezpečeného připojení prohlížečem. Dle výsledku pozorování je Google Chrome v tomto ohledu nejnázornějším.

Bylo očekáváno, že pokud se uživatel zajímá o bezpečnost svých dat, pak si také všímá zbarvení řádky s webovou adresou. Výsledek druhé hypotézy potvrzuje zmíněnou domněnku o charakteru reakce uživatele.

Výsledným zjištěním třetí hypotézy je potvrzeno, že pokud uživatel již někdy ověřoval či zkoumal digitální certifikát, pak byl i zabezpečeně připojený. Z výsledků lze také uvést, že většina uživatelů nemá povědomí o souvislosti mezi zabezpečeným připojením a podstatou digitálního certifikátu.

Čtvrtá hypotéza zjistila, že neexistuje závislost mezi věkem uživatele a jeho zájmem o bezpečnost svých dat. Je tedy patrné, že v rámci zvolených věkových kategorií existují rozdílné stupně znalosti problematiky – nelze tedy určit kategorii, která by na bezpečnost dat dbala nejvíc.

Druhým stanoveným dílčím cílem pro následujících 6 hypotéz bylo zjištění míry informovanosti uživatelů o digitálních certifikátech.

Hypotéza	H_0: Neexistuje statisticky významný vztah mezi		Vyhodnocení
$5H_0$	Zájmem o bezpečnost dat	Jím ověřeným digitálním certifikátem	**Zamítá se**
$6H_0$	Bezproblémovým zobrazením webové stránky	Překonáním varovné zprávy	**Přijímá se**
$7H_0$	Používaným prohlížečem	Překonáním varovné zprávy	**Zamítá se**
$8H_0$	Zájmem o bezpečnost dat	Spravováním certifikátů	**Zamítá se**
$9H_0$	Bezproblémovým zobrazením webové stránky	Znalostmi informačních technologií	**Přijímá se**
$10H_0$	Bezproblémovým zobrazením webové stránky	Pochopením významu varovné zprávy	**Přijímá se**

Tabulka 51: Vyhodnocení hypotéz pro druhý dílčí cíl

Zdroj: Vlastní zpracování

Příkladem vyhodnocení páté hypotézy, tedy závislosti těchto otázek, může být internetové bankovnictví – pro uživatele je bezpečnost zadávaných informací prioritou, z toho důvodu jsou také nuceni se obeznámit s problematikou digitálního certifikátu.

Pokud uživatel zvolil bezproblémové zobrazení webové stránky, pak musel obejít varovnou zprávu. Avšak z výsledku šesté hypotézy nebyla mezi otázkami nalezena žádná zásadní souvislost. Schopnost obejít varovnou zprávu tedy nezávisí na tom, zda ji uživatel při zobrazení webové stránky vnímal jako problém či nikoliv.

Každý prohlížeč vyžaduje jiný stupeň náročnosti na obejití zprávy. Ze sedmé hypotézy vyplynulo, že schopnost obejít varovnou hlášku je závislá na stupni náročnosti poskytované prohlížečem.

Osmá hypotéza určila, že pokud se uživatel aktivně zajímá o bezpečnost svých dat, pak je seznámen i se správou uložených digitálních certifikátů.

Devátá hypotéza zjistila, že nezáleží na úrovni znalostí informačních technologií k tomu, aby uživatel identifikoval problém při zobrazení webové prezentace.

Na základě výsledku desáté hypotézy lze usoudit, že nezáleží na pochopení významu varovné zprávu k tomu, aby při zobrazení webové prezentace byla identifikována jako problém.

Z celkového vyhodnocení dotazníkového šetření vyplývá, že uživatelům, nezávisle na věkové kategorii, záleží na bezpečnosti svých poskytnutých dat. Zároveň varovnou zprávu o nedůvěryhodném certifikátu, nezávisle na schopnosti ji obejít, znalostech IT a pochopením jejího významu, vnímají jako problém webové stránky. Na základě výzkumu tedy bylo zjištěno, že je potřeba využívat služeb důvěryhodných certifikačních autorit.

Vhodným řešením pro provozovatele domén, kteří plánují přechod na zabezpečené HTTPS, je využití důvěryhodného certifikátu, tudíž nelze využít kvalifikovanou autoritu eIdentity a vlastní certifikační autoritu. Dále již záleží na dalších požadavcích provozovatele, jako třeba na velikosti webového projektu či na stupni ověření.

Pro běžné webové stránky, operující pouze se základními informacemi o uživatelích, dostačuje bezplatné řešení. S ohledem na vyšší bezpečnost, bezpečné krátké platnosti certifikátu a nepotřeby přenášet registraci domény pod jinou společnost, je vhodným řešením certifikační autorita Let's encrypt, jejíž činnost byla vyzkoušena na praktické aplikaci.

Jak také potvrzuje provedený výzkum, zbarvení řádky s adresou webové stránky si všímá většina uživatelů. Proto vystavený digitální certifikát společně se zeleným pruhem označující ověřenou společnost působí na uživatele mnohem důvěryhodněji. Tento druh certifikátu je tedy vhodným řešením pro webové stránky zvažující výšší stupeň ověření, jelikož pracují s podrobnějšími informacemi o uživatelích a využívají například i platební brány.

Řešení vlastní certifikační autority není pro uživatele internetu důvěryhodné a nabízí se tak jako řešení v uzavřených firemních sítích, kde je do jednotlivých počítačových stanic vždy nainstalován kořenový certifikát vytvořené autority.

Dále z dotazníkového šetření lze usoudit, že sice uživatelé identifikují zbarvení řádku pro webovou adresu, které je závislé na grafickém zpracování prohlížeče, avšak jejich povědomost o bezpečnosti klesá v závislosti na hloubce této problematiky. Již méně respondentů ví, z jakého důvodu se řádka zbarvila. Další úbytek uživatelů zaznamenala znalost HTTPS a největší pak znalost SSL/TLS. Znalost o digitálních certifikátech mezi uživateli také není příliš veliká. Všechny tyto prvky spadají pod zabezpečené přípojení, a proto by bylo vhodné tuto problematiku všeobecně rozšířit k mladé generaci, tzn. věnovat se tématu již ve výuce informatiky na základních školách.

6 Závěr

V teoretické první části byl řešen význam pojmu autentizace společně s používanými metodami. Následující kapitola se již věnovala kryptografii, kde byly jednotlivě popsány principy hashovacích funkcí či zneužití replay attacku. Dále byly rozebrány symetrické, asymetrické šifry a zároveň bylo uvedeno využití jejich kombinace. Poslední část se zaměřila na problematiku elektronického podpisu.

Druhá část obsahuje důležité komunikační protokoly, které stanovují pravidla při elektronické komunikaci. Zároveň u HTTPS bylo zjištěno, že oproti loňskému roku proběhlo přes tento zabezpečený protokol o 70 % více žádostí. V rámci SSL/TLS byly popsány jednotlivé vývojové verze a princip fungování TLS. Z dostupných statistik byla prozkoumána využívanost jednotlivých verzí tohoto protokolu a bylo zjištěno, že i přes to, že SSLv2.0 a SSLv3.0 jsou považovány za již zastaralé a nebezpečené, jsou stále podporovány na více než 35 % stránkách z milionu nejlepších webových stránek.

Následující oddíl teorické části byl věnován certifikačním autoritám, kde byly popsány jejich hlavní činnosti, a byl zpracován diagram aktivit procesu vydání certifikátu. Taktéž byly vysvětleny důležité pojmy jako hierariche autorit, jejich důvěryhodnost, důvěryhodný strom či kořenová autorita. Poslední část se zaměřuje na metody vytvoření vlastní certifikační autority s pomocí komerčních řešení či open source softwaru.

Poslední kapitola teoretické části se zabývala samotnými digitálními certifikáty, kdy je popsán účel jejich použití, obsah či jejich možná rozšíření. Dále bylo potřeba specifikovat různé druhy certifikátů dostupných na českém trhu a určit postup pro zjištění kvality certifikátu. Poslední oddíl byl věnován životnímu cyklu certifikátu, který začíná od vytvoření žádosti a končí odvoláním na seznam CRL či vypršením platnosti. Současně s tímto tématem byla popsána možná obnova certifikátu.

V praktické části se první oddíl zaměřoval na analýzu certifikačních autorit. V první subkapitole byly uvedeny tři české akreditované certifikační autority, kde byly shrnuty základní informace dostupné z jejich webových stránek. Popsána tedy byla jejich historie, hierarchie, důvěryhodnost, registrační místa, postup k získání certifikátu a samotný ceník za jejich poskytované základní služby.

Druhá subkapitola byla věnována bezplatným způsobům k získání důvěryhodného certifikátu. Z několika společností byly vybrány – český zástupce od Zoneru, autorita Let's Encrypt založená na zajímavé myšlence a spravovaná komunitou ISRG. Metody získání

byly jednotlivě popsány. U Let's Encrypt byla úspěšně vyzkoušena praktická aplikace na vytvořenou doménu.

Ve třetí subkapitole byl obsah zaměřen na vytvoření certifikační autority a následně i certifikátu. K tomu byl využit sofwarový nástroj X Certificate and key management, který využívá kryptografickou knihovnu OpenSSL. Po úspešném vygenerování privátních klíčů, vytvoření self-signed certifikační autority a vytvoření žádosti o certifikát byl následně podepsán a vystaven samotný certifikát. Pro vytvoření praktického příkladu použitého do dotazníkového šetření bylo zapotřebí domény a webového serveru. U společnosti Wedos proto byla zaregistrována doména a zařízen webový hosting, kam byl certifikát nahrán a byl považován za nedůvěryhodný.

Druhý oddíl praktické části byl věnován dotazníkovému šetření. Nejdříve byly stanoveny cíle a k dílčímu cílům bylo dále určeno deset zajímavých hypotéz.

Dále byla stanovena metodika a organizace průzkumného šetření, v rámci níž byla charakterizována průzkumná metoda, soubor respondentů a pilotní studie, ve které bylo zjištěno několik nedostatků. Po jejich úpravě nastala realizace průzkumného šetření v období od 6. 3. 2016 do 13. 3. 2016, kdy byla získána data od 383 respondentů, ovšem 2 dotazníky musely být vyřazeny z důvodu irelevantních dat. Následně bylo provedeno třídění prvního stupně, kde byly analyzovány a interpretovány získaná data k jednotlivým otázkám. Poté bylo potřeba otestovat a ověřit stanovené hypotézy.

V následující kapitole byly porovnány akreditované certifikační autority a bezplatné metody pro získání důvěryhodných certifikátů. Dále byly shrnuty interpretace z třídění prvního stupně a interpretovány výsledné hypotézy.

V první hypotéze bylo zjištěno, že závisí na způsobu grafického zobrazení informace o zabezpečeném připojení prohlížečem, zároveň bylo posouzeno, že Google Chrome je v tomho ohledu nejnázornějším. Druhá hypotéza potvrdila domněnku, že pokud se uživatel zajímá o bezpečnost svých dat, pak si také všímá zbarvení řádky s webovou adresou. Třetí hypotéza odhalila, že většina uživatelů nemá povědomí o souvislosti mezi zabezpečeným připojením a podstatou digitálního certifikátu. Čtvrtá hypotéza určila, že nelze určit věkové kategorie, které by na bezpečnost dat dbaly nejvíce.

Pátá hypotéza určila, že existuje závislost mezi zájmem uživatele o bezpečnost svých dat a jím ověřeným certifikátem. Šestá hypotéza zjistila, že schopnost obejít varovnou zprávu nezávisí na tom, zda ji uživatel vnímal jako problém. Sedmá hypotéza určila, že

schopnost obejít varovnou zprávu je závislá na stupni náročnosti poskytované prohlížečem. Osmá hypotéza potvrdila, že pokud se uživatel zajímá o bezpečnost svých dat, pak je seznámen i se správou uložených certifikačních autorit. V deváté a desáté hypotéze bylo zjištěno, že nezáleží na úrovni znalostí informačních technologií a na pochopení významu varovné zprávy k identifikování problému při zobrazení webové stránky.

Provedené dotazníkové šetření tedy zjistilo, že uživatelům, nezávisle na věkové kategorii, záleží na bezpečnosti poskytnutých dat. Zároveň respondenti varovnou zprávu o nedůvěryhodném certifikátu, nezávisle na znalostech IT a pochopení jejího významu, vnímají jako problém webové stránky. Jako řešení bylo doporučeno využití důvěryhodné certifikační autority s ohledem na používání webové stránky a požadovaný stupeň ověření.

Dále výzkumem bylo ověřeno, že mezi uživateli existuje určitá znalost o zabezpečeném připojení, ta ovšem klesá v závislosti na hloubce této problematiky. Většinou tedy nerozumějí významu SSL/TLS či digitálnímu certifikátu a jeho možnostem. Bylo by proto vhodné problematiku zabezpečeného připojení okrajově zapojit do výuky informatiky již na základních školách, kdy se mladá generace začíná již volně pohybovat po internetu a poskytovat své osobní údaje.

Neustále roste počet útoků na osobní údaje, které je potřeba si chránit. Bezpečnostní standardy se neustále vyvíjejí. V nedávně době byla ještě podporována komunikace v rámci protokolu SSLv2.0 či certifikáty podepsané hashovacím algoritmem SHA-1. Avšak stačí nalezení jedné zásadní chyby a je nutností přejít na vyšší, a zatím bezpečnější, verze, tak jako je tomu i v těchto případech. Je tedy otázkou času, než bude prolomena hashovací funkce SHA-2 a bude ji muset zastoupit připravená SHA-3 či bude prolomen algoritmus pro asymetrické šifrování RSA a bude muset být nahrazen algoritmem EC.

7 Seznam použitých zdrojů

1. **Dostálek, Libor, Vohnoutová, Marta a Knotek, Miroslav.** *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2. aktualiz. vyd. Brno : Computer Press, 2009. ISBN 978-80-251-2619-6.

2. **Kunder, Maurice de.** The size of the World Wide Web (The Internet). *WorldWideWebSize.com.* [Online] [Citace: 17. 03 2016.] http://www.worldwidewebsize.com/.

3. **Shah, Neil.** MWC 2014: Internet of Things (IoT) Finally Becomes Internet of Everything (IoE). *Cisco Communities.* [Online] Cisco, 10. 03 2014. [Citace: 17. 03 2016.] https://communities.cisco.com/community/solutions/sp/mobility/blog/2014/03/10/mwc-2014-internet-of-things-iot-finally-becomes-internet-of-everything-ioe.

4. **Kurose, James F. a Ross, Keith W.** *Počítačové sítě.* 1. vyd. Brno : Computer Press, 2014. ISBN 978-80-251-3825-0.

5. **Gašparík, Petr.** Vícefaktorová autentizace v praxi. *SecurityWorld.* 2014, 4.

6. **Churý, Lukáš.** MD5 prolomena. *Programujte.com.* [Online] 25. 03 2006. [Citace: 05. 03 2016.] http://programujte.com/clanek/2006032501-md5-prolomena/.

7. **Ministerstvo vnitra ČR.** Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu. *Ministerstvo vnitra České republiky.* [Online] 23. 06 2009. [Citace: 17. 03 2016.] http://www.mvcr.cz/ministerstvo-vnitra-ceske-republiky.aspx.

8. **Cloutier, Jody.** Windows Enforcement of Authenticode Code Signing and Timestamping. *Resources and Tools for IT Professionals | TechNet.* [Online] Microsoft, 11. 02 2016. [Citace: 05. 03 2016.] http://social.technet.microsoft.com/wiki/contents/articles/32288.windows-enforcement-of-authenticode-code-signing-and-timestamping.aspx.

9. **NIST Tech Beat.** NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition. *National Institute of Standards and Technology.* [Online] 02. 10 2012. [Citace: 17. 03 2016.] http://www.nist.gov/itl/csd/sha-100212.cfm.

10. **Vlastimil Klima, Dr.** Soutěž NIST SHA-3 a Blue Midnight Wish. *Personal page: Vlastimil Klima, Dr.* [Online] 17. 07 2015. [Citace: 17. 03 2016.] http://cryptography.hyperlink.cz/BMW/BMW_CZ.html.

11. **NIST Tech Beat.** NIST Releases SHA-3 Cryptographic Hash Standard. *National Institute of Standards and Technology.* [Online] 05. 08 2015. [Citace: 5. 03 2016.] http://www.nist.gov/itl/csd/201508_sha3.cfm.

12. **Stallings, William.** *Cryptography and network security: principles and practice.* . Boston : Pearson, 2014. ISBN 0133354695.

13. **ROUNTREE, Derrick.** *Security for Microsoft Windows system administrators introduction to key information security concepts.* Burlington, MA : Syngress, 2011. ISBN 9781597495950.

14. **Krčmář, Petr.** Jen správně nasazené HTTPS je bezpečné. [Online] OpenSource řešení v sítích, 12. 11 2015. [Citace: 17. 03 2016.] https://www.youtube.com/watch?v=F3B5ajvODGM&index=3&list=PLJnyglSWBN5-9ahHY7yI1x-OUEj7hi1b8.

15. **Ankit, Jain.** Types of Cryptosystem. *Cryptography - The Science of Secrecy.* [Online] 01. 09 2014. [Citace: 17. 03 2016.] http://www.ankitjain.info/articles/Cryptography_ankit4.htm.

16. **Microsoft Edge Team.** HTTP Strict Transport Security comes to Internet Explorer 11 on Windows 8.1 and Windows 7. *Windows Blog.* [Online] Microsoft , 9. 6 2015. [Citace: 17. 03 2016.] https://blogs.windows.com/msedgedev/2015/06/09/http-strict-transport-security-comes-to-internet-explorer-11-on-windows-8-1-and-windows-7/.

17. **Evans, C., a další.** Public Key Pinning Extension for HTTP. *IETF Tools.* [Online] Internet Engineering Task Force, 4 2015. [Citace: 17. 03 2016.] https://tools.ietf.org/html/rfc7469. ISSN: 2070-1721.

18. **Brewster, Kahle.** HTTP Archive - Interesting Stats. *HTTP Archive.* [Online] 01. 03 2016. [Citace: 17. 03 2016.] http://httparchive.org/interesting.php.

19. **Courtot, Philippe.** Survey of the SSL Implementation of the Most Popular Web Sites. *Trustworthy Internet Movement.* [Online] 05. 03 2016. [Citace: 17. 03 2016.] https://www.trustworthyinternet.org/ssl-pulse/.

20. **Oppliger, Rolf.** *SSL and TLS: theory and practice.* Boston : Artech House, 2009. ISBN 978-15-969-3447-4.

21. **Peterka, Jiří.** *Báječný svět elektronického podpisu.* Praha : CZ.NIC, 2011. ISBN 978-80-904248-3-8.

22. **První certifikační autorita, a.s.** Komerční serverový certifikát. *První certifikační autorita, a.s.* [Online] 2016. [Citace: 03. 03 2016.] https://www.ica.cz/Ziskat-komercni-serverovy-certifikat.

23. **Entrust.** *Information Security, Digital Security, Data Security - Entrust.* [Online] Entrust, 2016. [Citace: 17. 03 2015.] https://www.entrust.com/ .

24. **Microsoft.** Active Directory Certificate Services. *Windows Server.* [Online] 2015. [Citace: 17. 03 2016.] https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx.

25. **Young, Eric a Hudson, Tim .** *OpenSSL: The Open Source toolkit for SSL/TLS.* [Online] 01. 03 2016. [Citace: 17. 03 2016.] https://www.openssl.org/.

26. **Hohnstädt, Christian.** *XCA - X Certificate and key management.* [Online] 01. 08 2015. [Citace: 17. 03 2016.] http://xca.sourceforge.net/.

27. **Peterka, RNDr. Jiří.** Uznávaný, nebo jen zaručený elektronický podpis? *Computerworld.* 2012, 03.

28. **Mgr. TOMÁŠ LECHNER, Ph.D.** Různé druhy certifikátů a jejich použití. *Národní pojištění.* 2014, 6.

29. **Zechmeister, Jindřich.** Tři úrovně ověření SSL certifikátů - jakou vybrat? *Magazín o bezpečnosti.* [Online] ZONER software, a.s., 2015. [Citace: 17. 03 2016.] http://www.blog.sslmarket.cz/ssl/tri-urovne-overeni-ssl-certifikatu-dv-ov-ev-jakou-vybrat/.

30. **Česká pošta, s.p.** Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p. PostSignum QCA. *Certifikační autorita PostSignum.* [Online] 10. 01 2014. [Citace: 17. 03 2016.] http://www.postsignum.cz/files/politiky/CPS_QCA_v3-0.pdf.

31. **DigiCert.** Enable OCSP Stapling on Your Server. *SSL Certificate Authority.* [Online] 2015. [Citace: 17. 03 2016.] https://www.digicert.com/enabling-ocsp-stapling.htm.

32. **Česká pošta, s.p.** *Certifikační autorita PostSignum.* [Online] Česká pošta, s.p., 2016. [Citace: 17. 03 2016.] http://www.postsignum.cz/.

33. **eIdentity a.s.** *APCS eIdentity a.s.* [Online] eIdentity a.s., 2016. [Citace: 17. 03 2016.] http://www.eidentity.cz/app.

34. **ZONER software, a.s.** *SSLmarket - Nejširší nabídka důvěryhodných SSL certifikátů.* [Online] 2016. [Citace: 09. 03 2016.] https://www.sslmarket.cz/.

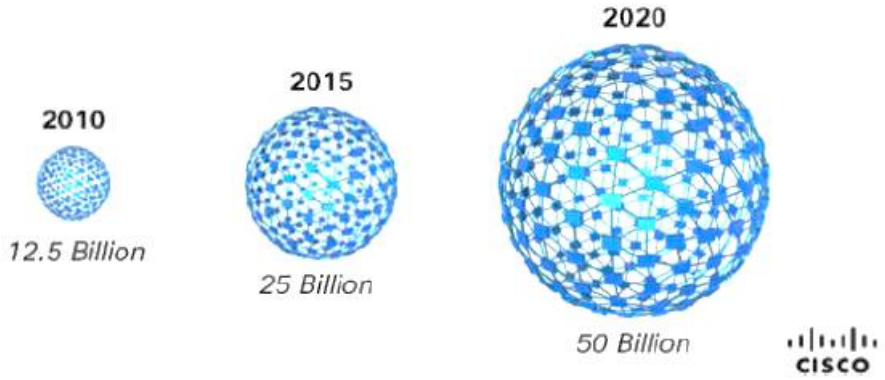
35. **Internet Security Research Group.** *Let's Encrypt - Free SSL/TLS Certificates.* [Online] 09. 03 2016. [Citace: 22. 03 2016.] https://letsencrypt.org/.

36. **Hendl, Jan.** *Přehled statistických metod: analýza a metaanalýza dat. 4., rozš. vyd.* Praha : Portál, 2012. ISBN 978-80-262-0200-4.

37. **Odbor statistiky obyvatelstva.** Úroveň vzdělání obyvatelstva podle výsledků sčítání lidu. [Online] 23. 12 2014. [Citace: 18. 03 2016.] https://www.czso.cz/documents/10180/20536250/17023214.pdf/7545a15a-8565-458b-b4e3-e8bf43255b12?version=1.1.

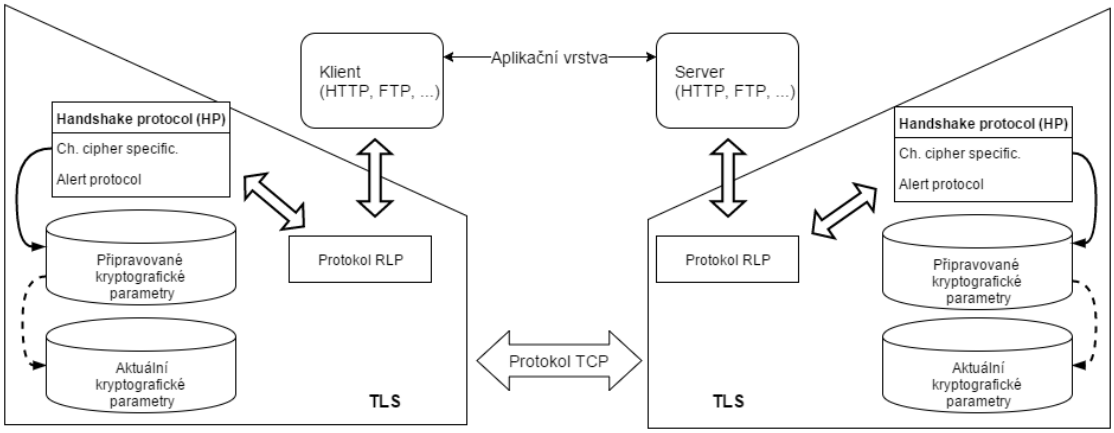
8 Přílohy

Příloha A: Počet zařízení připojených k internetu



Zdroj: (3)

Příloha B: Používané protokoly v TLS



Zdroj: Vlastní zpracování dle (1 str. 384)

Příloha C: Podrobný princip spojení TLS

Navázání spojení probíhá postupně dle následujících kroků. Nejdříve se klient musí spojit s protokolem TCP a ihned pomocí protokolu HP začít dialog, jehož cílem je vytvoření TLS relace, musí tedy: (1 stránky 383–401)

- se dohodnout na použitých šifrovacích algoritmech. Klientova úloha je nabízet sady algoritmů, ze kterých si server zvolí.
- následně si vymění náhodná čísla mezi klientem a serverem.

- klient a server si navzájem vymění certifikáty a šifrovací informace, které slouží ke vzájemné autentizaci. Autentizace není povinná, ovšem je doporučovaná alespoň autentizace serveru.
- poté proběhne výměna kryptografických parametrů z důvodu vygenerování předběžného sdíleného tajemství (premaster secret), které slouží k vytvoření hlavního sdíleného tajemství (master secret). Z hlavního tajemství si oba účastnici zjistí obsah kryptografického materiálu, jehož pomocí je zajištěno šifrování vzájemné komunikace.
- klient a server musí ověřit, zda protější strana vytvořila stejné hlavní sdílené tajemství a nejedná se tedy o podvržený protějšek.
- poskytnout šifrovací materiály protokolu RLP, mezi které patří symetrické kryptografické klíče a sdílené tajemství, pomocí něhož je vypočítán kryptografický kontrolní součet.

Základ vztahu důvěry relace mezi serverem a klientem je hlavní sdílené tajemství. V případě obnovení relace je proces jednodušší, jelikož se již předpokládá znalost hlavního tajemství mezi stranami a není proto potřeba strany autentizovat a vyměňovat si kryptografické podklady. Proto si klient se serverem pouze vymění nová náhodná čísla a ještě s pomocí hlavního tajemství si obě strany vygenerují nové šifrovací materiály. (1 stránky 383–401)

Zřízení nové relace probíhá pomocí důležitého Handshake protokolu, kdy se spojené strany domlouvají na použitém kryptografickém algoritmu a klíči. Komunikace začíná ve chvíli, kdy klient odešle zprávu serveru `ClientHello`, která obsahuje nevyplněné identifikační číslo relace, nabídku podporovaných kryptografických algoritmů a náhodná čísla důležitá pro výpočet sdíleného tajemství. (1 stránky 383–401)

Server následně odpovídá klientovi zprávou `ServerHello` obsahující přidělené identifikační číslo relace, vybraný kryptografický algoritmus, který bude použit, a náhodná čísla. V případě, že se server chce autentizovat, přiloží ještě další zprávu `Certificate` obsahující jeho certifikát. Pokud vyžaduje server i autentizaci klienta, předá mu ve zprávě `CerttificateRequest` seznam jedinečných jmen, který obsahuje pro server důvěryhodných seznam certifikačních autorit. Komunikaci server uzavírá prázdnou zprávou `ServerHelloDone` signalizující, že nyní je očekávaná reakce klienta. (1 stránky 383–401)

Pokud to server nevyžaduje, klient může libovolně prokázat svou identitu zasláním zprávy `Certificate` obsahující jeho certifikát. Klíčovou zprávou, která musí být odeslána vždy, je `ClientKeyExchange`. Obsahem této zprávy je předběžné tajemství šifrované za pomoci veřejného klíče z certifikátu serveru, což je také důležitou součástí pro výpočet hlavního tajemství, tím se provede i samotná autentizace serveru. V situaci, kdy by se na druhé straně ocitl podvržený server, nevlastnil by správný soukromý klíč k danému veřejnému klíči a nedokázal by tak dešifrovat poskytnuté předběžné tajemství. (1 stránky 383–401)

Po splnění uvedených kroků již obě strany sdílí hlavní tajemství a klient pomocí protokolu Change Cipher Specification signalizuje, že byly přenastaveny šifrovací klíče. Následně odesílá serveru již zašifrovanou zprávu `Finished` obsahující důkaz, že klient má správně vypočteno společné hlavní tajemství. (1 stránky 383–401)

I server pomocí protokolu Change Cipher Specification signalizuje, že přešel na nové šifrovací klíče a odesílá klientovi zašifrovanou zprávu `Finished` s důkazem o správném vytvoření hlavního sdíleného tajemství. Tím navazování komunikace končí a začíná samotný přenos šifrovaných aplikačních dat. Integrita přenášených dat je zabezpečena tím způsobem, že do každého RLP fragmentu je vložen kryptografický kontrolní součet (MAC). (1 stránky 383–401)

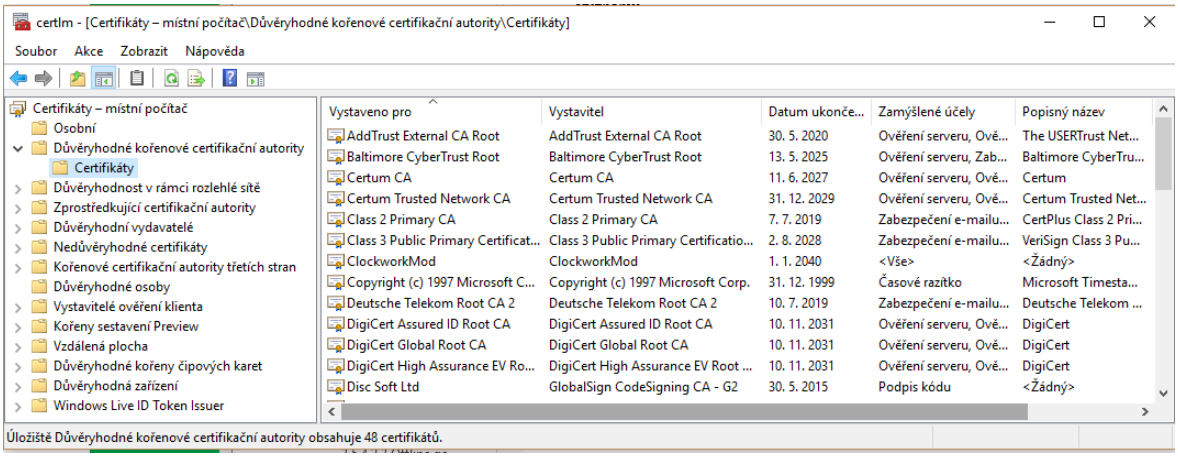
V případě obnovení již dříve existující relace je proces mnohem jednodušší. Dialog klienta se serverem začíná stejnou zprávou `ClientHello` a `ServerHello`, ovšem nyní s jinými náhodnými čísly ale s předchozím identifikačním číslem relace. Obě strany již znají hlavní sdílené tajemství a mají k dispozici nová náhodná čísla, pomocí nichž si vygenerují nové bloky klíčů. Poté již pomocí protokolu Change Cipher Specification signalizují přechod na šifrovanou komunikaci, kde si vzájemně odešlou zprávu `Finished` potvrzující použití správného hlavního sdíleného tajemství. Po úspěšném provedení započíná přenos šifrovaných dat. (1 stránky 383–401)

Uživatel o těchto krocích protokolu nemá ani tušení, jelikož všechny probíhají na pozadí. Jediný jeho zásah nastává v situaci, kdy server žádá ověření klienta a je tedy nutné předložit jeho platný certifikát. (1 stránky 383–401)

Samotný uživatel se může setkat s ještě jedním požadavkem na jeho zásah, který nastává v případě, kdy je potřeba posoudit důvěryhodnost serveru, respektive jeho certifikátu. Zde v některých situacích dochází k problému, kdy kořenový certifikát autority,

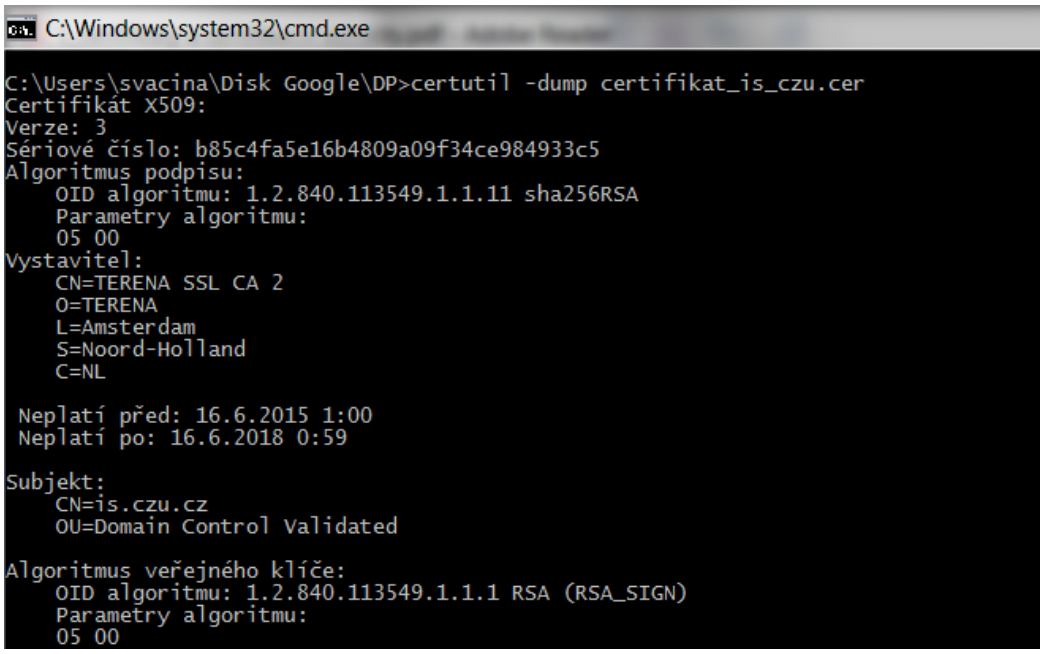
která měla na starosti vydání certifikátu, není uložen v úložišti webového prohlížeče. V takovém případě webový přohlížeč prohlásí danou certifikační autoritu za nedůvěryhodnou a zobrazí varování. Rozhodnutí, zda označit vydávající certifikační autoritu jako důvěryhodnou, je ponecháno na samotném uživateli. (1 stránky 383–401)

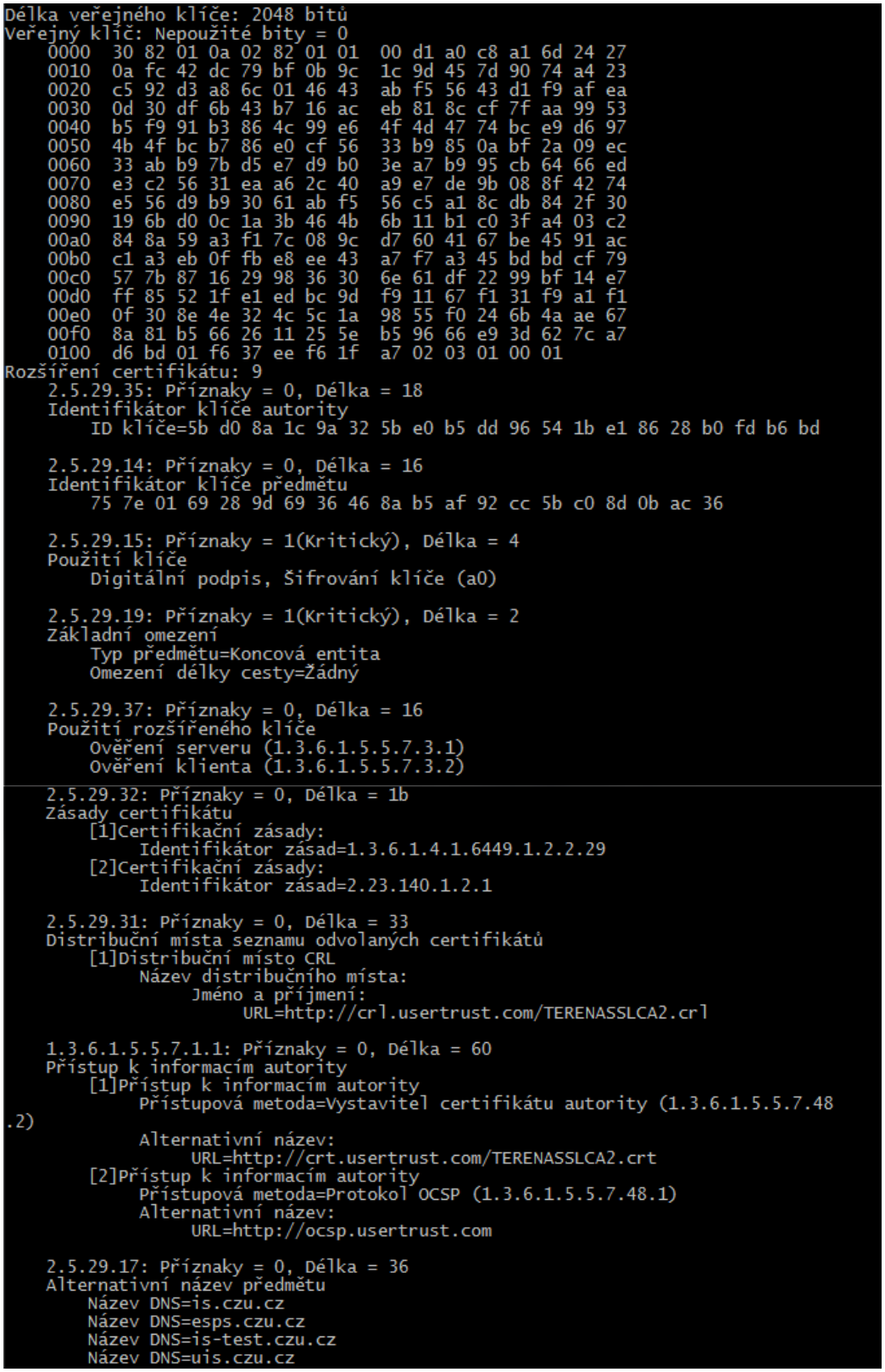
Příloha D: Úložiště kořenových certifikačních autorit v MS Windows



Zdroj: Vlastní zpracování

Příloha E: Zobrazený certifikát is.czu.cz




Délka veřejného klíče: 2048 bitů
Veřejný klíč: Nepoužité bity = 0
0000 30 82 01 0a 02 82 01 01 00 d1 a0 c8 a1 6d 24 27
0010 0a fc 42 dc 79 bf 0b 9c 1c 9d 45 7d 90 74 a4 23
0020 c5 92 d3 a8 6c 01 46 43 ab f5 56 43 d1 f9 af ea
0030 0d 30 df 6b 43 b7 16 ac eb 81 8c cf 7f aa 99 53
0040 b5 f9 91 b3 86 4c 99 e6 4f 4d 47 74 bc e9 d6 97
0050 4b 4f bc b7 86 e0 cf 56 33 b9 85 0a bf 2a 09 ec
0060 33 ab b9 7b d5 e7 d9 b0 3e a7 b9 95 cb 64 66 ed
0070 e3 c2 56 31 ea a6 2c 40 a9 e7 de 9b 08 8f 42 74
0080 e5 56 d9 b9 30 61 ab f5 56 c5 a1 8c db 84 2f 30
0090 19 6b d0 0c 1a 3b 46 4b 6b 11 b1 c0 3f a4 03 c2
00a0 84 8a 59 a3 f1 7c 08 9c d7 60 41 67 be 45 91 ac
00b0 c1 a3 eb 0f fb e8 ee 43 a7 f7 a3 45 bd bd cf 79
00c0 57 7b 87 16 29 98 36 30 6e 61 df 22 99 bf 14 e7
00d0 ff 85 52 1f e1 ed bc 9d f9 11 67 f1 31 f9 a1 f1
00e0 0f 30 8e 4e 32 4c 5c 1a 98 55 f0 24 6b 4a ae 67
00f0 8a 81 b5 66 26 11 25 5e b5 96 66 e9 3d 62 7c a7
0100 d6 bd 01 f6 37 ee f6 1f a7 02 03 01 00 01
Rozšíření certifikátu: 9
2.5.29.35: Příznaky = 0, Délka = 18
Identifikátor klíče autority
ID klíče=5b d0 8a 1c 9a 32 5b e0 b5 dd 96 54 1b e1 86 28 b0 fd b6 bd
2.5.29.14: Příznaky = 0, Délka = 16
Identifikátor klíče předmětu
75 7e 01 69 28 9d 69 36 46 8a b5 af 92 cc 5b c0 8d 0b ac 36
2.5.29.15: Příznaky = 1(Kritický), Délka = 4
Použití klíče
Digitální podpis, Šifrování klíče (a0)
2.5.29.19: Příznaky = 1(Kritický), Délka = 2
Základní omezení
Typ předmětu=Koncová entita
Omezení délky cesty=Žádný
2.5.29.37: Příznaky = 0, Délka = 16
Použití rozšířeného klíče
Ověření serveru (1.3.6.1.5.5.7.3.1)
Ověření klienta (1.3.6.1.5.5.7.3.2)
2.5.29.32: Příznaky = 0, Délka = 1b
Zásady certifikátu
[1]Certifikační zásady:
Identifikátor zásad=1.3.6.1.4.1.6449.1.2.2.29
[2]Certifikační zásady:
Identifikátor zásad=2.23.140.1.2.1
2.5.29.31: Příznaky = 0, Délka = 33
Distribuční místa seznamu odvolaných certifikátů
[1]Distribuční místo CRL
Název distribučního místa:
Jméno a příjmení:
URL=http://crl.usertrust.com/TERENASSLCA2.crl
1.3.6.1.5.5.7.1.1: Příznaky = 0, Délka = 60
Přístup k informacím autority
[1]Přístup k informacím autority
Přístupová metoda=Vystavitel certifikátu autority (1.3.6.1.5.5.7.48
.2)
Alternativní název:
URL=http://crt.usertrust.com/TERENASSLCA2.crt
[2]Přístup k informacím autority
Přístupová metoda=Protokol OCSP (1.3.6.1.5.5.7.48.1)
Alternativní název:
URL=http://ocsp.usertrust.com
2.5.29.17: Příznaky = 0, Délka = 36
Alternativní název předmětu
Název DNS=is.czu.cz
Název DNS=esps.czu.cz
Název DNS=is-test.czu.cz
Název DNS=uis.czu.cz

```
Algoritmus podpisu:
    OID algoritmu: 1.2.840.113549.1.1.11 sha256RSA
    Parametry algoritmu:
    05 00
Podpis: UnusedBits=0
    0000  d6 61 d5 a6 41 80 f2 8d  92 f8 70 9b d5 f2 01 4d
    0010  cb 98 65 32 6b cc bc 5c  45 ab 9e 68 cf c9 96 d6
    0020  1a 26 f5 70 d8 bd 3d d1  8a a1 48 4e b8 fe 37 40
    0030  bd 07 26 8c 15 6b 0b f2  a6 41 ea 39 e5 69 ed 3b
    0040  ff cc 5e 8a a8 ff 8d a9  dd b2 39 19 1b fa 47 2f
    0050  cb c0 4e 85 24 8e 63 0a  32 ea 8c 4b a4 36 24 02
    0060  e1 e8 79 69 36 02 be fb  16 10 49 04 16 fe c9 9f
    0070  6a 56 ca f0 7f 55 c2 6d  6b 60 31 2a f8 6d 30 32
    0080  df d1 03 fb 59 8a 53 5c  e8 ed 20 e0 00 a3 19 08
    0090  b3 53 93 cb c1 0a 94 d5  b9 ce 9a fd 36 9b 2b 11
    00a0  32 3a d3 bc 65 26 4d 32  18 04 cb 80 66 95 b2 16
    00b0  0d b3 a0 a1 bd c3 3f 93  ba dd 95 b7 30 1b 08 a0
    00c0  4e db f0 5d 92 90 66 62  73 8c a9 e4 0a 07 f8 2a
    00d0  d7 7a 6e 9e a0 3c 48 43  bd 76 21 fe c5 83 99 30
    00e0  bf 8c 51 53 3c 21 b6 e9  0a bd 04 e1 91 a5 8a 07
    00f0  b7 20 0a 9f 8e 6a 18 f1  9e 43 0c c7 91 a2 57 2d
Certifikát jiný než kořenový
Algoritmus hash ID klíče (rfc-sha1): 75 7e 01 69 28 9d 69 36 46 8a b5 af 92 cc 5
b c0 8d 0b ac 36
Algoritmus hash ID klíče (sha1): d2 5c 31 4d 3b c8 ef fc 69 9f e0 ce 67 e9 25 f9
 d2 cd c5 a3
Algoritmus hash certifikátu (md5): 82 85 dc 92 f7 a7 08 e1 f0 80 4b f4 b4 b5 33
aa
Algoritmus hash certifikátu (sha1): 81 50 32 be 3e 14 cc 0c 5a 15 80 42 f5 c9 5a
 bf 12 71 05 a1
CertUtil: Příkaz -dump byl úspěšně dokončen.
```

Zdroj: Vlastní zpracování

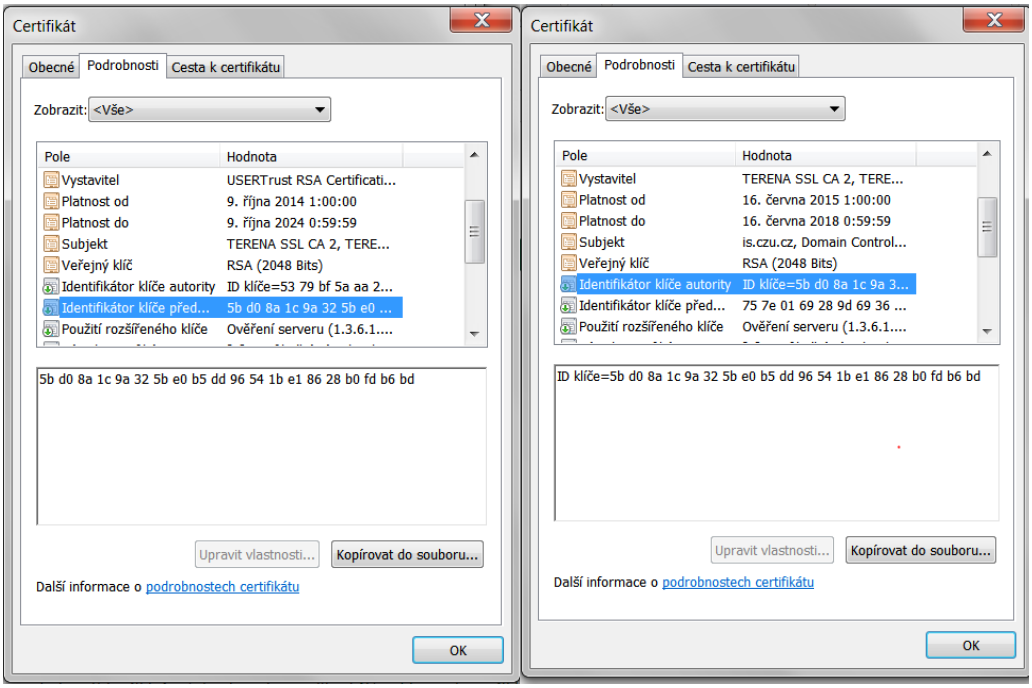
Příloha F: Standardní rozšíření dle RFC-5280

Rozšíření certifikátu	Certifikáty autorit	Koncové certifikáty
Identifikátor klíče autority (Authority Key Identifier)	Položka je povinná pro všechny nekořenové certifikáty a zároveň nesmí mít označení jako závažná.	
Identifikátor klíče předmětu (Subject Key Identifier)	Položka je povinná, nesmí být závažná.	Doporučovaná položka, nesmí být závažná.
Použití klíče (Key Usage)	Povinná informace v certifikátech určených pro verifikaci elektronických podpisů certifikátů a CRL, měla by mít označení závažná.	
Použití rozšířeného klíče (Extended Key Usage)	Povinná položka, pro některé druhy certifikátu (DVCS, TSA, atd.)	
Platnost soukromého klíče (Private Key Usage Period)		
Zásady certifikátu (Certificate Policies)	Volitelné	
Mapování zásad (Policy Mappings)	V případě použití označeno jako závažné.	–
Subject Directory Attributes	V případě použití nesmí být označené jako závažné.	

Rozšíření certifikátu	Certifikáty autorit	Koncové certifikáty
Alternativní název předmětu (Subject Alternative Name)	Certifikát CA nesmí mít položku předmětu prázdnou, rozšíření je proto volitelné a nesmí být označeno jako závažné.	V případě, kdy je předmět prázdný, musí být využito toto rozšíření označené jako závažné.
Alternativní jméno úřadu (Issuer Alternative Name)	Závažnost by neměla být označena, některé aplikace ji nerozeznají.	
Základní omezení (Basic Constraints)	Musí být využito a označeno závažností.	–
Omezení jmen (Name Constraints)	V případě využití označeno jako závažné.	–
Omezení zásad (Policy Constraints)	V případě využití označeno jako závažné.	–
Distribuční místa seznamu CRL (CRL Distribution Points)	Nemělo by být označeno jako závažné	
Omezení Any-Policy (Inhibit Any-Policy)	V případě použití označené jako závažné.	–
Nejnovější seznam CRL (Freshest CRL)	Nesmí být označeno jako závažné.	
Přístup k informacím autority (Authority Information Access)	Nesmí být označeno jako závažné. Určeno pro privání internetová rozšíření	
Přístup k informacím předmětu (Subject Information Access)	Nesmí být označeno jako závažné.	
Biometrické informace (Biometric Information)	Nesmí být označeno jako závažné. Určené pro kvalifikované certifikáty	
Qualified Certificate Statements	Nemusí, ale může být označeno jako závažné. Určené pro kvalifikované certifikáty	
Název šablony certifikátu (Certificate Template Name)	Určené pro Microsoft.	

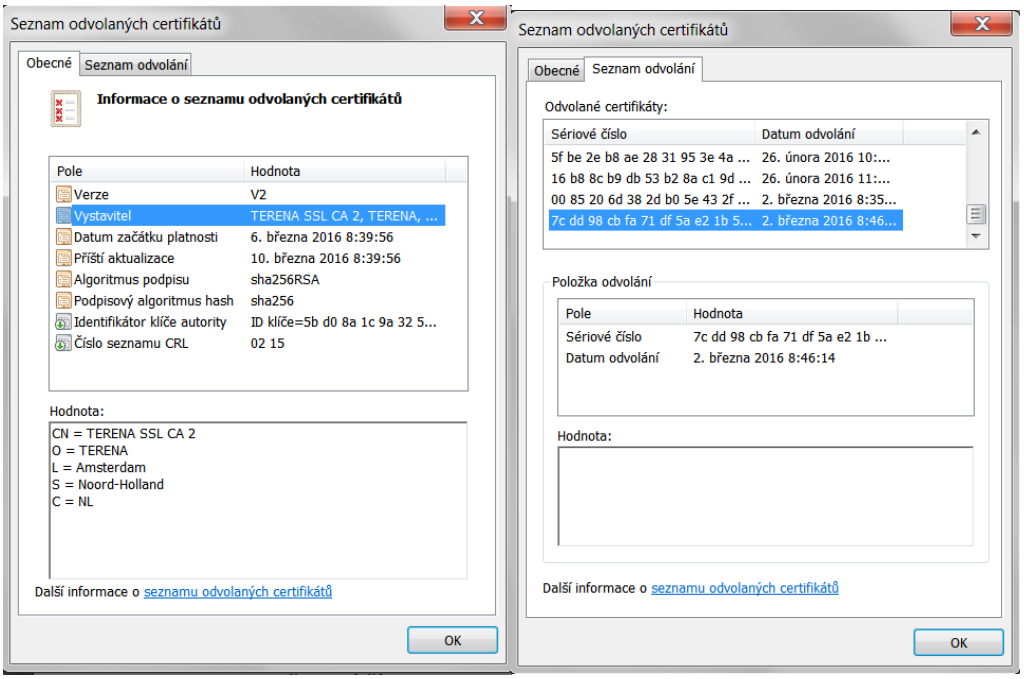
Zdroj: (1 str. 64)

Příloha G: Nadřízený a ověřovaný certifikát is.czu.cz



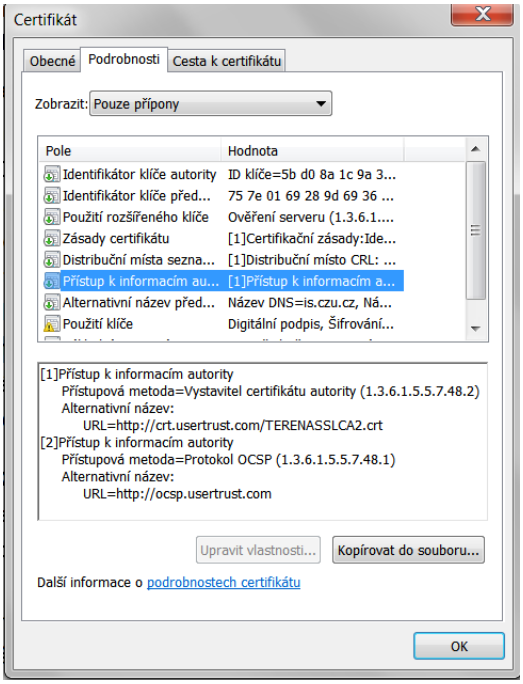
Zdroj: Vlastní zpracování

Příloha H: Seznam CRL v certifikátu is.czu.cz



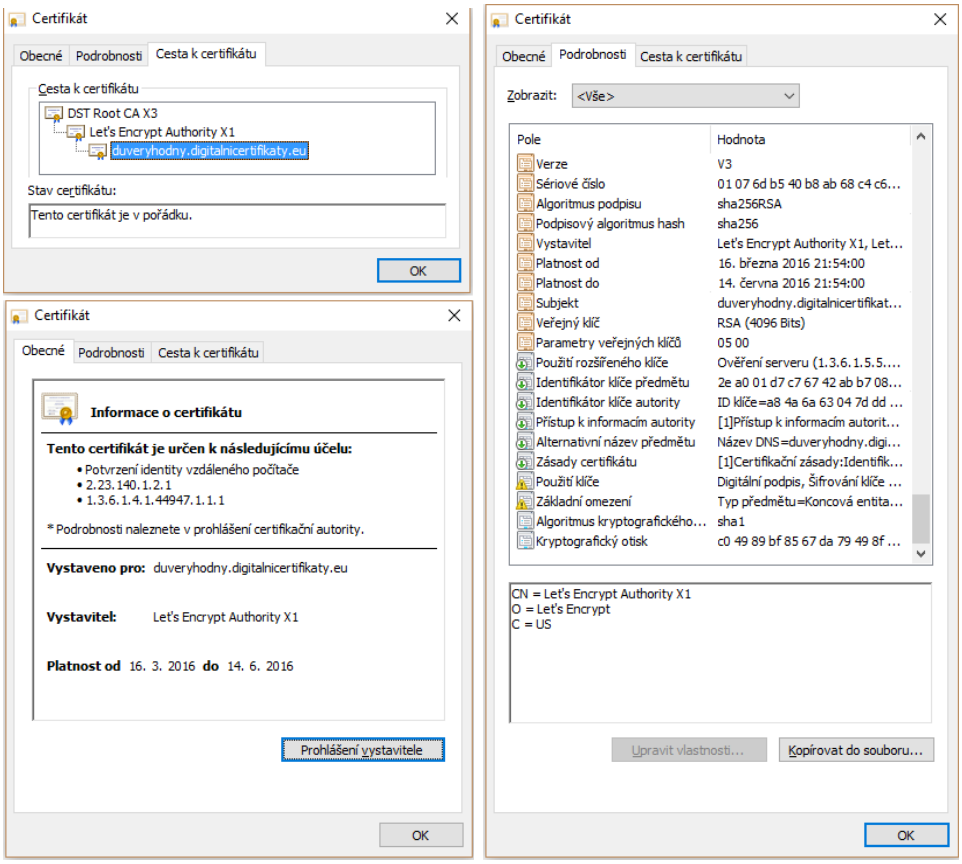
Zdroj: Vlastní zpracování

Příloha I: Protokol OCSP pro certifikát is.czu.cz



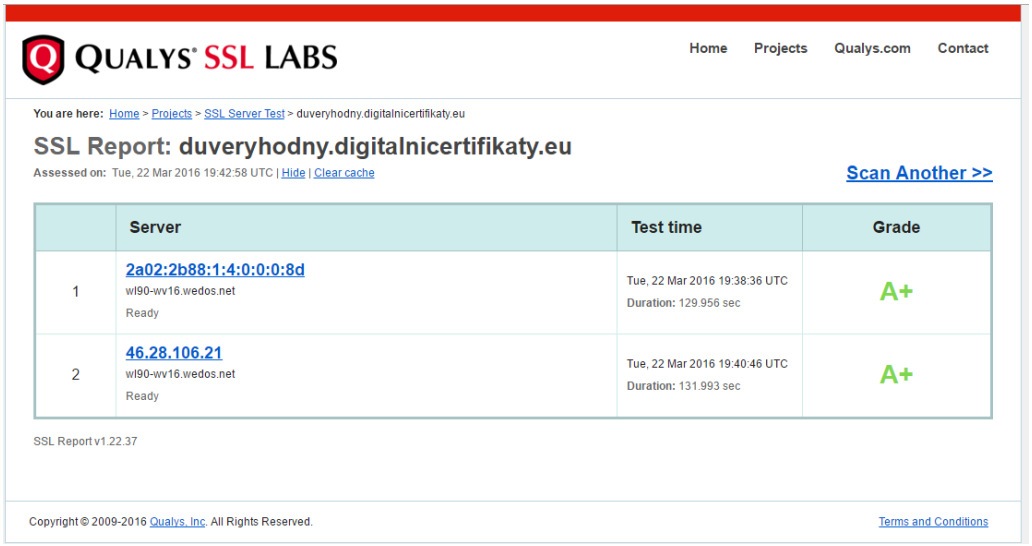
Zdroj: Vlastní zpracování

Příloha J: Důvěryhodný certifikát pomocí Let's Encrypt



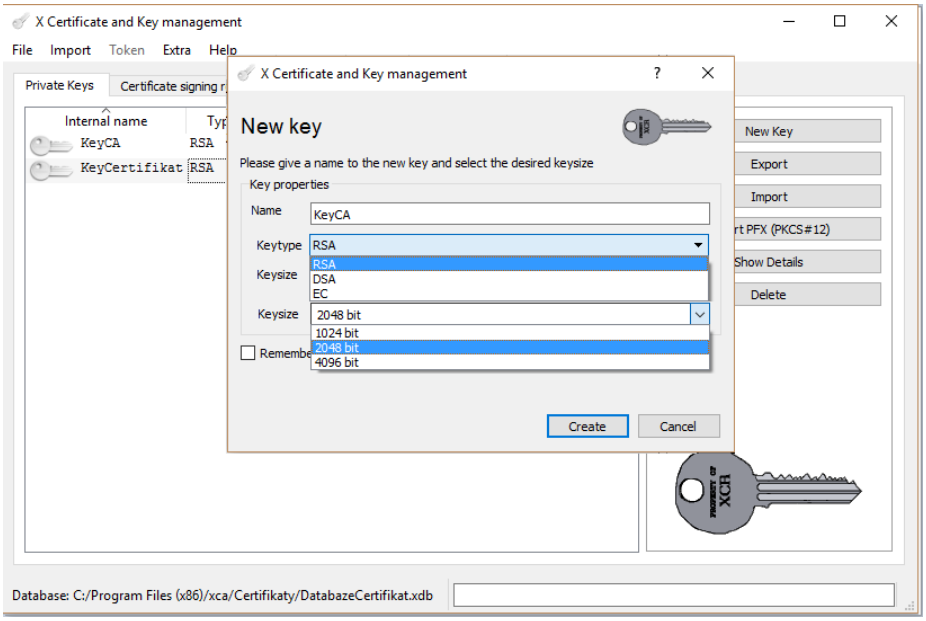
Zdroj: Vlastní zpracování

Příloha K: Hodnocení zabezpečené stránky



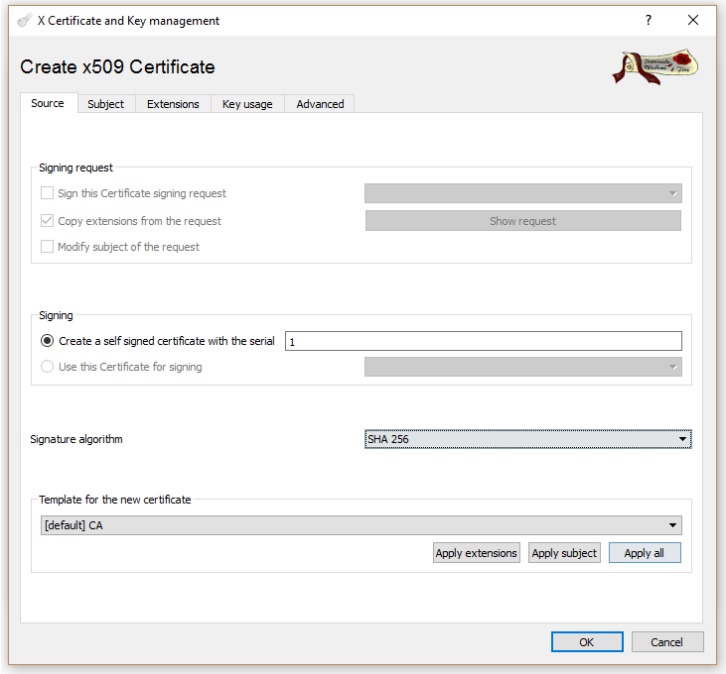
Zdroj: Vlastní zpracování

Příloha L: Vytvoření privátního klíče



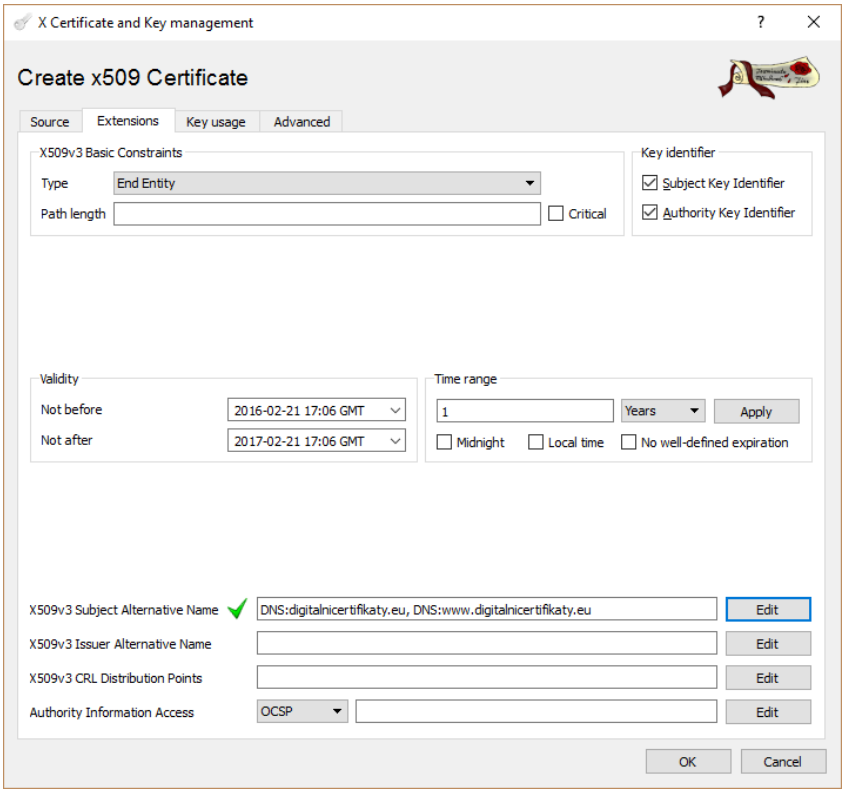
Zdroj: Vlastní zpracování

Příloha M: Vytvoření certifikátu certifikační autority – Source



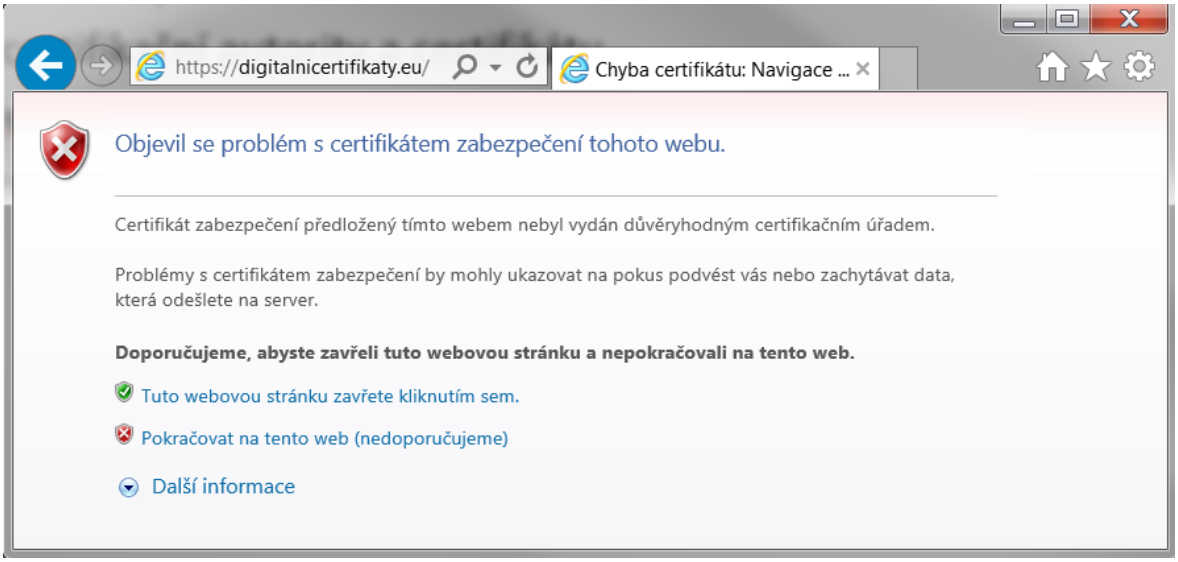
Zdroj: Vlastní zpracování

Příloha N: Schválení žádosti o certifikát - Extensions



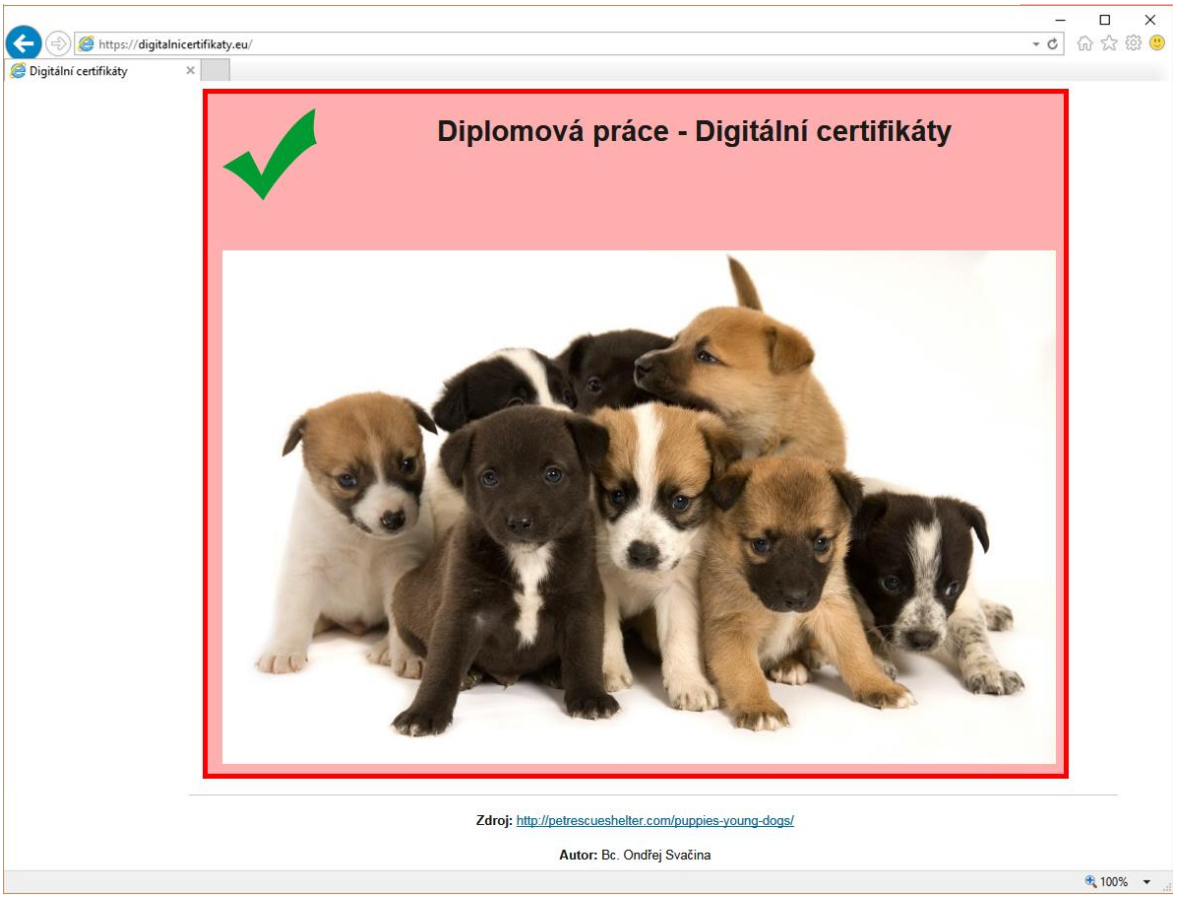
Zdroj: Vlastní zpracování

Příloha O: Prohlášení prohlížeče o nedůvěryhodnosti certifikátu



Zdroj: Vlastní zpracování

Příloha P: Zobrazení webové stránky



Zdroj: Vlastní zpracování

Příloha Q: Dotazník

Digitální certifikáty

Dobrý den,

jmenuji se Ondřej Svačina a jsem studentem 2. ročníku magisterského studia Informatiky na České zemědělské univerzitě v Praze.

Rád bych Vás požádal o vyplnění dotazníku k mé diplomové práci na téma Digitální certifikáty.

Jeho vyplnění Vám zabere jen pár minut.

Děkuji za Váš čas.

*Povinné pole

Otázky I. část

1. **V jakém prohlížeči máte otevřený tento dotazník?** *
   Označte jen jednu elipsu.
   - ◯ Internet Explorer
   - ◯ Chrome
   - ◯ Firefox
   - ◯ Opera
   - ◯ Safari
   - ◯ Jiný

2. **Jaká je Vaše znalost informačních technologií?** *
   Označte jen jednu elipsu.
   - ◯ Základní
   - ◯ Uživatelská
   - ◯ Nadstandardní uživatelská
   - ◯ Odborná

3. **Jak často využíváte internetové připojení?** *
   Označte jen jednu elipsu.
   - ◯ Denně
   - ◯ 2-3x za týden
   - ◯ 1x za týden
   - ◯ Méně než 1x za týden
   - ◯ Vůbec

4. **Zajímáte se o bezpečnost Vašich poskytnutých dat?** *
   Označte jen jednu elipsu.

   - ◯ Ano
   - ◯ Ne

5. **Využíváte některé z těchto služeb?** *
   Zaškrtněte všechny platné možnosti.

   - ☐ Nakupování na e-shopech
   - ☐ Elektronické bankovnictví
   - ☐ Komunikace s úřady (e-governemnt)
   - ☐ Webový email
   - ☐ Žádná z možností

Otázky II. část

6. **Zobrazí se Vám bez problému webová prezentace po kliknutí na: https://goo.gl/TYFtzV ?** *
   Označte jen jednu elipsu.

   - ◯ Ano *Přeskočte na otázku 7.*
   - ◯ Ne *Přeskočte na otázku 8.*

Otázky II.A část

7. **Jaký obsah jste nalezl/a na webové prezentaci?** *
   Označte jen jednu elipsu.

   - ◯ Obrázek koťátek
   - ◯ Obrázek štěňátek
   - ◯ Chybovou hlášku
   - ◯ Obrázek hříbátek
   - ◯ Obrázek telátek

Přeskočte na otázku 9.

Otázky II.B část

8. **Na jaký problém jste narazil/a?** *

   _____

Přeskočte na otázku 9.

Otázky III. část

9. Byl/a jste někdy zabezpečeně připojen/a? *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

10. Všiml/a jste si někdy zbarvení v řádce s adresou webové stránky? *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

Zbarvení v řádce s adresou webové stránky

11. Víte, proč se řádka s webovou adresou zbarvila? *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

12. Při připojení k zabezpečenému webu se webová adresa změní na HTTPS, víte, co to znamená? *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

13. Víte, co znamená spojení SSL/TLS? *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

Otázky IV. část

14. Už jste někdy ověřoval/a | zkoumal/a digitální certifikát? *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

15. **Víte, co znamená varovná hláška "Certifikát zabezpečení předložený tímto webem nebyl vydán důvěryhodným certifikačním úřadem."?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

16. **Víte, jak obejít varovnou zprávu v případě nedůvěryhodného či neplatného certifikátu?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

17. **Víte, co je to digitální certifikát?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

18. **Víte, jak spravovat uložené digitální certifikáty?** *
Označte jen jednu elipsu.

- ◯ Ano
- ◯ Ne
- ◯ Nejsem si jistý/á

Otázky V. část

19. **Jaký je Váš věk?** *

_____

20. **Jaké je Vaše pohlaví?** *
Označte jen jednu elipsu.

- ◯ Muž
- ◯ Žena

21. **Jaké je Vaše nejvyšší dosažené vzdělání?** *
Označte jen jednu elipsu.

- ◯ Základní
- ◯ Středoškolské bez maturity
- ◯ Středoškolské s maturitou
- ◯ Vyšší odborné
- ◯ Vysokoškolské

22. **Jaký je Váš obor vzdělání?** *
Označte jen jednu elipsu.

- ◯ Technický
- ◯ Informatický
- ◯ Humanitní
- ◯ Lékařský
- ◯ Jiný

Děkuji za vyplnění.

Zdroj: Vlastní zpracování