Význam elektronického podpisu

The importance of the electronic signature

Bc. Petr Katovský

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr KATOVSKÝ**
Osobní číslo:	**A09813**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Význam elektronického podpisu**

Zásady pro vypracování:

1. **Práci zpracujte jako výukovou pomůcku do předmětu Kriminalistické technologie a systémy.**
2. **Analyzujte aktuální stav využití elektronického podpisu v ČR a jeho význam.**
3. **Zahrňte úpravu dle české legislativy a její srovnání s legislativou evropskou.**
4. **Vysvětlete technickou stránku elektronického podpisu.**
5. **Popište využití v praxi.**
6. **Zpracujte výklad pojmů.**
7. **Práci doplňte grafickou dokumentací.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DOSTÁLEK, Libor. VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1. vyd. Brno: Computer Press, 2006. 536 s. ISBN: 80-251-0828-7**
2. **BOSÁKOVÁ, Dagmar. KUČEROVÁ, Alena. PECA, Jaroslav. VONDRUŠKA, Pavel. Elektronický podpis – přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů. 2. vyd. Olomouc: ANAG, 2004. 141 s. ISBN 80-7263-125-X**
3. **BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Olomouc: ANAG, 2008. 160 s. ISBN 978-80-7263-465-1**
4. **KATZ, Jonathan. Digital Signatures. 1st ed. London: Springer, 2010. 183 s. ISBN 978-0-387-27711-0**
5. **ŠTĚDROŇ, Bohumír. E-justice. 1. vyd. Praha: Linde, 2008. 272 s. ISBN 978-80-7201-714-0**
6. **LIDINSKÝ, Vít. ŠVARCOVÁ, Ivana. BUDIŠ, Petr. LOEBL, Zbyněk. PROCHÁZKOVÁ, Barbora. eGovernment bezpečně. 1. vyd. Praha: GRADA, 160 s. ISBN 978-80-247-2462-1**

Vedoucí diplomové práce: **Ing. Jiří Pálka**
Ústav elektroniky a měření

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá významem a využitím elektronického podpisu v České republice. Vysvětluje technickou stránku elektronického podpisu, úpravu dle české legislativy a srovnání s legislativou evropskou. Praktická část popisuje získání kvalifikovaného certifikátu, porovnává certifikační autority v České republice a ukazuje využití elektronického podpisu v praxi.

Klíčová slova: elektronický podpis, kryptografie, certifikát, certifikační autorita, zákon o elektronickém podpisu;

ABSTRACT

The diploma work is concerned in electronic signature signification and utilisation in the Czech Republic. It explains the technical circumstances of the electronic signature, adjustment to the Czech legislature and comparing with the European legislature. The operative part describes ways of gaining the competent certificate, compares different certification authorities in the Czech Republic and shows how to put electronic signature into practice.

Keywords: electronic signature, cryptography, certificate, certification authority, the law about digital signature;

Děkuji Ing. Jiřímu Pálkovi a JUDr. Vladislavu Štefkovi za vedení během mé práce.

Děkuji své manželce a dceři za podporu a trpělivost během studia.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Elektronizace zasahuje do všech oblastí našeho života. Věci, užívané v běžném životě, dostávají svoji elektronickou podobu místo papírové. Týká se to i elektronického podpisu, který je možné považovat za rovnocenného vlastnoručnímu podpisu. O elektronickém podpisu se stále mluví, ovšem jen málokdo tomuto tématu podrobněji rozumí.

Právě snaha problematice porozumět a umožnit podrobný pohled do světa elektronického podpisu, kde je možné tuto moderní technologii úspěšně a bez obav využívat, je důvodem vzniku této diplomové práce.

Hlavním cílem je podat ucelenou představu o technologii, využití a právní stránce elektronického podpisu formou výukové pomůcky do předmětu Kriminalistické technologie a systémy, analyzovat aktuální stav využití elektronického podpisu v ČR a porovnat úpravu české legislativy s legislativou evropskou.

Praktická část se zabývá porovnáním certifikačních autorit v České republice, výběrem nejvhodnější autority a následným získáním a využitím elektronického podpisu v praxi.

Očekávaný přínos této práce je z teoretického hlediska předložení komplexní výukové pomůcky do předmětu Kriminalistické technologie a systémy. V praktické části práce je očekáván přínos v podobě podrobného popisu využití elektronického podpisu v praxi.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÝ PODPIS

1.1 Geneze elektronického podpisu

Do poloviny devadesátých let v České republice neexistovala ucelená koncepce státní politiky v oblasti informačních systémů. První zlom nastal 1. listopadu 1996, kdy vznikl Úřad pro státní informační systém. Úřad byl ustanoven zákonem zákona č. 365/2000 Sb. o informačních systémech veřejné správy a převzal kompetence v oblasti budování Státního informačního systému od Ministerstva hospodářství České republiky. [27]

Vznik elektronického podpisu v ČR se spojuje s rokem 1999 a dokumentem nazývaným Státní informační politika - cesta k informační společnosti. Jedná se o první ucelenou koncepci státu v oblasti budování tzv. informační společnosti. V tomto dokumentu bylo mimo jiné konstatováno, že pro rozvoj informační společnosti v České republice chybí legislativní zázemí, které by se zabývalo oblastí elektronického obchodu, elektronického podpisu a používání dokumentů v elektronické podobě. Jedním z prioritních úkolů bylo uzákonit elektronický podpis a dát dokumentům v elektronické podobě stejnou právní váhu jako dokumentům klasickým.

V prosinci 1999, byla přijata směrnice Evropské Unie pro elektronický podpis. [10] Krátce po tomto přijetí došlo ke shodě zástupců Úřadu pro státní informační systém na dalším společném postupu při prosazování přijetí zákona o elektronickém podpisu. Právě z tohoto postupu pak vycházel návrh zákona o elektronickém podpisu, který byl v červenci 2000 pod číslem 227/2000 Sb. přijat Parlamentem České republiky.

1.2 Výklad klíčových pojmů

Pro jednodušší orientaci v klíčových pojmech a rychlého získání přehledu spojených s elektronickým podpisem slouží tato kapitola.

Akreditace

Akreditace ve smyslu zákona o elektronickém podpisu je osvědčení vydávané Ministerstvem vnitra ČR poskytovatelům certifikačních služeb. Je to osvědčení, že poskytovatel certifikačních služeb splňuje podmínky jako akreditovaný poskytovatel certifikačních služeb stanovené zákonem.

Autorizace

Proces, při kterém se ověří, zda je daná identita oprávněna obdržet specifické kategorie informací, které služba nabízí.

Certifikační autorita - CA

Fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako třetí, nezávislý subjekt, který prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu (fyzickou identitu) s jeho dvojicí klíčů (elektronickou identitou) a zároveň garantuje jedinečnost subjektů podle užité identifikace subjektu v rámci vydávaných certifikátů.

Certifikát

Datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje
data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu.

CRL - Certificate revocation list

Seznam zneplatněných certifikátů. Seznam je pravidelně aktualizován a je on-line dostupný. Jsou v něm uvedeny certifikáty, které byly zneplatněny na žádost jejich držitele či jiného subjektu. Žádosti o zneplatnění se podávají např. z důvodu, kdy došlo k prozrazení soukromého klíče.

Časové razítko

Datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Držitel certifikátu

Fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu, které byl certifikát vydán.

Elektronický podpis

Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.

Elektronická značka

Elektronickou značkou jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které splňují následující požadavky:

- jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu;
- byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou;
- jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Nástroj elektronického podpisu

Technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů.

2 KRYPTOGRAFIE

Kryptografie neboli šifrování dat je nauka o transformování dat do podoby, která je čitelná jenom za určitých podmínek. Slovo Kryptografie pochází z řečtiny – kryptós (je skrytý) a gráphein (psát). Ne každá informace je ovšem určená všem. Jinými slovy, přenášená data je potřeba chránit. Zejména hovoříme-li o komunikaci ve sféře státní správy, vojenství, zdravotnictví, financí, obchodu nebo služeb je nutné, aby důvěryhodnost elektronické komunikace byla stejná nebo vyšší jako u klasické komunikace prováděné na základě osobního styku.

Stupeň zabezpečení zprávy je dán zvolenou šifrovací metodou zahrnující typ užitého šifrovacího algoritmu, způsob jeho aplikace a délkou šifrovacího klíče. Obecně rozlišujeme dvě šifrovací metody - symetrickou kryptografii a asymetrickou kryptografii, jejíž součástí je kryptografie s veřejným klíčem.

2.1 Symetrické šifry

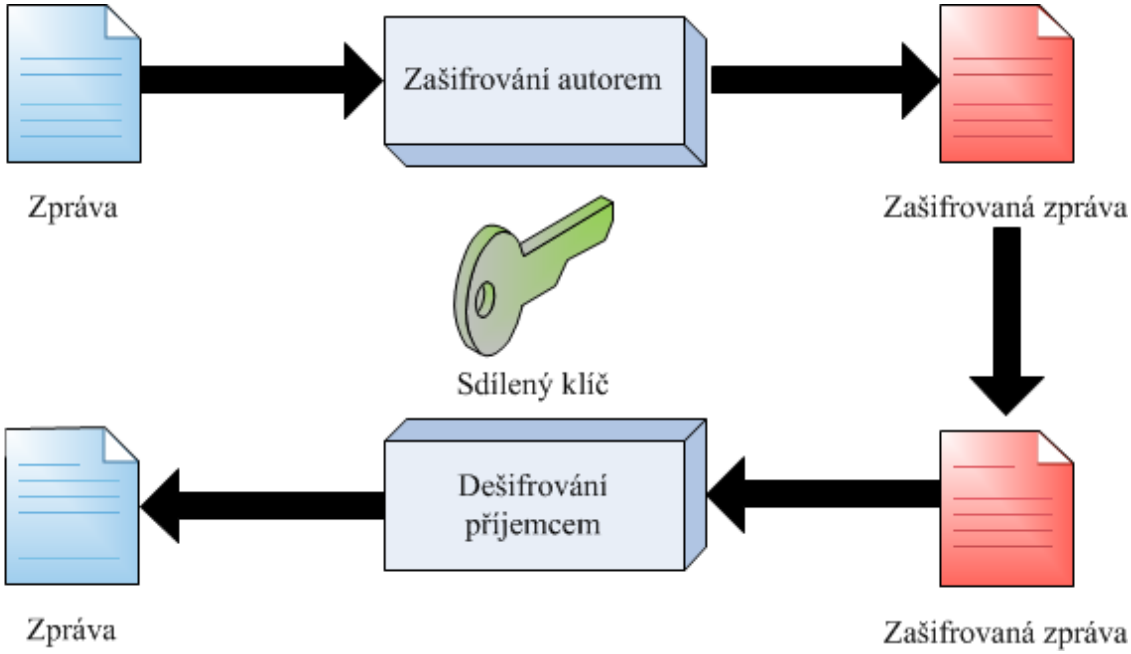
Symetrické šifrování je založeno na jediném šifrovacím klíči, který musí být znám jak odesílateli, tak příjemci. Znamená to, že stejný klíč, který byl použit k zašifrování zprávy na straně odesilatele, bude použit i na straně příjemce. Volbou délky klíče významně ovlivníme stupeň zabezpečení. Délka klíče 128 bitů je v současnosti uváděna jako doporučený standard, nicméně čím dál častěji se začínají objevovat požadavky na délku klíče 256 bitů. Při současném výkonu počítačů je nemožné v přijatelném čase vyzkoušet všechny varianty klíčů a tím prolomit šifru.

Použití jednoho klíče pro šifrování i dešifrování je největší slabina symetrického šifrování. Nebezpečí spočívá v tom, že se nějakým způsobem musí šifrovací klíč dostat oběma stranám – ta která chce data zašifrovat a ta která chce data dešifrovat. Pro přenos šifrovacího klíče je tak potřeba použít nějaký zabezpečený přenos. Další nevýhodou je obtížná distribuce šifrovacích klíčů v rozsáhlých sítích a jejich složitá logistika.

Největší výhoda symetrického šifrování spočívá v nenáročnosti na výpočetní výkon. Toto zatížení je měřitelně až tisíckrát menší než při šifrování asymetrickém a je tedy výrazně rychlejší.

Symetrické šifry dělíme na dvě kategorie a to na šifry blokové a šifry proudové:

- blokové šifry - jedná se o rozšířenější šifrování, které výchozí bitový sled rozdělí na bitová slova a ty poté vhodně doplní bitovou šifrou tak, aby všechna slova měla shodnou velikost;
- proudové šifry - šifrování probíhá pomocí šifrovacího klíče postupně bit po bitu, každý bit je jednotlivě zašifrován.



Obr. 1. Symetrická šifra. Zdroj [Vlastní zpracování]

Symetrických šifrovacích algoritmů je celá řada. Snad nerozšířenějším je algoritmus DES, používající šifrovací klíč délky 56 bitů. Dnes se však považuje za nedostatečný. Z algoritmu DES byl odvozen algoritmus 3DES s klíčem 112 bitů nebo 168 bitů. Dále se používají algoritmy s délkou klíče 128 bitů (IDEA, RC2, RC4 atd.). Aktuálně doporučovaným algoritmem je však algoritmus AES s délkou klíče 128, 192 nebo 256 bitů. [1]

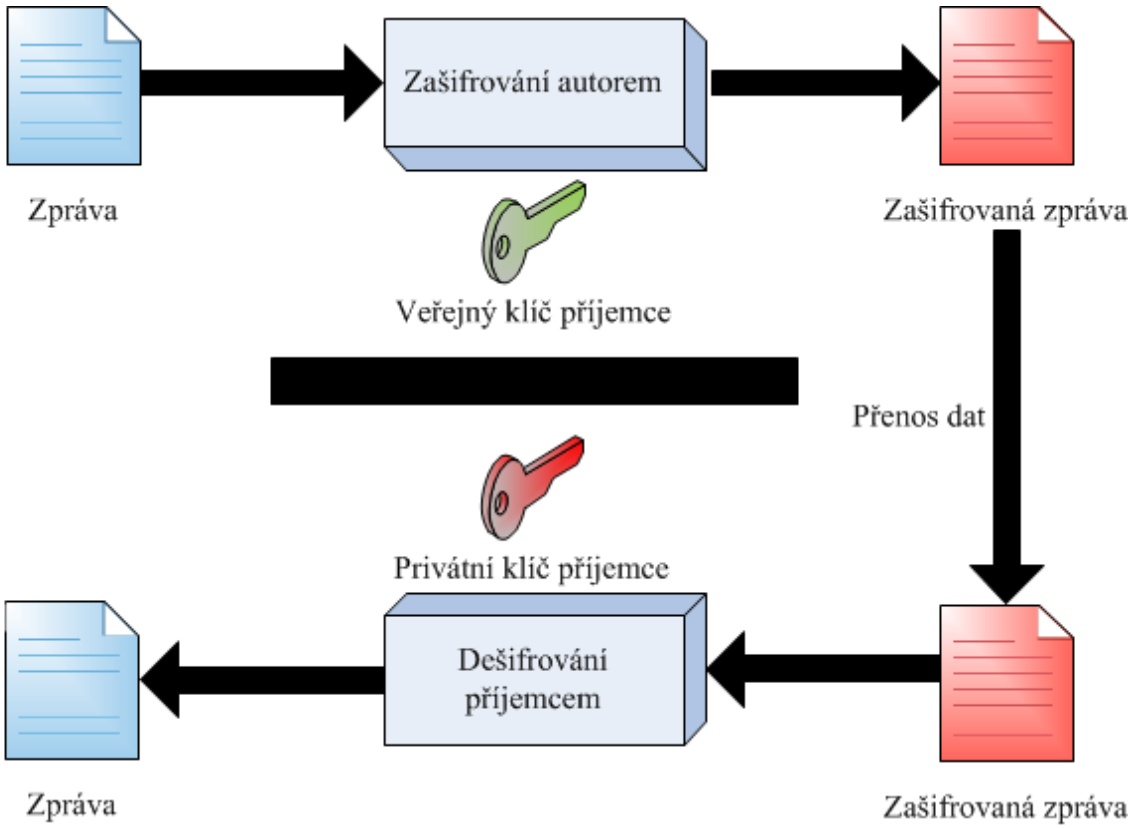
2.2 Asymetrické šifry

Rozdílným typem šifer jsou asymetrické šifry. Tyto šifry nepoužívají jeden privátní šifrovací klíč sdílený mezi příjemcem a odesilatelem, ale používá se dvojice šifrovacích klíčů. Jeden klíč pro dešifrování a druhý pro šifrování. U elektronického podpisu nemluvíme o šifrovacím a dešifrovacím klíči, ale o veřejném a privátním klíči.

Podstata spočívá v tom, že data šifrovaná veřejným klíčem lze dešifrovat pouze se znalostí druhého privátního klíče a naopak. Privátní klíč je s maximální mírou chráněn majitelem (tokeny, čipové karty, CD v trezoru atd.), zatímco druhý klíč je naopak zveřejněn. Je-li zpráva zašifrována privátním klíčem a příjemce zprávy má k dispozici odpovídající veřejný klíč, je schopen zprávu dešifrovat pomocí veřejného klíče. Protože je veřejný klíč vystaven na Internetu, nelze privátním klíčem šifrovanou zprávu považovat za zašifrovanou v plném smyslu slova, ale pouze za autorizovanou.

Pokud chce osoba A šifrovat zprávu osobě B asymetrickou šifrou, potom:

1. Osoba B, příjemce zprávy, si musí vygenerovat dvojici klíčů: veřejný klíč a privátní klíč.
2. Osoba B si uloží svůj privátní klíč do důvěryhodného úložiště klíčů. Např. na disk, na čipovou kartu atd. Soukromý klíč je aktivem osoby B, který si musí střežit.
3. Osoba B distribuuje svůj veřejný klíč do celého světa.
4. Osoba A po obdržení veřejného klíče osoby B šifruje zprávu osobě B jejím veřejným klíčem.
5. Osoba B (příjemce) dešifruje přijatou šifrovanou zprávu svým privátním klíčem a získá původní zprávu.



Obr. 2. Asymetrická šifra. Zdroj [Vlastní zpracování]

Jednou ze základních vlastností šifrování na bázi asymetrických algoritmů je skutečnost, že je relativně jednoduché za využití veřejného klíče šifrovat text, ale na základě znalosti veřejného klíče a veřejným klíčem šifrované zprávy je velice obtížné získat původní zprávu.

Pravděpodobně nejznámějším asymetrickým šifrovacím algoritmem je algoritmus RSA. Délka šifrovacích klíčů pro algoritmus RSA se považuje za ještě bezpečnou, pokud je alespoň 1024 bitů. Často se však používají klíče dlouhé 2048 nebo i 4096 bitů. Existují i jiné asymetrické algoritmy. Dnes se často mluví o algoritmu ECC Elliptic Curve Cryptography. Obecně se míní, že z bezpečnostního hlediska odpovídá 1024 bitů dlouhému RSA klíči 160 bitů dlouhý ECC klíč, přičemž výpočetní náročnost je srovnatelná. Jiným algoritmem je Diffie-Hellmanův (DH) algoritmus. Bez ohledu na délku klíčů obecně platí, že asymetrické šifrovací algoritmy jsou výpočetně mnohem náročnější než symetrické algoritmy. [1]

2.3 Hashovací funkce

Použití asymetrických algoritmů je mnohem pomalejší než používání symetrických algoritmů. Proto při se při tvorbě elektronického podpisu nešifruje privátním klíčem odesilatele celá zpráva, ale nejprve se na zprávu použije takzvaná hashovací funkce. Hash je jednocestná funkce, která z libovolně dlouhého textu vytvoří krátký řetězec konstantní délky. Výsledný řetězec (otisk) by měl maximálně charakterizovat původní text. [4] Typická velikost výsledného textu je 16 B (např. algoritmus MD-5) nebo 20 B (algoritmus SHA-1). Dnes se již algoritmy MD-5 a SHA-1 vesměs považují za slabé, proto se stále častěji setkáváme s novými algoritmy produkujícími delší otisky: SHA-224 (otisk dlouhý 28 B), SHA-256 (otisk 32 B), SHA-384 (otisk 48 B) a SHA-256 někdy též označovanou SHA-2 s otiskem dlouhým 64 B. Jednocestnou funkcí se rozumí algoritmy, které nejsou výpočetně náročné. Je však výpočetně velice náročné k výsledku nalézt původní text. [1]

Z hlediska bezpečnosti musí hashovací funkce splňovat následující požadavky:

1. **Odolnost vůči získání předlohy** (Preimage resistance). Pro všechny výstupy z hashovací funkce je výpočetně nemožné získat vstup, kterému odpovídá daný otisk. Z dané hash hodnoty nelze získat původní dokument, jedná se o jednocestnou funkci.
2. **Odolnost vůči získání jiné předlohy** (2nd preimage resistance) Je výpočetně prakticky nemožné najít dokument, jehož hash hodnota odpovídá hash hodnotě původního dokumentu.
3. **Odolnost vůči nalezení kolize** (collision resistance) je prakticky nemožné najít dva dokumenty se stejnou hash hodnotou.

Bezpečnost hashovacích funkcí je jeden z klíčových parametrů bezpečnosti elektronického podpisu. Zákonem o elektronickém podpisu je implementována směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy. Pro praktickou část implementace směrnice jsou orgánem k tomu komisí určeném, tj. Evropským ústavem pro telekomunikační normy (European Telecommunications Standards Institute, ETSI) vydávány dokumenty typu „technical specification (TS)“. Jedním z nich je ETSI TS 102 176-1 V2.0.0 (dále jen „ALGO Paper“), který stanoví přípustné algoritmy a jejich parametry pro elektronické podpisy a kvalifikované certifikáty, které jsou vydávány v souladu se směrnicí. Ministerstvo vnitra se

při zveřejňování kryptografických algoritmů a jejich parametrů řídí tímto dokumentem. ALGO Paper ETSI TS 102 176-1 V2.0.0 (2007-11) stanoví pro jednotlivé algoritmy dobu, po kterou lze předpokládat, že budou považovány za bezpečné. [7]

Tab. 1. Doporučené hashovací funkce. Zdroj [7]

Entry name of the hash function	1 year	3 years	6 years	10 years (speculative)
sha1	usable	unknown	unusable	unusable
ripemd160	usable	usable	unusable	unusable
sha224	usable	usable	usable	unusable
sha256	usable	usable	usable	unusable
sha384	usable	usable	usable	usable
sha512	usable	usable	usable	usable
Whirlpool	usable	usable	usable	usable

Ačkoliv výše uvedená doporučení popisující bezpečnost a použitelnost kryptografických algoritmů se týkají především elektronického podpisu, můžeme je aplikovat i obecně, například pro oblast šifrování nebo autentizaci.

Národní bezpečnostní úřad nařizuje certifikčním autoritám k 31. 12. 2010 přejít od hashovací funkce SHA-1 na novou generaci hashovacích funkcí SHA-2 (SHA-224, SHA-256, SHA-384 a SHA-512) a doporučuje prozkoumat všechny bezpečnostní aplikace i kryptografické prostředky, ve kterých se využívá hashovacích funkcí a posoudit vliv kryptoanalytických útoků na jejich bezpečnost.

Bylo tedy nezbytné ukončit používání hashovací funkce třídy SHA-1 a nahradit ji hashovací funkcí třídy SHA-2. Poskytovatelé certifikačních služeb ukončili používání algoritmu SHA-1 při vydávání kvalifikovaných certifikátů k 31. 12. 2009. Pro vytváření elektronického podpisu je možné po přechodnou dobu nadále používat algoritmus SHA-1, nejdéle však do 31. 12. 2010. [7]

Pro algoritmus RSA stanoví ALGO paper ETSI TS 102 176-1 V2.0.0 (2007-11) následující délky klíčů pro tvorbu elektronického podpisu. [8]

Tab. 2. Délka klíčů. Zdroj [8]

Parameter	1 year	3 years	6 years	10 years (speculative)
MinModLen	1 024	1 536	2 048	?

Je zřejmé, že délka klíče 1024 bitů pro algoritmus RSA je již považována za nedostatečnou.

Zákon o elektronickém podpisu neumožňuje ministerstvu vnitra přikazovat nebo omezovat použití konkrétních kryptografických algoritmů uživatelům elektronického podpisu, jeho pravomoc sahá pouze k akreditovaným poskytovatelům certifikačních služeb. To prakticky znamená, že certifikační autority musí v souladu s výše uvedenými standardy a s vyhláškou ministerstva s účinností od 1. 1. 2010 vydávat kvalifikované certifikáty využívající silnější hashovací funkci SHA-2 a kryptografii RSA s klíčem 2048.

2.4 Elektronický podpis

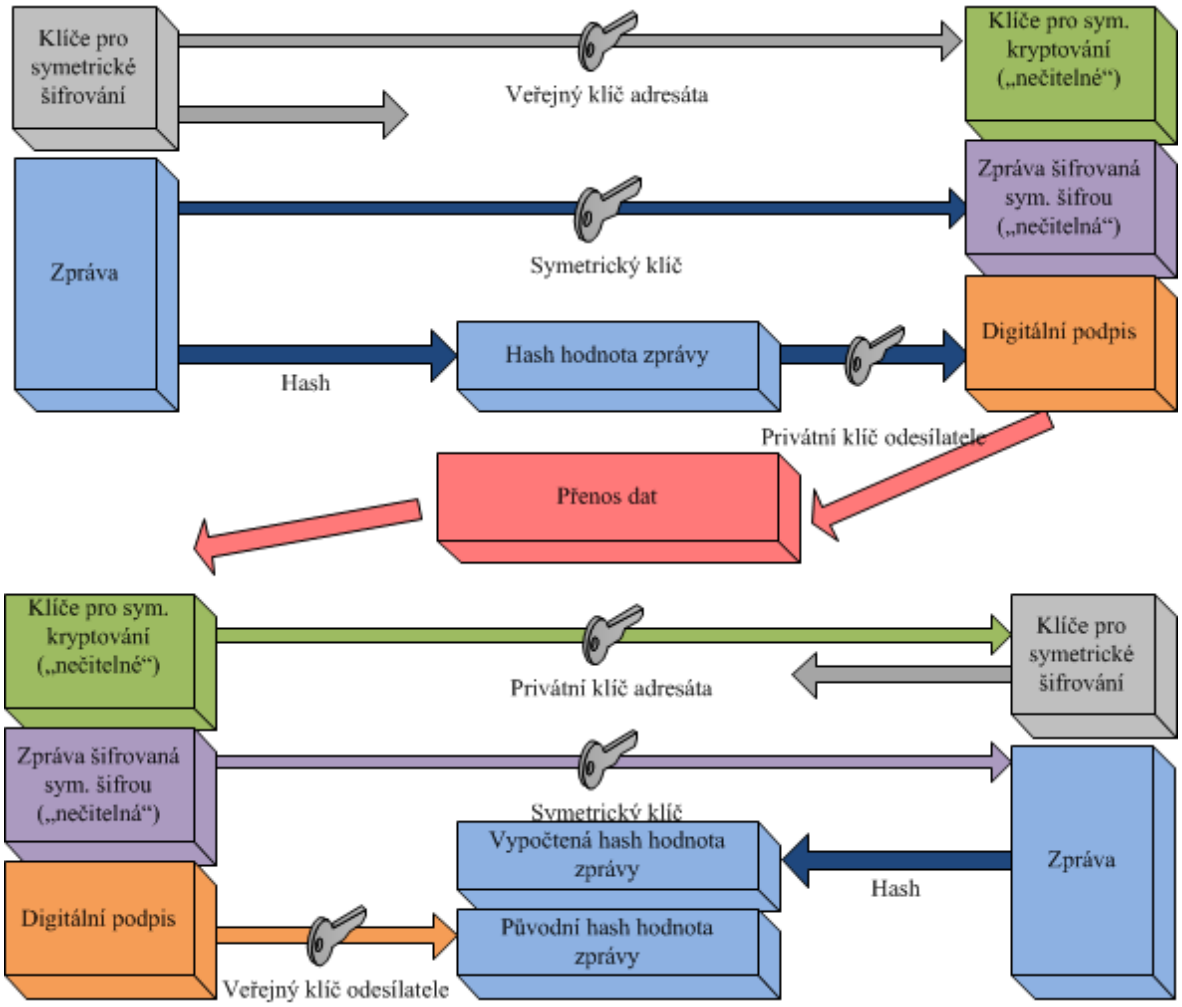
Jednou z podmínek pro praktické využití a nasazení elektronického podpisu a elektronické komunikace je nastavení takových principů a postupů, které bude možné považovat za rovnocenné běžné papírové agendě.

Tyto požadavky se řeší prostřednictvím kryptografických technologií. Elektronický podpis umožňuje zajistit autentizaci komunikujících stran, důvěryhodnost komunikačních systémů, průkaznost jejich kroků a integritu přenášených zpráv.

Jednotlivé kroky prakticky užívané šifrované komunikace s využitím elektronického podpisu lze popsat takto:

1. Odesilatel zprávy nejprve vytvoří hash hodnotu zprávy a tu zašifruje svým privátním klíčem, čímž zprávu elektronicky podepíše (vznikne elektronický podpis zprávy).

2. Následně se celá zpráva zašifruje symetrickým klíčem (zajištění důvěrnosti zprávy). Symetrická šifra se používá z důvodu podstatně větší rychlosti šifrování.
3. Samotný symetrický klíč je poté zašifrován veřejným klíčem adresáta, čímž je zaručeno, že se k tomuto klíči dostane pouze adresát se svým privátním klíčem, který ho užije k dešifrování zprávy.
4. Zašifrovaná a elektronicky podepsaná zpráva je zaslána po Internetu adresátovi.
5. Adresát zprávu dešifruje za pomoci svého soukromého klíče a získá přístup k symetrickému klíči.
6. Celá zpráva se dešifruje pomocí symetrického klíče.
7. Adresát zprávu ověří pomocí veřejného klíče odesílatele (ověření elektronického podpisu) a výpočtem hash hodnoty zprávy a jejím srovnáním s dešifrovanou hash hodnotou z elektronického podpisu. Pokud jsou srovnávané hash hodnoty shodné, je zřejmé, že zpráva nebyla během podepsání a přenosu změněna (kontrola integrity zprávy).



Obr. 3. Šifrovaná komunikace. Zdroj [Vlastní zpracování]

3 CERTIFIKAČNÍ AUTORITY A CERTIFIKÁTY

Certifikát je možné chápat jako jistou podobu občanského průkazu. Obsahuje jméno a příjmení uživatele, jeho veřejný klíč, datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a další technické informace.

Certifikační autorita (CA) vystupuje při vzájemné komunikaci dvou subjektů jako třetí, nezávislý a důvěryhodný subjekt, který prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu (fyzickou identitu) s jeho dvojicí klíčů (elektronickou identitou), respektive následně s jeho elektronickým podpisem. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu v rámci vydávaných certifikátů. To je zajištěno legislativními a technickými pravidly provozu instituce CA. Splnění těchto požadavků potvrdí CA podpisem dokumentu svým soukromým klíčem a následným vydáním tohoto certifikátu. [3]

3.1 Druhy certifikátů

Certifikační autorita, která certifikát vystaví, musí zaručit jeho důvěryhodnost. To znamená, že veřejný klíč uživatele, uvedený v příslušném certifikátu, skutečně patří osobě, která je v certifikátu uvedena jako její vlastník. Tato důvěryhodnost je zajištěna tím, že certifikační autorita sama podepíše vystavený certifikát svým vlastním elektronickým podpisem. Za důvěryhodnost certifikátu tedy ručí jeho vydavatel, sama certifikační autorita.

Certifikáty CA jsou dvojího druhu. V závislosti na lokální legislativě členských zemí EU je CA vydán certifikát institucí, jejíž důvěryhodnost byla určena a ověřena zvláštním zákonem. (na Slovensku například Národný bezpečnostný úrad - CA NBÚ SR). [23]

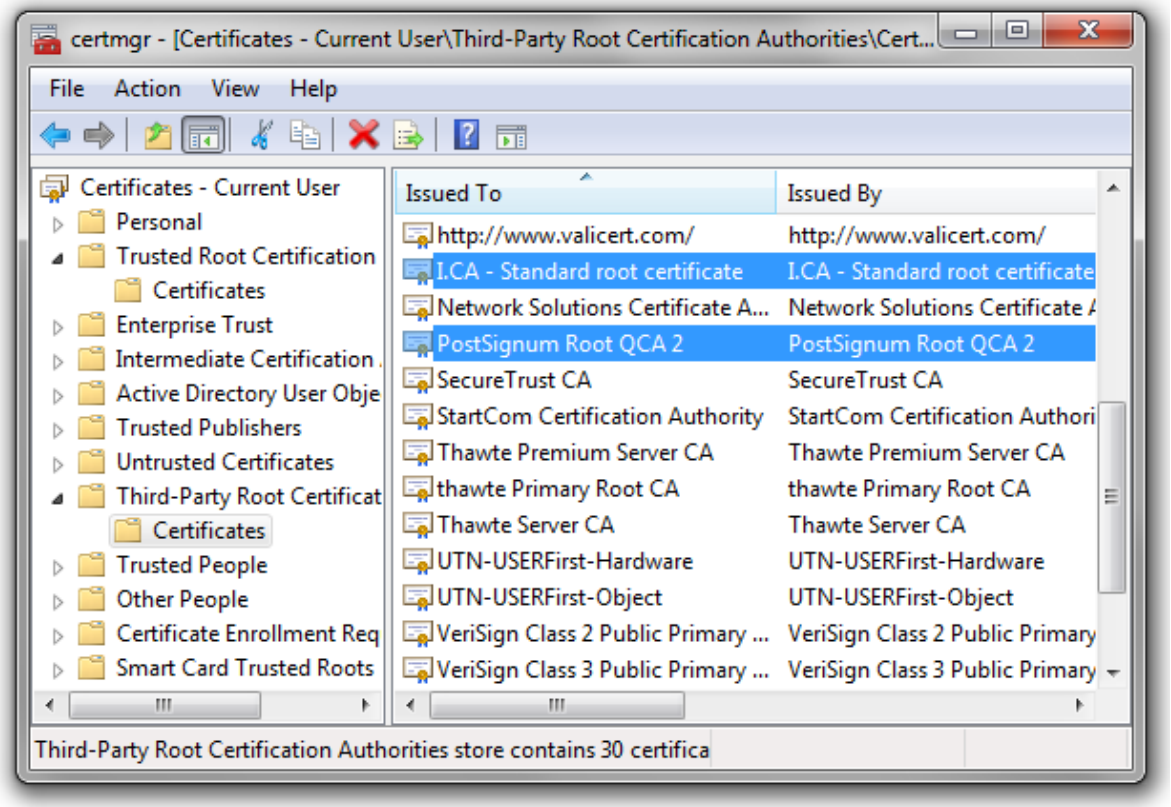
Častější případ je ten, že si CA vydá certifikát sama. Tento druh certifikátu se nazývá kořenový. Neznamená to ovšem, že automaticky poskytuje dostatečnou záruku pravosti a důvěryhodnosti vydavatele. Tuto důvěryhodnost získá CA až po splnění následujících podmínek:

- splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona č. 227/2000 Sb., (zákon o elektronickém podpisu);

- splnění podmínek, požadavků a postupů stanovených vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb);
- ověření kvalifikovaných systémových certifikátů Ministerstvem informatiky podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu.

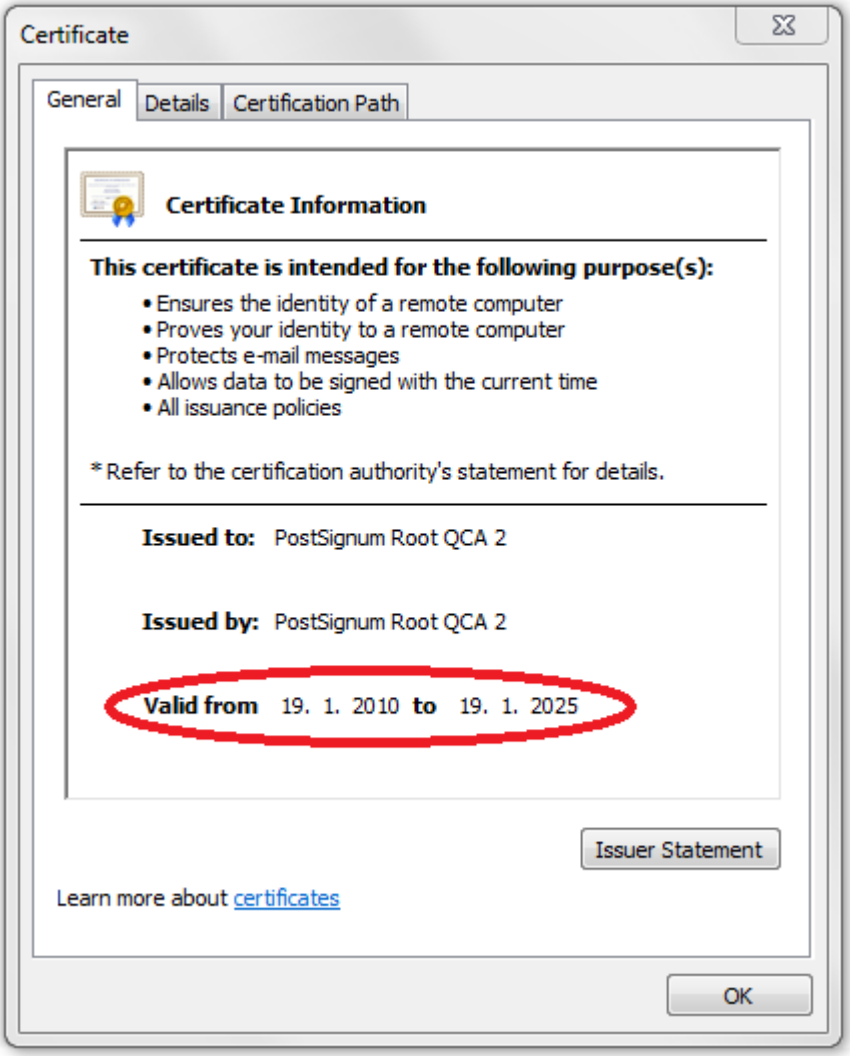
3.1.1 Kořenové certifikáty

V prostředí Windows jsou ke dni 21. 3. 2011 předinstalovány kořenové certifikáty pouze dvou ze tří tuzemských poskytovatelů certifikačních služeb - společnost I. CA a.s. a PostSignum Česká pošta s. p.. Kořenové certifikáty třetího tuzemského poskytovatele eIdentity a.s. je nutné nainstalovat do části úložiště důvěryhodných certifikátů na svém počítači manuálně. Instalací kořenového certifikátu se zabývá podrobněji kapitola 5.3 v praktické části diplomové práce.



Obr. 4. Kořenové certifikáty v úložišti Windows. Zdroj [Vlastní zpracování]

Certifikáty CA mají omezenou životnost. Jsou sice vydávány na relativně dlouhou dobu (podstatně delší než platnost klientského certifikátu), ale i tento certifikát po určité době vyprší. Z tuzemských CA má nejdelší platnost PostSignum, která vydala svůj kořenový certifikát na 15 let. Následuje eIdentity s délkou 12 let a I.CA s 10ti lety.



Obr. 5. Platnost certifikátu. Zdroj [Vlastní zpracování]

3.1.2 Klientské certifikáty

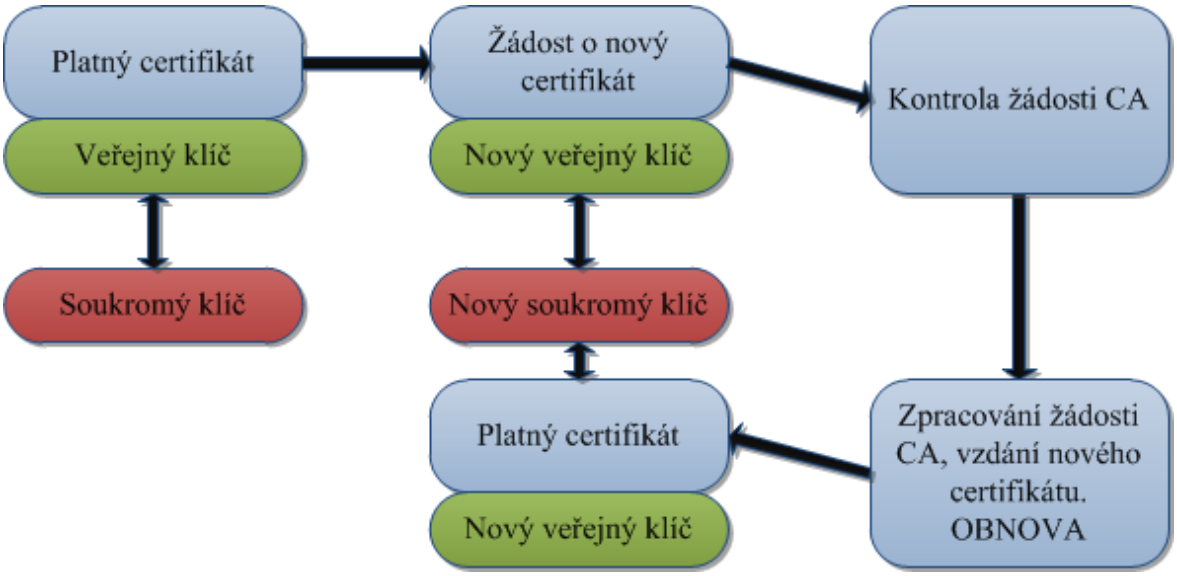
Certifikačních autority vydávají několik druhů klientských certifikátů.

1. **Komerční certifikát** je nejrozšířenějším typem. Toto označení se používá u certifikátů, které nejsou spojeny se zákonem o elektronickém podpisu. Tento certifikát je vhodný pro použití v uzavřených systémech, kde je mezi účastníky bezpečné komunikace současně uzavřena smlouva, řešící mimo jiné i podmínky komunikace (zajištění autentizace komunikujících stran, šifrování přenášených zpráv).
2. **Serverové certifikáty** patří také mezi komerční certifikáty. Jsou určené pro bezpečnou komunikaci serverů nebo pro autentizaci webových serverů přes protokol https. v certifikátu je obsaženo jednoznačné jméno serveru.
3. **Kvalifikované certifikáty** jsou určeny výhradně pro elektronický podpis. Kvalifikovaný certifikát je vytvořen tak, že splňuje všechny aktuální požadavky dané legislativou v souladu se zákonem o elektronickém podpisu. Využívá se zejména při komunikaci s úřady státní správy, kde nelze použít komerční certifikáty.
4. **Systémový kvalifikovaný certifikát** není přímo vázán na konkrétní osobu. Je určen zejména pro organizace, které potřebují zautomatizovat elektronické podepisování například odesílaných odpovědí na obdržené zprávy či výpisů z různých registrů.
5. **Testovací certifikát** slouží mimo jiné k ověření funkčnosti technologie, použité pro realizaci tvorby elektronického podpisu. Platnost testovacího certifikátu je krátká, řádově několik dní. Tyto certifikáty nejsou zveřejňovány na seznamu veřejných certifikátů a jsou vydávány zdarma.

3.1.3 Obnova certifikátu

Aby uživatel nemusel každý rok žádat o nový certifikát a procházet celou proceduru vydání nového certifikátu znovu, je možné u CA zažádat o obnovu certifikátu. CA při obnově certifikátu využije informace, které získala při vydání předchozího certifikátu.

Celý proces obnovy certifikátu má dvě podmínky, které je nutno dodržet. První podmínkou je, že osobní údaje, které uživatel uvedl při vydání předchozího certifikátu, jsou stále platné. Druhou podmínkou je, aby žádost o obnovu a obnova certifikátu proběhla ještě v době platnosti předchozího certifikátu.



Obr. 6. Proces obnovy certifikátu. Zdroj [Vlastní zpracování]

V praxi to obvykle probíhá tak, že uživatel před vypršením platnosti stávajícího certifikátu obdrží na e-mail uvedený v certifikátu upozornění na blížící se expiraci certifikátu. Obsahem tohoto e-mailu je URL odkaz na webové stránky CA spolu s postupem, který umožní provést obnovu certifikátu elektronicky. Obnovený certifikát je poté zaslán elektronickou poštou uživateli.

3.1.4 Zneplatnění certifikátu

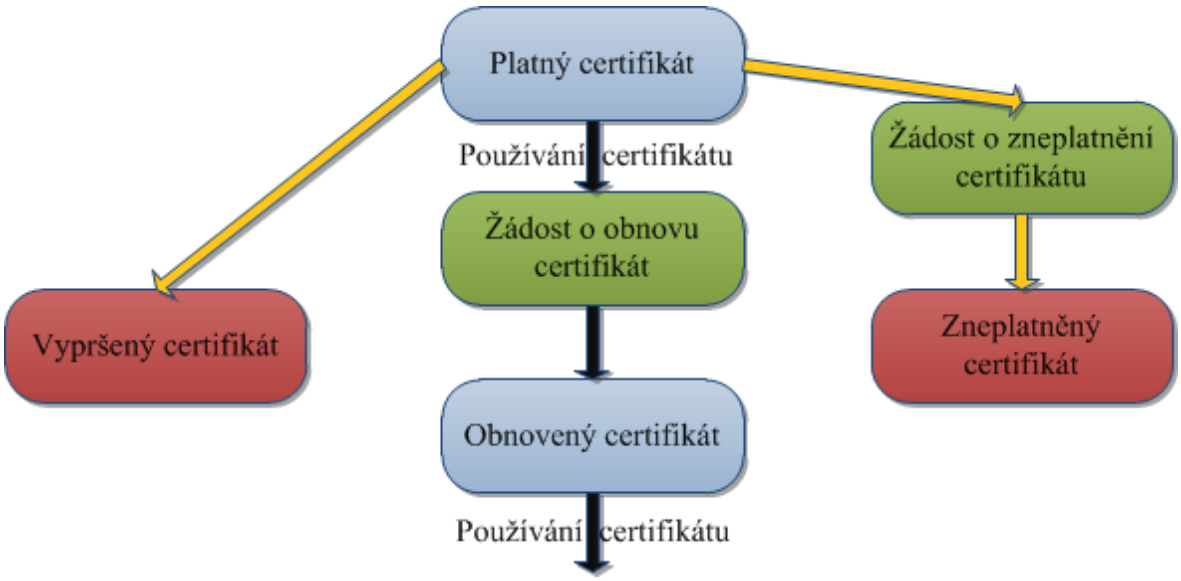
Platnost certifikátu je možné mimořádné ukončit i v době jeho řádné platnosti. Nejčastěji se tak děje z důvodu prozrazení klíčů vlastníka certifikátu nebo krádeže počítače.

Zneplatnění certifikátu lze provést osobní návštěvou CA, kde je potřeba nahlásit požadované údaje.

- jméno a příjmení;
- sériové číslo certifikátu; včetně informace, zda se jedná o dekadické nebo hexadecimální číslo;

- certifikační autoritu, která vydala certifikát;
- heslo pro zneplatnění.

Všechny tyto informace lze vyčíst z protokolu o vydání certifikátu. Sériové číslo certifikátu je v protokolu uvedeno v dekadickém tvaru. Pracovník CA ověří, zda heslo pro zneplatnění souhlasí. [18]



Obr. 7. Životní cyklus certifikátu. Zdroj [Vlastní zpracování]

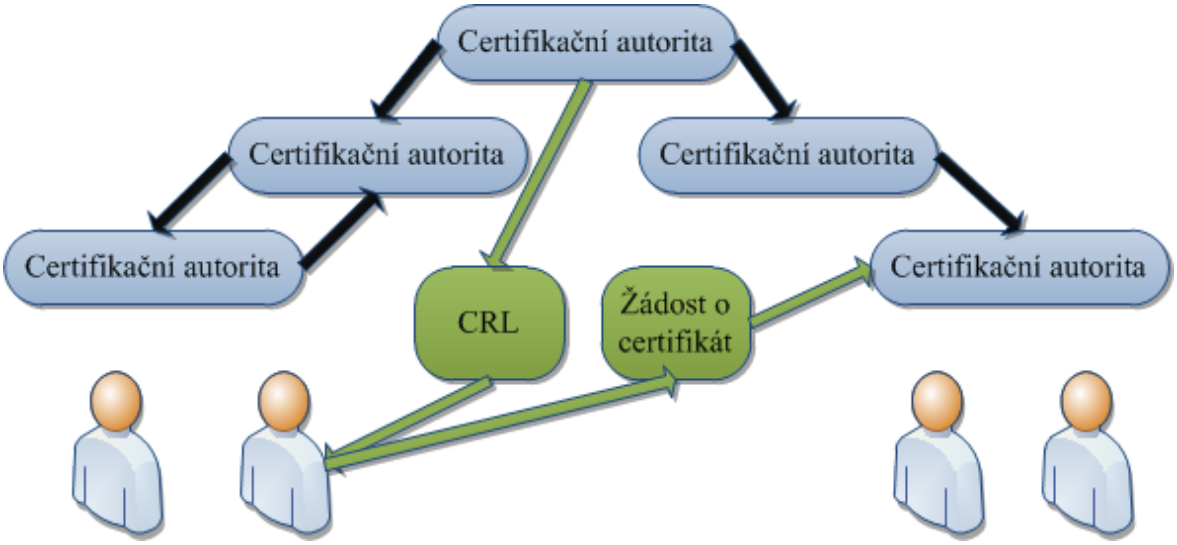
Odvolaný certifikát je zařazen do seznamu zneplatněných certifikátů CRL - Certificate revocation list. Certifikační autority vydávají tento veřejně přístupný seznam v pravidelných intervalech na svých webových stránkách. V něm jsou zapsány informace o certifikátech, které jejich vlastníci nechali zneplatnit.

3.2 Certifikační autority

Digitální certifikát svazuje konkrétní osobu s párem klíčů, sloužících pro vytvoření a ověření elektronického podpisu. Pokud má být ovšem certifikát pro příjemce zprávy důvěryhodný, musí jej vydat nějaký nezávislý, dostatečně důvěryhodný subjekt. A tímto subjektem je právě certifikační autorita.

Činnost certifikační autority by se dala přirovnat k činnosti notáře při ověřování klasického podpisu. Je zde ovšem jedna zásadní odlišnost - zatímco notář musí ověřit každý jednotlivý podpis, certifikační autorita neověřuje vlastní podpis, ale data pro vytváření elektronického podpisu, skutečných podpisů potom můžeme pomocí těchto dat vytvořit libovolné množství. [25]

CA nemusí existovat pouze samostatně. Na Internetu, kde mezi jednotlivými CA panuje konkurenční prostředí, není propojování jednotlivých CA běžné. Jinak je tomu ale v rozsáhlých sítích nebo organizacích, kde je běžné propojení na různých úrovních poskytovaných služeb. CA jsou propojeny ve stromové struktuře, kde si pomocí vzájemné autentizace směrem vzhůru projevují důvěru.



Obr. 8. Propojení certifikačních autorit. Zdroj [Vlastní zpracování]

3.3 Časová razítka

Časové razítko spojuje dokument v elektronické podobě s časovým okamžikem jeho vzniku a zaručuje, že konkrétní data v elektronické podobě v daný časový okamžik existovala. Časové razítko důvěryhodným způsobem označuje elektronický dokument v konkrétním čase a je tedy elektronickým důkazem o existenci určitého dokumentu v daném čase.

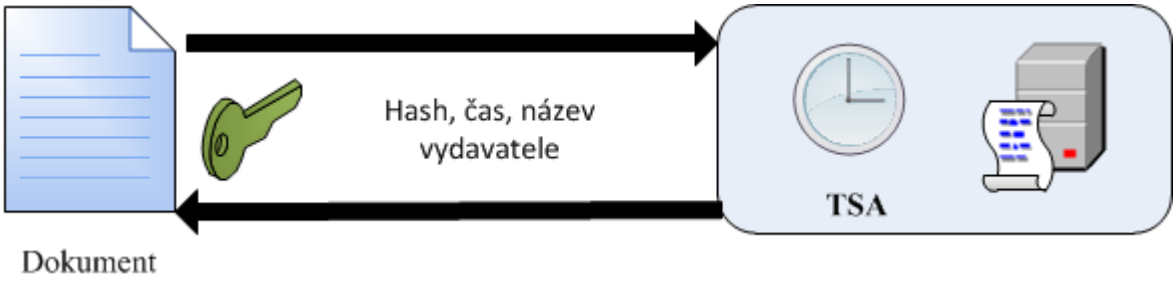
Zásadní rozdíl mezi certifikátem a časovým razítkem je v tom, že certifikát je vázán na osobu či subjekt vlastníka, zatímco časové razítko je spojeno s dokumentem.

Nejdůležitějším údajem, který je vkládán do časového razítka, je čas vydání. Ke zjištění přesného času využívají certifikační autority synchronizaci s důvěryhodnými časovými servery pomocí NTP protokolu.

Časová razítka vydává poskytovatel certifikačních služeb na základě obdržené žádosti. Prvním krokem je vytvoření jedinečného otisku (hash) dokumentu, ke kterému má být časové razítko vystaveno. Tento hash řetězec poté je zaslán poskytovateli certifikačních služeb. Autorita doplní hash řetězec o přesný časový údaj a z tohoto spojení je vygenerován nový hash, který poskytovatel elektronicky podepíše svým privátním klíčem časové autority. Tyto podepsaná data zašle zpět označené jako časové razítko.

Vydání časového razítka lze rozdělit do několika fází:

1. Vytvoření žádosti o vydání časového razítka.
2. Odeslání žádosti o vydání časového razítka poskytovateli certifikačních služeb.
3. Zpracování žádosti o časové razítko.
4. Přijetí odpovědi od poskytovatele certifikačních služeb.
5. Kontrola odpovědi na žádost o vydání časového razítka.



Obr. 9. Postup získání časového razítka. Zdroj [Vlastní zpracování]

Mezi nejčastější způsoby využití patří práce s dokumenty. Časové razítko se využívá ve spojení s elektronickým podpisem, kdy je potřeba jednoznačně doložit čas, ve kterém dokument existoval a zároveň prokázat autenticitu.

4 ELEKTRONICKÝ PODPIS A LEGISLATIVA

Vůbec prvním platným zákonem o elektronickém podpisu se stal UTAH Digital Signature Act v roce 1995. V Evropě směřoval rozvoj legislativy ke standardizaci, která se promítala do lokálních zákonů. V říjnu 1997 bylo předloženo Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů sdělení nazvané "O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování". [9] Závazným výstupním dokumentem z toho sdělení pro členské státy EU je směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999. [10]

Transformace požadavků směrnice do právních norem jednotlivých států byla realizována několika způsoby. Tím nejrozšířenějším je vydání zákona o elektronickém podpisu jako samostatné právní normy. Touto cestou se vydala i Česká republika, kde byl zákon o elektronickém podpisu přijat v roce 2000 a ČR se tak stala teprve třetí zemí na světě, kde vstoupil v platnost zákon Zákon č. 227/2000 Sb. o elektronickém podpisu. [11]

Tehdejší garant elektronického podpisu, Úřad pro ochranu osobních údajů, udělil společnosti První certifikační autorita I.CA, a.s. akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 18. 3. 2002. Tím byla v České republice fakticky zahájena éra legalizace a využívání zaručeného elektronického podpisu.

4.1 Legalizace a standardizace elektronického podpisu

V mezinárodním měřítku se průkopníkem standardizace a legalizace elektronického podpisu stala komise OSN pro mezinárodní právo UNCITRAL - United Nations Commission on International Trade Law, která byla založena Rezolucí OSN č. 2205(XX) ze dne 17. prosince 1966. [12] Byla založena za účelem odstraňování právních překážek v mezinárodním obchodu a koordinovat rozvoj mezinárodního obchodního práva. Komise má v současnosti 60 členských států, přičemž Českou republiku v komisi zastupuje Ministerstvo průmyslu a obchodu.

Komise UNCITRAL vydává mnoho různých dokumentů týkajících se mezinárodního obchodu. Z oblasti elektronického podpisu jsou nejdůležitější dokumenty:

- doporučení UNCITRAL, týkající se právní závaznosti elektronických údajů (1985);
- vzorový zákon UNCITRAL o elektronickém obchodu (1996);
- vzorový zákon o elektronickém podpisu (2001);
- úmluva o užití elektronických sdělení v mezinárodním obchodě (2005). [13]

Z hlediska legalizace a standardizace elektronického podpisu bylo důležitým okamžikem předložení a schválení vzorového zákona o elektronickém obchodu Valným shromážděním OSN v prosinci 1996. Zákon obsahuje následující hlavní body: [3]

1. Obecná opatření
   1.1. Okruh aplikace
   1.2. Definice pojmů
   1.3. Interpretace
   1.4. Změna úmluv
2. Aplikace právních požadavků na datové zprávy
   2.1. Aplikace rozpoznání datových zpráv
   2.2. Dokument
   2.3. Podpis
   2.4. Originál
   2.5. Přístupnost a průkazná váha datové zprávy
   2.6. Uchovávání datových zpráv
3. Komunikace datovými zprávami
   3.1. Vytváření a platnost kontraktů
   3.2. Rozpoznávání účastníků datových zpráv
   3.3. Atributy datových zpráv
   3.4. Potvrzení přijetí
   3.5. Čas a místo odeslání a přijetí datových zpráv

Po schválení vzorového zákona o elektronickém obchodu komise UNCITRAL zahájila přípravu příslušných podkladů pro oblast elektronického podpisu a poskytování certifikačních služeb. Příprava, které se zúčastnilo 50 států a mezinárodních organizací, byla završena v roce 2001 předložením a schválením vzorového zákona UNCITRAL o elektronickém podpisu. Komise doporučila všem signatářským státům zvážit využití tohoto zákona při tvorbě domácích právních předpisů.

Vzorový zákon se dělí na dvě samostatné části. První část popisuje hlavní pojmy, terminologii a definice. Součástí druhé části je návod k ustanovení modelového zákona o elektronickém podpisu. Skládá se z následujících bodů:

1. Účel a původ modelového zákona
    1.1. Účel
    1.2. Podklady
    1.3. Historie
2. Modelový zákon jako nástroj pro harmonizaci zákonů
3. Obecné znaky elektronického podpisu
    3.1. Funkce podpisu
    3.2. Digitální podpis a jiné elektronické podpisy
    3.3. Elektronický podpis založený na jiných technikách než kryptografii s veřejnými klíči
    3.4. Digitální podpis založený na kryptografii s veřejnými klíči
    3.5. Technické pojmy a terminologie
        3.5.1. Kryptografie
        3.5.2. Veřejné a soukromé klíče
        3.5.3. Hash funkce
        3.5.4. Digitální podpis
        3.5.5. Ověření digitálního podpisu
    3.6. Infrastruktura veřejných klíčů a poskytovatelé certifikačních služeb

4.2 Legislativa a směrnice v EU

Vývoj k vytvoření závazné směrnice EU k elektronickému podpisu trval zhruba dva roky s cílem stanovit její principy, zaměření a konkrétní pojmy. Výsledkem vývoje je směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999. [10]

Obsah směrnice se zaměřuje především na elektronické podpisy používané pro účely autentizace (ověření identity subjektu) a aplikací zaručených elektronických podpisů. Dále se věnuje použitelnosti a právní validitě elektronických podpisů připojených ke konkrétním dokumentům a stanoví požadavky, které mají být splněny poskytovateli certifikačních služeb.

Směrnice dodržuje následující principy:

- technologická neutralita (základním smyslem je orientace na technologie digitálních podpisů, s cílem zůstat neutrální a vyhovět tak i jiným technologickým principům);

- pro poskytovatele certifikačních služeb není apriori definováno žádné schéma pro autorizaci k provádění těchto služeb tak, aby v budoucnu existovala principiální možnost technologických inovací;
- rozpoznání zákonné platnosti elektronických podpisů tak, aby nemohla být popřena jejich platnost na základě toho, že jsou v elektronické podobě a byla zaručena ekvivalence s ručně napsaným podpisem. [14]

Směrnice počítá s tím, že v každé členské zemi bude ustanoveno vlastní akreditační schéma pro poskytovatele certifikačních služeb. Podle směrnice musí být např. kvalifikované certifikáty vydané poskytovateli certifikačních služeb, kteří jsou akreditováni dle národního akreditačního schématu jedné členské země, právně uznávané v ostatních členských zemích EU.

Komisi EU a ostatním členským zemím jsou členské země EU dle směrnice povinny poskytovat následující informace:

- o národním akreditačním schématu;
- jména a adresy národních institucí, zodpovědných za akreditaci a dohled;
- jména a adresy všech poskytovatelů certifikačních služeb.

Jedním z klíčových přínosů směrnice Evropského parlamentu a Rady 1999/93/ES je zavedení společné terminologie ve vztahu k elektronickému podpisu. Stanoví přesný obsah celé řady souvisejících pojmů jako podepisující osoba, data pro vytváření podpisu, data pro ověřování podpisu, prostředek pro vytváření podpisu, atd. Tyto pojmy se dále přenáší do lokálních legislativ členských zemí EU a zvyšují tak srozumitelnost a výklad pojmů. Pro účely této směrnice se rozumí:

1. **Elektronickým podpisem** údaj v elektronické podobě, který je připojen či logicky spojen s jinými elektronickými daty a který slouží jako metoda ověření pravosti.
2. **Zaručeným elektronickým podpisem** elektronický podpis, který splňuje tyto požadavky:

   2.1. je jednoznačně spojen s podepisující osobou;

   2.2. umožňuje zjistit totožnost podepisující osoby;

2.3. je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou;

2.4. je spojen s daty, ke kterým se vztahuje tak, aby bylo možno zjistit jakoukoli následnou změnu těchto dat.

3. **Podepisující osobou** jakákoli osoba, která má prostředek pro vytváření podpisu a která jedná na svůj účet nebo na účet fyzické či právnické osoby nebo subjektu, které zastupuje.
4. **Daty pro vytváření podpisu** jedinečná data, jako jsou kódy nebo soukromé šifrovací klíče, které podepisující osoba používá k vytvoření elektronického podpisu.
5. **Prostředkem pro vytváření podpisu** konfigurovaný softwarový nebo hardwarový prostředek pro využití dat pro vytváření podpis.
6. **Prostředkem pro bezpečné vytváření podpisu** prostředek pro vytváření podpisu, který splňuje požadavky uvedené v příloze III.
7. **Daty pro ověřování podpisu** data, jako kódy nebo veřejné šifrovací klíče, které se používají pro ověřování elektronického podpisu.
8. **Prostředkem pro ověřování podpisu** konfigurovaný softwarový nebo hardwarový prostředek pro využití dat pro ověřování podpisu.
9. **Osvědčením** elektronické potvrzení, které spojuje data pro ověřování podpisu s určitou osobou a potvrzuje totožnost této osoby.
10. **Kvalifikovaným osvědčením** osvědčení, které splňuje požadavky uvedené v příloze I a které vydává ověřovatel, jenž splňuje požadavky uvedené v příloze II.
11. **Ověřovatelem** subjekt nebo právnická či fyzická osoba, která vydává osvědčení nebo poskytuje jiné služby související s elektronickými podpisy.
12. **Produktem pro elektronický podpis** hardware nebo software nebo jeho odpovídající části, které jsou určeny k tomu, aby je ověřovatel používal pro poskytování služeb souvisejících s elektronickými podpisy, nebo které jsou určeny pro vytváření nebo ověřování elektronických podpisů.
13. **Dobrovolnou akreditací** jakékoli povolení, které stanoví zvláštní práva a povinnosti pro poskytování ověřovacích služeb a které uděluje na žádost dotčeného ověřovatele

veřejný nebo soukromý subjekt pověřený stanovením těchto práv a povinností a dohledem nad jejich dodržováním, přičemž ověřovatel není oprávněn vykonávat práva vyplývající z povolení, dokud neobdrží rozhodnutí tohoto subjekt. [10]

Požadavek na akceptování dokumentů opatřených zaručeným elektronickým podpisem jako důkazu při soudním řízení nebo při komunikaci se státní správou ve vztahu občan-stát souvisí s tím, že elektronický podpis je datům v elektronické podobě ve stejném vztahu, jako je vlastnoruční podpis k dokumentům vlastnoručně psaným. Tyto požadavky členských států EU na důvěryhodný elektronický podpis se dělí do pěti základních kategorií:

1. **Kvalifikovaný podpis**. Na tvorbu zaručeného elektronického podpisu musí být použito bezpečné zařízení jako čipová karta nebo podobné zařízení a pro ověření podpisu je užíván kvalifikovaný certifikát.
2. **Kvalifikovaný certifikát**. V tomto případě se neřeší, jaký nástroj klient pro tvorbu zaručeného elektronického podpisu použije. Vyžaduje se pouze užití párových dat spojených s kvalifikovaným certifikátem.
3. **Nedefinovaný certifikát**. Netrvá se na užívání kvalifikovaného certifikátu a neexistuje žádný dohled nad vydáváním a správou certifikátů.
4. **Nedefinovaný podpis.** Netrvá se na užívání kvalifikovaného certifikátu a neexistuje definice elektronického podpisu.
5. **Autentizace.** Systém založený na ověřování pomocí přihlašovacího jména a hesla.

Požadavky jednotlivých států EU na formy elektronického podpisu. [15]

Tab. 3. Formy elektronického podpisu. Zdroj [15]

Kvalifikovaný podpis	Kvalifikovaný certifikát	Nedefinovaný certifikát	Nedefinovaný podpis	Autentizace
Belgie	Bulharsko	Dánsko	Anglie	Kypr
Irsko	Chorvatsko	Lucembursko	Irsko	
Itálie	Česká republika	Polsko		
Lotyšsko	Estonsko			
Portugalsko	Finsko			
Slovensko	Francie			
Španělsko	Maďarsko			
Švédsko	Malta			
Rakousko	Německo			
	Nizozemí			
	Rumunsko			
	Řecko			
	Slovinsko			
	Turecko			

Ve většině legislativ zemí EU je zřejmá snaha o zrovnoprávnění elektronického podpisu a vlastnoručního podpisu v rámci jeho uznatelnosti při právních úkonech. Začlenění požadavků směrnice Evropského parlamentu a Rady 1999/93/ES do právních norem jednotlivých států bylo provedeno několika způsoby. Tím nejrozšířenějším je vydání zákona o elektronickém podpisu jako samostatné právní normy. Tento postup zvolila také Česká republika.

V současné době v rámci zemí EU pracuje na problematice elektronického podpisu sdružení FESA (Forum of European Supervisory Authorities for Electronic Signatures).

FESA je evropské fórum institucí, které na národní úrovni vykonávají akreditační a dozorčí činnost podle Směrnice 1999/93/ES o zásadách společenství pro elektronické podpisy. Jeho členem je v současné době více než 20 států. Cílem fóra je podpora vzájemné spolupráce a koordinace svěřených kompetencí na mezinárodní úrovni, vytváření jednotných stanovisek a komunikace s orgány EU, především s Evropskou komisí. Zástupci členských institucí FESA se schází pravidelně třikrát do roka ke schválení společných stanovisek a k projednání úkolů vzešlých z dosavadní praxe jednotlivých institucí. [3]

4.3 Zákon o elektronickém podpisu v ČR

Česká republika je třetí zemí na světě, kde byl přijat a vstoupil v platnost zákon upravující užívání elektronického podpisu. Zásadním legislativním dokumentem je zákon č. 227/2000 Sb. o elektronickém podpisu. Roli kontrolního a akreditačního orgánu zastává Ministerstvo vnitra ČR. Mezi jeho povinnosti stanovené zákonem o elektronickém podpisu patří zejména:

- udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb;
- vyhodnocování shody nástrojů elektronického podpisu s požadavky stanovenými zákonem o elektronickém podpisu a prováděcí vyhláškou;
- ověřování kvalifikovaných certifikátů poskytovatelů certifikačních služeb, kteří požádali o udělení akreditace;
- dozor nad dodržováním zákona o elektronickém podpisu.

Ministerstvo dále zpracovává návrhy právních předpisů v oblasti elektronického podpisu. V jeho působnosti je rovněž zajištění mezinárodní spolupráce v této oblasti a plnění úkolů plynoucích z členství ČR v mezinárodních organizacích.

Zákon č. 227/2000 Sb. upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. [16] Aktuální verze s účinností od 30 prosince 2010 obsahuje osm částí:

1. Elektronický podpis.
2. Změny občanského zákoníku.
3. Změny občanského soudního řádu.
4. Změny trestního řádu.
5. Změny zákona o ochraně osobních údajů.
6. Změny zákona o správních poplatcích.
7. Řízení podle zákona o elektronickém podpisu.
8. Účinnost.

Jednou z klíčových částí zákona o elektronickém podpisu je vymezení pojmů. Český zákon o elektronickém podpisu definuje elektronický podpis jako „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě", [16] což je vlastně upravená definice daná směrnicí Evropského parlamentu a Rady 1999/93/ES.

U zaručeného elektronického podpisu je situace obdobná. Český zákon opět vychází z definice dané směrnicí 1999/93/ES a říká nám, že zaručeným elektronickým podpisem je elektronický podpis, který splňuje následující požadavky:

1. Je jednoznačně spojen s podepisující osobou.
2. Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
3. Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
4. Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat. [16]

Česká legislativa na rozdíl od většiny legislativ zemí EU obsahuje navíc definici elektronické značky. Pod pojmem elektronická značka rozumíme "údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené" [16] a které splňují tyto požadavky:

1. Jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu.
2. Byly vytvořeny a připojeny k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou.
3. Jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

Z technologického hlediska je elektronická značka stejná jako zaručený elektronický podpis, tj. jedná se o digitální podpis. Odlišnost elektronické značky a zaručeného elektronického podpisu má především právní charakter. Elektronický podpis vytváří fyzická osoba (stejně jako vlastnoruční), elektronickou značkou může datové zprávy označovat i právnická osoba nebo organizační složka státu. Lze ji přirovnat k otisku úředního razítka. Použití elektronické značky urychlí vydávání podepsaných dokumentů, protože značkami budou dokumenty opatřovány automatizovaně, bez nutnosti ověření obsahu každé označované datové zprávy.

Další nejvýznamnější definice uvedené v zákoně o elektronickém podpisu jsou uvedené v následujícím přehledu:

- **podepisující osobou** je fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby;
- **datovou zprávou** jsou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou;
- **certifikátem** je datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu;
- **poskytovatelem certifikačních služeb** je fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy;

- **držitelem certifikátu** je fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro označující osobu a které byl certifikát vydán;
- **kvalifikovaným časovým razítkem** je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem;
- **nástrojem elektronického podpisu** je technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů;
- **elektronickou podatelnou** je pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv;
- **akreditací** je osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

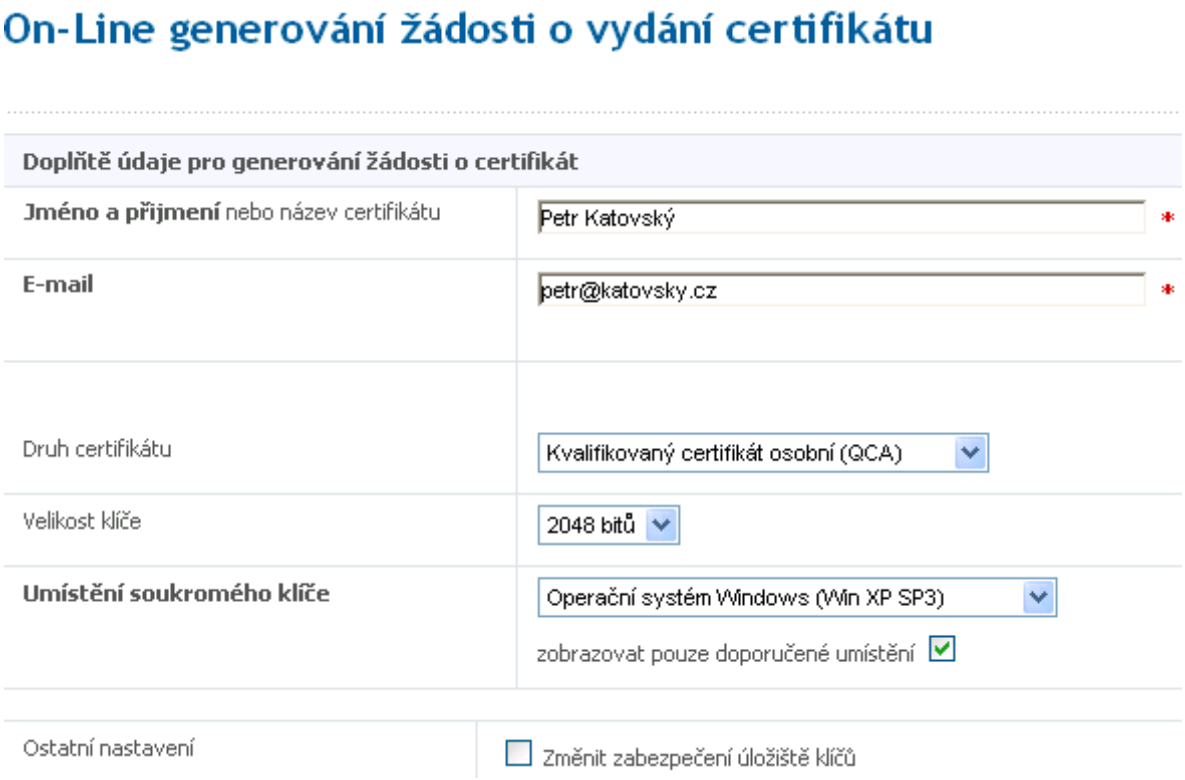
II. PRAKTICKÁ ČÁST

5 ZÍSKÁNÍ KVALIFIKOVANÉHO CERTIFIKÁTU

Certifikační autority v rámci bezpečné elektronické komunikace hrají roli třetí nezávislé strany mezi odesílatelem elektronicky podepsané zprávy a příjemcem. Primární funkcí CA je vydávání certifikátů. Získání, instalaci a zálohování kvalifikovaného certifikátu u certifikační autority PostSignum ukazují následující kapitoly.

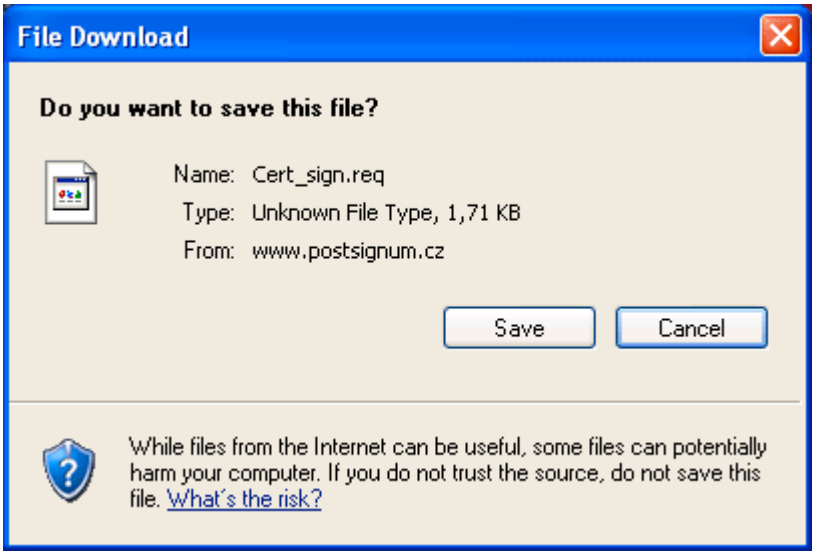
5.1 Získání certifikátu

Prvním krokem je vygenerování párů klíčů pro použití v asymetrické kryptografii a vytvoření žádosti o certifikát na webových stránkách PostSignum.



Obr. 10. Generování žádosti a certifikát. Zdroj [Vlastní zpracování]

Pro vydání certifikátu je tento soubor nutno předat pracovníkovi pobočky České pošty se službou Czech POINT [19] nebo jej zaslat mailem na podatelnu PostSignum.



Obr. 11. Uložení žádosti o certifikát. Zdroj [Vlastní zpracování]

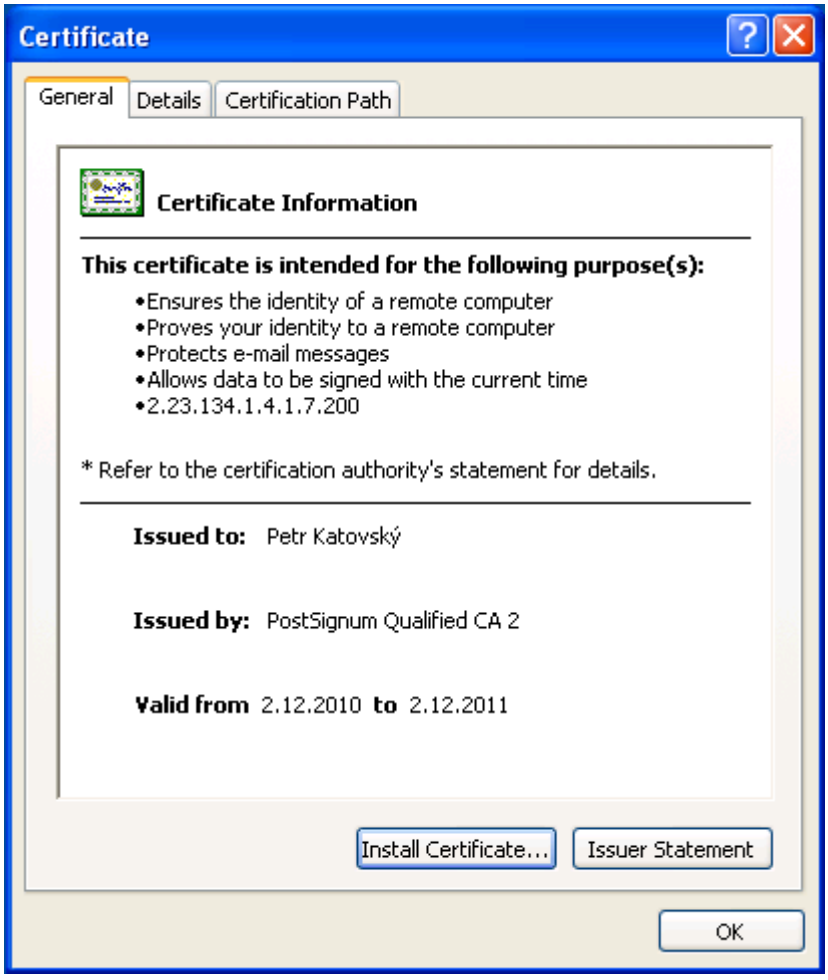
Na pobočku České pošty se službou Czech POINT je potřeba se dostavit s:

- vyplněným formulářem smlouvy (dvojí vyhotovení);
- údaji pro vydání certifikátu (zákaznický formulář);
- elektronickou žádostí o certifikát;
- dvěma osobními doklady (občanský průkaz, cestovní pas, řidičský průkaz, průkaz ZTP nebo rodný list – povinně musí být vždy předložen první nebo druhý uvedený doklad). [18]

5.2 Instalace certifikátu

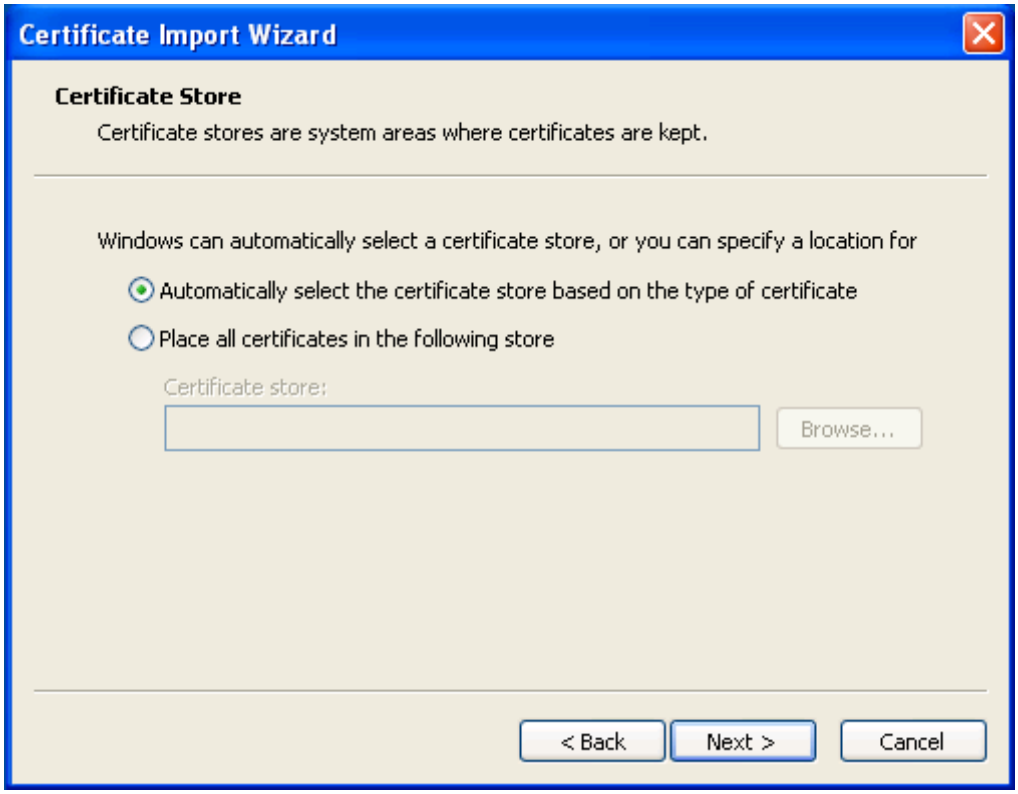
Kvalifikovaný certifikát je dle předchozí domluvy s pracovníkem České pošty vydán na přenosném médiu, je zaslán elektronickou poštou nebo je možno ho získat z webových stránek PostSignum.

Po spuštění instalace je vhodná kontrola údajů.



Obr. 12. Instalace certifikátu. Zdroj [Vlastní zpracování]

Průvodce importem certifikátu doporučuje automatický výběr úložiště.



Obr. 13. Automatický výběr úložiště. Zdroj [Vlastní zpracování]

Dokončení instalace certifikátu.

Obr. 14. Dokončení instalace.
Zdroj [Vlastní zpracování]

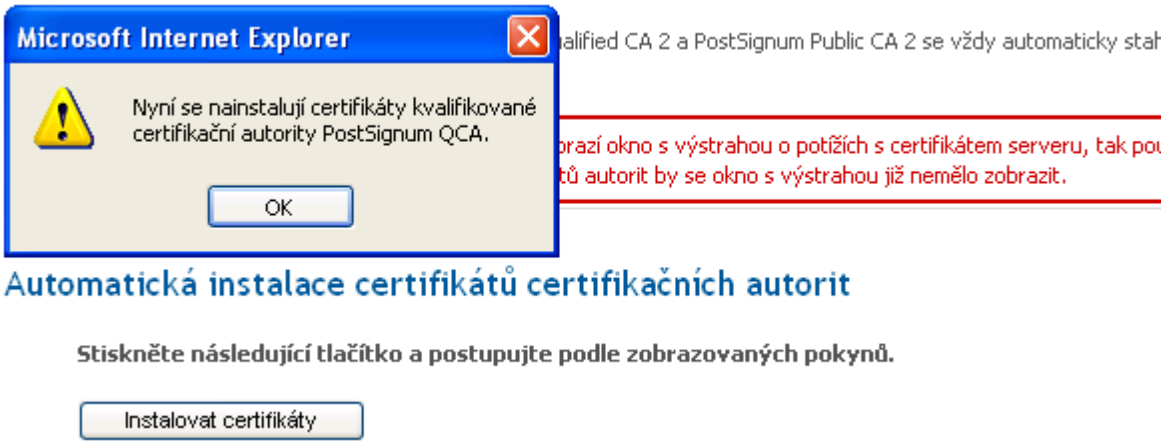
5.3 Instalace kořenového certifikátu

Pro bezproblémovou funkci aplikací (e-mail, webový prohlížeč) a aby operační systém dokázal správně vyhodnotit platnost elektronického podpisu, je nezbytné zkontrolovat instalaci kořenového certifikátu certifikační autority. Certifikáty certifikačních autorit používané v České republice bohužel nebyly až donedávna obsaženy v operačním systému Windows.

Instalací certifikátů autorit do operačního systému zajistíme důvěryhodnost používaných certifikátů. Při použití certifikátu vydaným certifikační autoritou, které důvěřujeme, pak operační systém či jiná aplikace chápe tyto certifikáty jako důvěryhodné a lze je začít využívat.

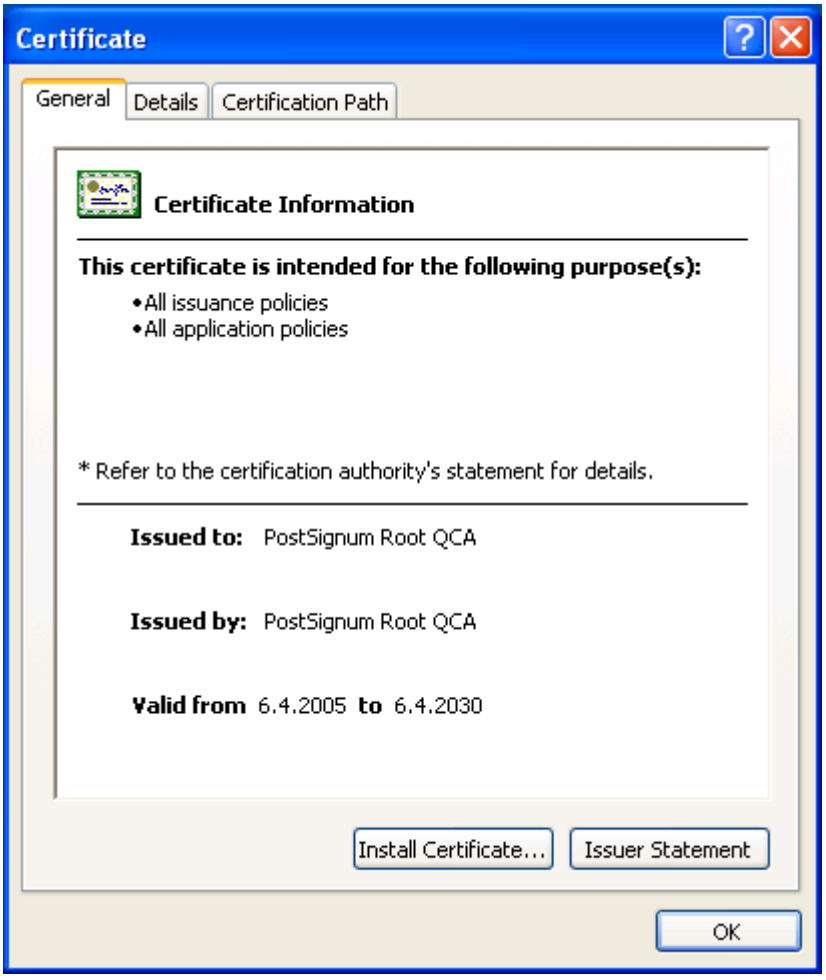
Dne 24. 5. 2010 vydal výrobce operačních systémů Windows v rámci programu Microsoft Root Certificate Program aktualizační balíček s novými kořenovými certifikáty. V balíčku je obsažen i kořenový certifikát certifikační autority České pošty PostSignum a to konkrétně tento: CN=PostSignum Root QCA 2,O=Česká pošta, s.p. [IČ 47114983],C=CZ

Chybějící kořenový certifikát se instaluje přímo z webových stránek certifikační autority PostSignum.



Obr. 15. Instalace kořenového certifikátu certifikační autority. Zdroj [Vlastní zpracování]

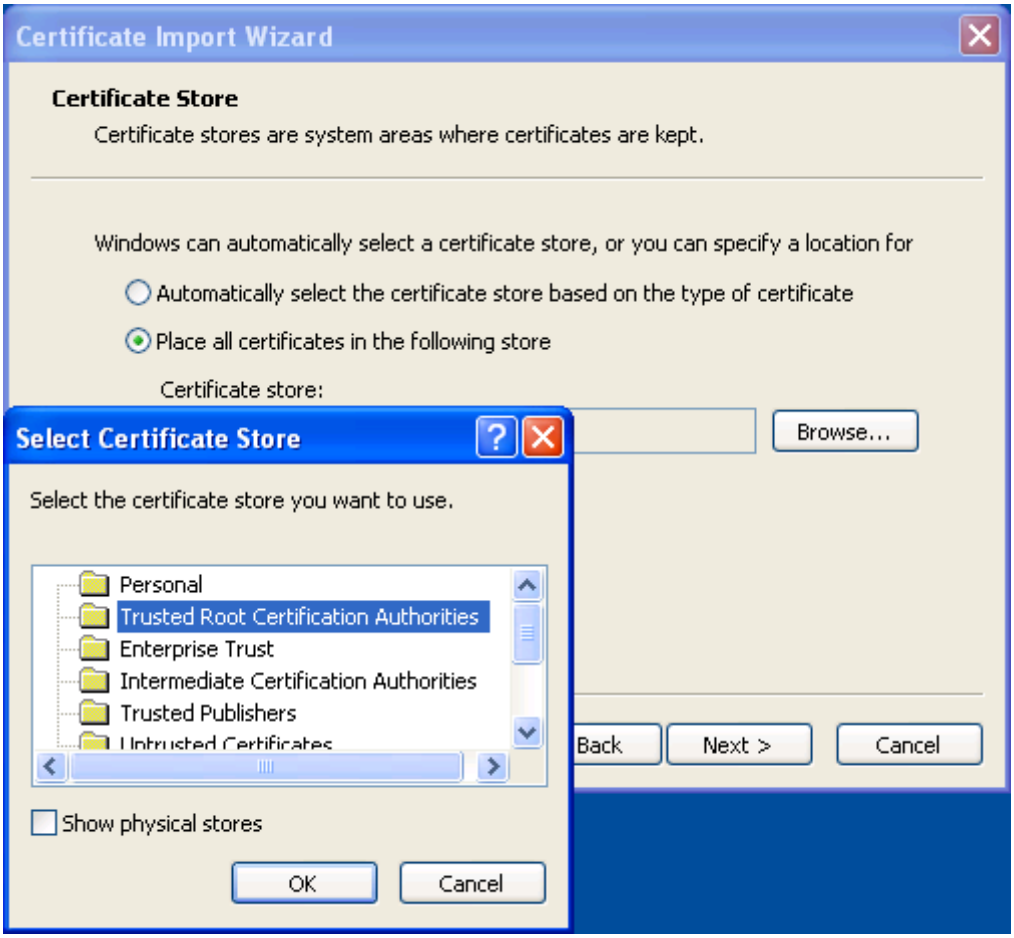
Pravost kořenového certifikátu lze ověřit dle hash (otisku) hodnoty certifikátu a podle hash hodnoty uvedené na webových stránkách PostSignum.



Obr. 16. Průběh instalace kořenového certifikátu.

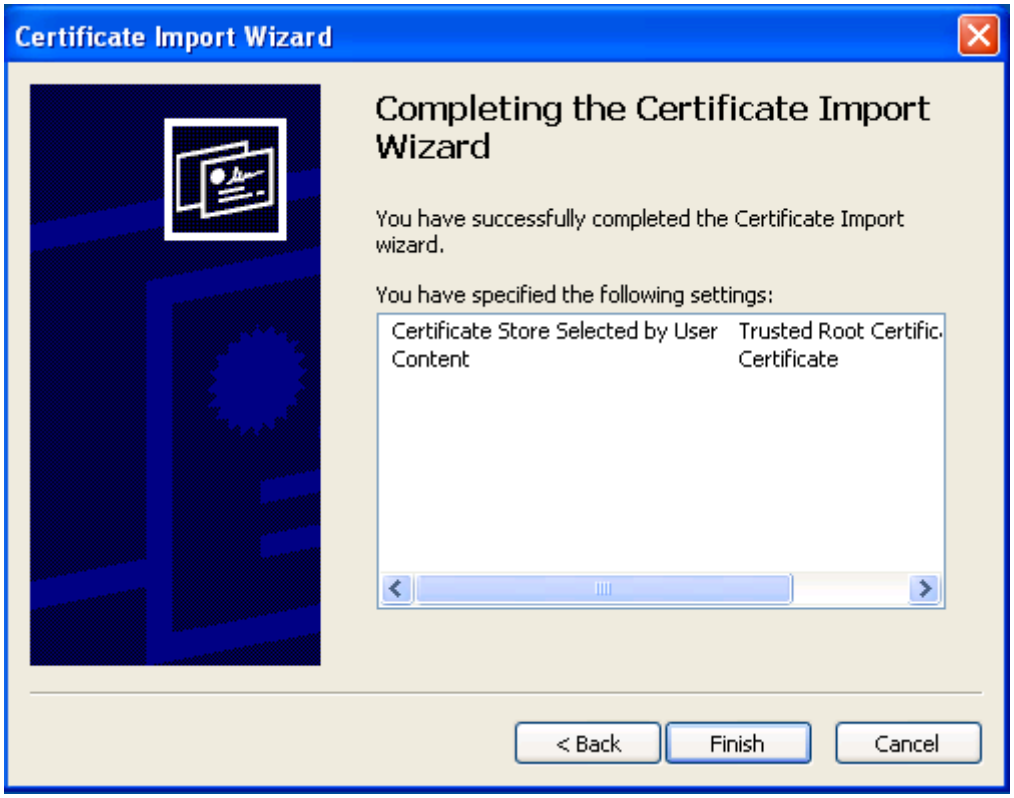
Zdroj [Vlastní zpracování]

Je nutné uložit kořenový certifikát do správného úložiště, v tomto případě mezi důvěryhodné kořenové certifikační autority.



Obr. 17. Výběr úložiště. Zdroj [Vlastní zpracování]

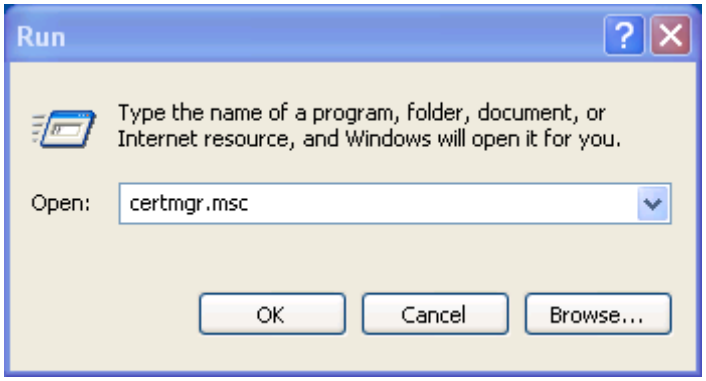
Po ukončení instalace je vhodné zkontrolovat, zda je kořenový certifikát uložen ve správném úložišti (příkaz certmgr.msc v operačním systému Windows).



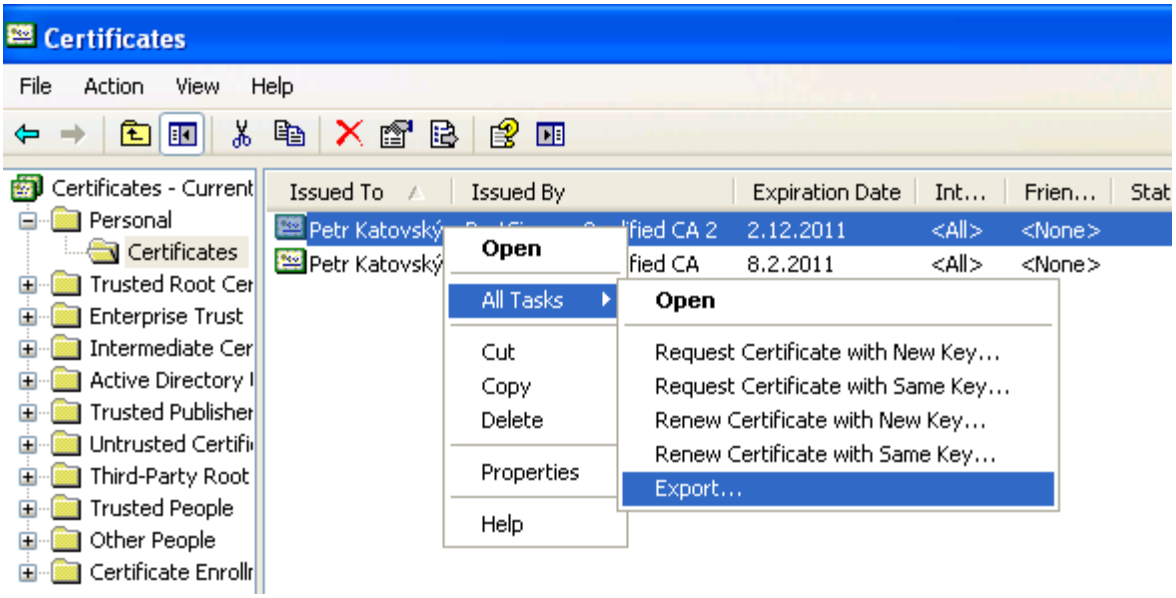
Obr. 18. Dokončení instalace kořenového certifikátu. Zdroj [Vlastní zpracování]

5.4 Zálohování soukromého klíče a certifikátu

Pro případ havárie počítače, poškození úložiště klíčů nebo potenciální ztráty soukromého klíče je vhodné vytvořit si zálohu svých citlivých dat a uložit ji na bezpečné místo. V prostředí operačního systému Windows je opět možné využít manažera certifikátů (příkaz certmgr.msc) spustitelného z příkazového řádku.

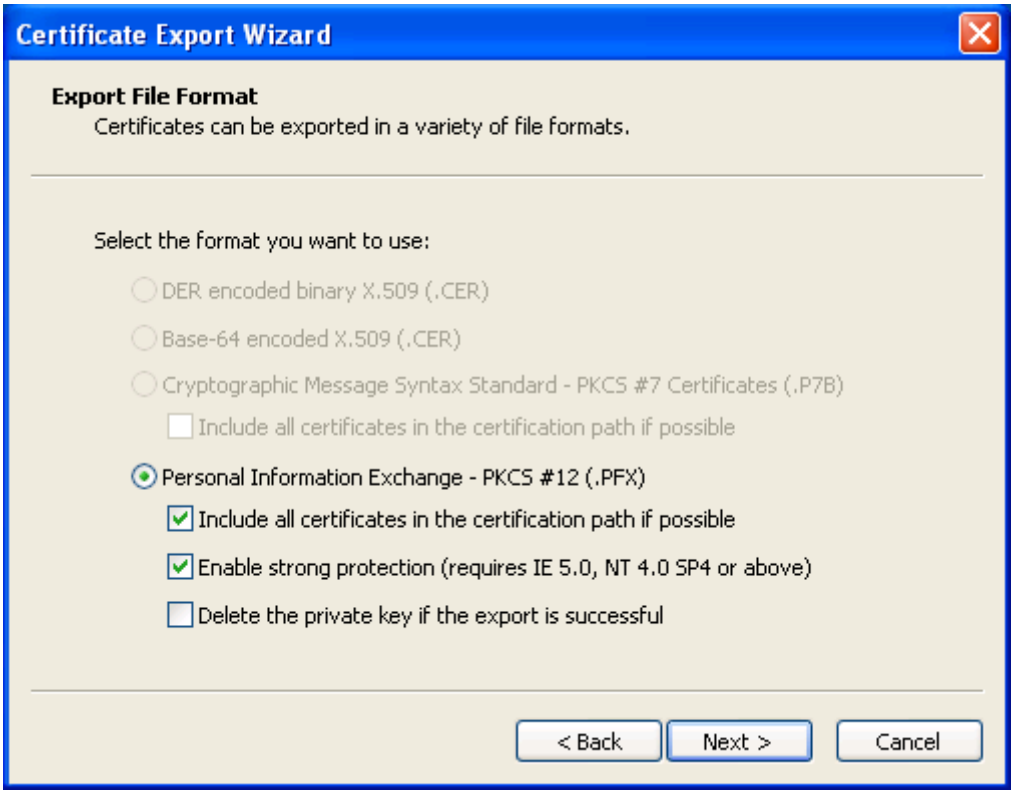


Obr. 19. Spuštění manažera certifikátů.
Zdroj [Vlastní zpracování]



Obr. 20. Export certifikátu. Zdroj [Vlastní zpracování]

Volbu formátu, ve kterém bude uložen certifikát je doporučeno ponechat na původní volbě a neměnit ji.



Obr. 21. Volba formátu certifikátu. Zdroj [Vlastní zpracování]

Heslo, kterým má být exportovaný soubor chráněn, není nutné zadat, ale ke zvýšení bezpečnosti se doporučuje. Zadané heslo musí být v obou políčkách shodné.

Obr. 22. Vložení hesla. Zdroj [Vlastní zpracování]

Pokud export certifikátu podle zadaných parametrů proběhl v pořádku, zobrazí se zpráva potvrzující úspěšný export. Soubor zálohy má příponu .pfx.

Obr. 23. Ukončení exportu. Zdroj [Vlastní zpracování]

Zálohu certifikátu je možno použít v případě havárie počítače nebo v případě přenosu klíče a certifikátu na jiný počítač. S vytvořenou zálohou je třeba zacházet s náležitou péčí, protože tato záloha by mohla být snadno zneužita.

Výše popsaný postup získání, instalace a zálohování certifikátu je s malými obměnami užíván většinou důvěryhodných certifikačních autorit v České Republice.

6 CERTIFIKAČNÍ AUTORITY V ČESKÉ REPUBLICE

Začátkem roku 2011 působí v České republice tři poskytovatelé kvalifikovaných certifikačních služeb:

1. Česká pošta, s. p. (PostSignum).
2. První certifikační autorita, a. s.
3. eIdentity a. s.

Ministerstvo vnitra zveřejňuje jejich seznam na svých webových stránkách v souladu s § 9 odst. 2, písm. e) zákona č. 227/2000 Sb. [20]

6.1 PostSignum Česká pošta, s. p.

Dne 3. září 2005 nabylo účinnosti rozhodnutí, kterým Ministerstvo informatiky udělilo České poště akreditaci k poskytování certifikačních služeb. Vedle elektronických podpisů začala Česká pošta nabízet i takzvané elektronické značky.

Akreditace Ministerstva informatiky opravňuje Českou poštu k vydávání kvalifikovaných certifikátů, které slouží k vytváření elektronického podpisu, a kvalifikovaných systémových certifikátů, které umožňují používat takzvané elektronické značky.

6.1.1 Služby

Certifikační autorita PostSignum poskytuje služby vydávání certifikátů a poskytování kvalifikovaného časového razítka. Konkrétně se jedná o služby:

1. Kvalifikovaný certifikát.
2. Komerční certifikát.
3. Kvalifikované Časové razítko.

6.1.2 Ceny

Tab. 4. Kvalifikované certifikáty Postsignum. Zdroj [18]

Certifikační politika	Cena bez DPH 20%	Cena s DPH 20%
Kvalifikované osobní certifikáty	330 Kč	396 Kč
Kvalifik. systémové certifikáty (elektr. značka)	1490 Kč	1788 Kč

Tab. 5. Komerční certifikáty Postsignum. Zdroj [18]

Certifikační politika	Cena bez DPH 20%	Cena s DPH 20%
Komerční osobní certifikáty	290 Kč	348 Kč
Komer. serverové certifikáty	667 Kč	800 Kč
Komer. šifrovací certifikáty	667 Kč	800 Kč

Tab. 6. Kvalifikovaná časová razítka PostSignum. Zdroj [18]

Vydané množství razítek za měsíc	Cena bez DPH 20%	Cena s DPH 20%
1 - 30	100 Kč	120 Kč
31 - 100	300 Kč	360 Kč
101 - 350	850 Kč	1020 Kč
351 - 1 000	2 000 Kč	2 400 Kč
1 001 - 3 500	5 000 Kč	6 000 Kč
3 501 - 10 000	12 500 Kč	15 000 Kč

10 001 - 35 000	35 000 Kč	42 000 Kč
35 001 - 100 000	75 000 Kč	90 000 Kč
100 001 - 250 000	150 000 Kč	180 000 Kč
250 001 a více	200 000 Kč	240 000 Kč

6.2 První certifikační autorita, a. s.

Certifikační autorita I.CA zahájila poskytování svých služeb v roce 1996 jako součást produktového portfolia společnosti PVT, a.s. Postupně I.CA přerostla hranice projektu, a tak byla počátkem roku 2001 založena dceřiná společnost PVT, a.s. s názvem První certifikační autorita, a.s. Tato společnost převzala od mateřské společnosti veškeré činnosti, které bezprostředně souvisí s poskytováním certifikačních služeb.

I.CA je v současnosti největším poskytovatelem komplexních služeb vydávání a správy certifikátů v České republice. Svoje služby poskytuje také na Slovensku. Pro zajištění realizace požadavků svých klientů provozuje infrastrukturu tzv. registračních autorit. Tato kontaktní pracoviště umožňují optimální dostupnost nabízených služeb.

Úřad pro ochranu osobních údajů udělil První certifikační autoritě, a.s. I.CA akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 18. 3. 2002. I.CA takto úspěšně ukončila akreditační proces a je oprávněna zahájit poskytování služeb v oblasti kvalifikovaných certifikátů.

Vydávání kvalifikovaných certifikátů určených zejména pro komunikaci v oblasti orgánů veřejné moci I.CA zahájila dne 25. 3. 2002 plně v intencích výše uvedeného zákona.

Ministerstvo informatiky ČR udělilo společnosti První certifikační autorita, a.s. rozšířenou akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu s účinností od 01. 02. 2006. Od tohoto data je I.CA oprávněna poskytovat kvalifikované certifikační služby nejen v oblasti kvalifikovaných certifikátů, ale i v oblastech kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek. [21]

6.2.1 Služby

Certifikační autorita I.CA poskytuje služby vydávání kvalifikovaných a komerčních certifikátů. Konkrétně se jedná o služby:

1. **Kvalifikovaný certifikát.** Je vhodný především pro komunikaci občanů se státní správou a samosprávou, stejně jako pro komerční aplikace.
2. **Kvalifikovaný certifikát – COMFORT.** Součástí certifikátu je čipová karta Starcos. Na tuto kartu se generují privátní klíče při tvorbě žádosti.
3. **Komerční certifikát**. Je vhodný pro použití v uzavřených systémech pro šifrování a autentizaci.
4. **Komerční certifikát – COMFORT**. Obdobné použití jako komerční certifikát. Součástí certifikátu je čipová karta Starcos.

6.2.2 Ceny

Tab. 7. Kvalifikované certifikáty I.CA. Zdroj [21]

Certifikační politika	Cena bez DPH 20%	Cena s DPH 20%
Typ Standard	395 Kč	495 Kč
Typ Comfort	984 Kč	1230 Kč

Tab. 8. Kvalifikované systémové certifikáty I.CA. Zdroj [21]

Certifikační politika	Cena bez DPH 20%	Cena s DPH 20%
Kvalifikovaný systémový certifikát - Standard	624 Kč	780 Kč
Kvalifikovaný systémový certifikát - Comfor	1212 Kč	1515 Kč

Tab. 9. Komerční certifikáty I.CA. Zdroj [21]

Certifikační politika	Cena bez DPH 20%	Cena s DPH 20%
Komerční certifikát - Standard	316 Kč	395 Kč
Komerční serverový certifikát	904 Kč	1170 Kč

6.3 eIdentity a. s.

Dne 27. 9. 2005 nabylo účinnosti rozhodnutí, kterým Ministerstvo informatiky ČR udělilo firmě eIdentity a.s. akreditaci pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Společnost eIdentity a.s. vznikla počátkem roku 2004 s orientací na komplexní služby v oblasti správy elektronické identity.

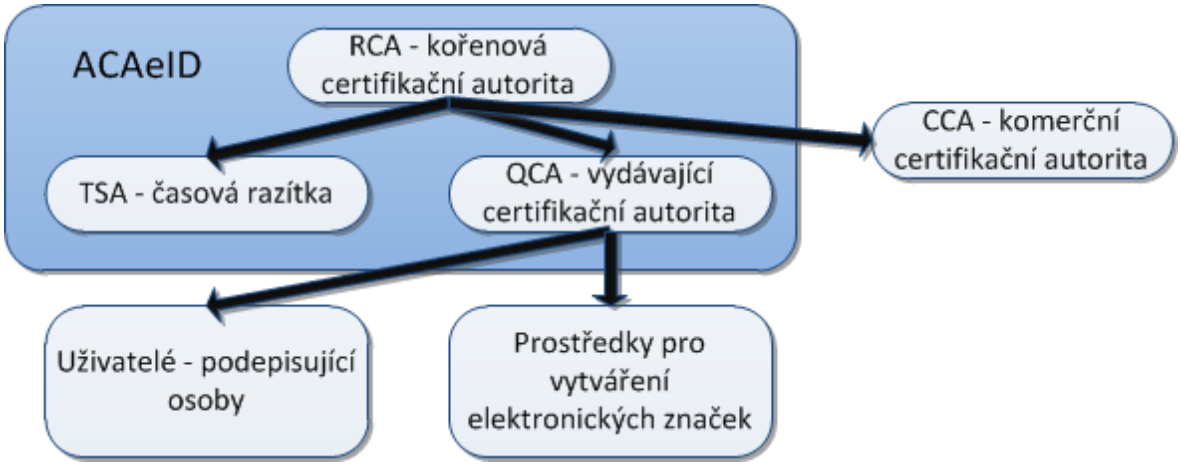
6.3.1 Služby

Jedním ze základních nabízených produktů je poskytování certifikačních služeb fyzickým a právnickým osobám i technologickým komponentám. Využití důvěryhodným způsobem vydaných elektronických certifikátů při vytváření a ověřování elektronických podpisů nebo pro účely šifrování dat umožňuje uživatelům zajistit vysokou úroveň důvěrnosti, nepopiratelnosti a integrity elektronické komunikace.

Kvalifikované certifikáty či kvalifikované systémové certifikáty vydává Akreditovaná certifikační autorita eIdentity a.s. (ACAeID). Tato certifikační autorita získala akreditaci MIČR pro výkon činnosti akreditovaného poskytovatele certifikačních služeb v souladu se zákonem 227/2000 Sb. o elektronickém podpisu a vydává kvalifikované certifikáty pro použití pouze ve spojitosti s elektronickým podpisem.

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

kvalifikovaný systémový certifikát pro autoritu vydávající kvalifikovaná časová razítka (TSA). [22]



Obr. 24. Struktura ACAeID. Zdroj [Vlastní zpracování]

Certifikační autorita ACAeID poskytuje služby vydávání časových razítek, kvalifikovaných nebo komerčních certifikátů. Konkrétně se jedná o služby:

1. Vydání kvalifikovaného certifikátu.
2. Vydání kvalifikovaného systémového certifikátu.
3. Vydání kvalifikovaného časového razítka.
4. Vydání komerčního certifikátu pro elektronický podpis.
5. Vydání komerčního certifikátu pro šifrování zpráv.
6. Vydání komerčního certifikátu pro identifikaci.

6.3.2 Ceny

Tab. 10. Kvalifikované certifikáty eIdentity. Zdroj [22]

Certifikační politika	Cena bez DPH 20%	Cena s DPH 20%
Kvalifikovaný osobní certifikát	395 Kč	474 Kč
Kvalifikovaný systémový certifikát	2 900 Kč	3480 Kč

Tab. 11. Časové razítka eIdentity. Zdroj [22]

Časové razítko	Cena bez DPH 20%	Cena s DPH 20%
V rámci obnovy či nové objednávky certifikátu (50ks)	zdarma	zdarma
Při překročení limitu jednorázový poplatek (max 1000ks	1500 Kč	1800 Kč

Tab. 12. Komerční certifikáty eIdentity. Zdroj [22]

Certifikační politika	Cena bez DPH 20%	Cena s DPH 20%
Komerční certifikát	295 Kč	254 Kč
Komerční serverový certifikát	895 Kč	1074 Kč

6.4 Porovnání certifikačních autorit

Certifikační autority lze hodnotit dle mnoha kritérií. Z hlediska běžného uživatele, který uvažuje o získání kvalifikovaného certifikátu, jsou nedůležitější tyto:

- cena certifikátu;
- rozsah služeb CA;
- důvěryhodnost CA.

Rozsah služeb CA, druhy vydávaných certifikátu, ceny certifikátů a důvěryhodnost CA jsou zpracovány v následujícím přehledu.

Tab. 13. Porovnání služeb a certifikátů certifikačních autorit. Zdroj [Vlastní zpracování]

	Cerifikační autority		
Služby	PostSignum	I.CA.	eIdentity
Kvalifikovaný osobní certifikát	✓	✓	✓
Kvalifikovaný systémový certifikát	✓	✓	✓
Komerční osobní certifikát	✓	✓	✓
Komerční serverový certifikát	✓	✓	✓
CRL	✓	✓	✓
Zneplatnění certifikátu	✓	✓	✓
Časová razítka	✓	✓	✓
Testovací certifikát	✓	✓	☐

Tab. 14. Porovnání cen certifikačních autorit s DPH. Zdroj [Vlastní zpracování]

	Cerifikační autority		
Služby	PostSignum	I.CA.	eIdentity
Kvalifikovaný osobní certifikát	396 Kč	495 Kč	474 Kč
Kvalifikovaný systémový certifikát	1788 kč	780 Kč	3480 Kč
Komerční osobní certifikát	348 Kč	395 Kč	254 Kč
Komerční serverový certifikát	800 Kč	1170 Kč	1074 Kč
Zneplatnění certifikátu	zdarma	zdarma	zdarma
Testovací certifikát	zdarma	zdarma	☐

6.4.1 Vyhodnocení certifikačních autorit

Z porovnání **cen certifikátů** jednotlivých autorit vyplývá, že z hlediska získání kvalifikovaného osobního certifikátu je nejvýhodnější nabídka České pošty PostSignum. Cena je sice výrazně vyšší, než notářské ověření podpisu, což je ale kompenzováno faktem, že s pomocí kvalifikovaného osobního certifikátu je možné podepsat neomezené množství dokumentů nebo zpráv.

Rozsah služeb a **druhy vydávaných certifikátů** CA jsou v současné době téměř na stejné úrovni. Všechny certifikační autority vydávají všechny typy běžných certifikátů, časová razítka a pravidelně vydávají seznamy zneplatněných certifikátů (CRL). Testovací certifikát nevydává pouze autorita eIdentity.

Pro stanovení **důvěryhodnosti** jednotlivých CA není jednoduché stanovit jednoznačná kritéria. Základem je návštěva webových stránek CA a prostudování všech informací, které

jsou zde zveřejněny. Podrobné informace (certifikační politika, dostupnost certifikační autority, rozsah a kvalita nápovědy, technická podpora, podmínky publikování CRL, formáty vydávaných certifikátů) jsou podány a zpracovány přehledně u všech CA. Také vzhledem k tomu, že se jedná o známé společnosti působící na našem trhu poměrně dlouhou dobu, lze porovnávané certifikační autority označit za důvěryhodné.

Závěrem lze říci, že výběr certifikační autority pro získání kvalifikovaného certifikátu je spíše individuální záležitostí, dle osobních preferencí každého uživatele. Doporučit lze všechny tři certifikované a akreditované autority v České republice.

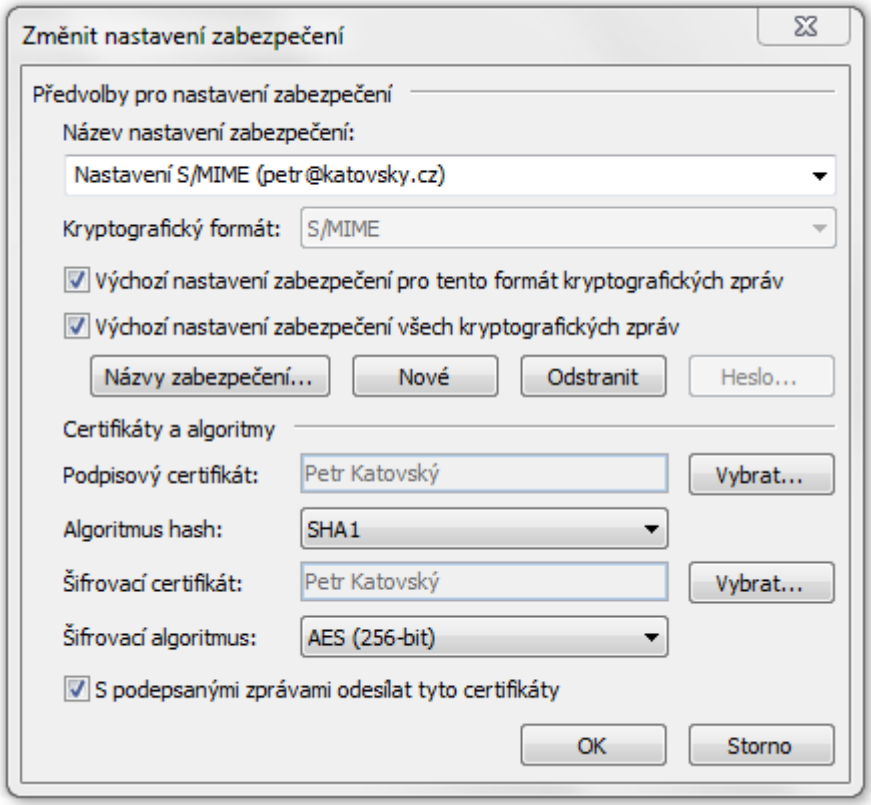
7 ELEKTRONICKÁ KOMUNIKACE V PRAXI

Elektronický podpis má široké možnosti využití. Z pohledu běžného uživatele elektronické komunikace, je využití elektronického podpisu spojeno téměř výhradně se základními komunikačními nástroji, jako je elektronická pošta a webovými servery přístupnými pomocí internetového prohlížeče. Pomocí těchto nástrojů může uživatel využívat zabezpečenou a důvěryhodnou komunikaci přes nechráněné sítě jako je Internet.

Základy architektury bezpečné pošty byly položeny v polovině 70. let. Standardem pro předávání zpráv prostřednictvím elektronické pošty je protokol MIME (Multipurpose Internet Mail Extensions) definovaný v RFC-822 a RFC-822. Pro bezpečnou elektronickou poštu je využívána bezpečná (Secure) verze tohoto protokolu, která se označuje jako S/MIME. S/MIME je definován v RFC-2632 až RFC-2634. Protokol S/MIME podporuje řadu kryptografických funkcí (hash, symetrická a asymetrická kryptografie), využívá certifikáty a umožňuje zasílat podepsaná a zašifrovaná data. Nastavení a použití kvalifikovaného certifikátu v aplikaci Outlook 2010 ukazují následující kapitoly.

7.1 Nastavení certifikátu

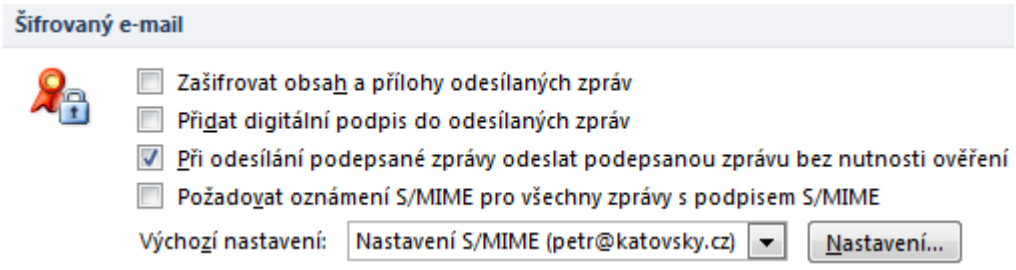
V certifikátu musí být dle standardu S/MIME uvedena emailové adresa. Poštovní klienti kontrolují odesilatele i příjemce zprávy na shodu adresy uvedené v certifikátu a ve zprávě. K nastavení požadované úrovně zabezpečení slouží v aplikaci Outlook 2010 Centrum zabezpečení.



Obr. 25. Nastavení zabezpečení a certifikátu v Outlook 2010.

Zdroj [Vlastní zpracování]

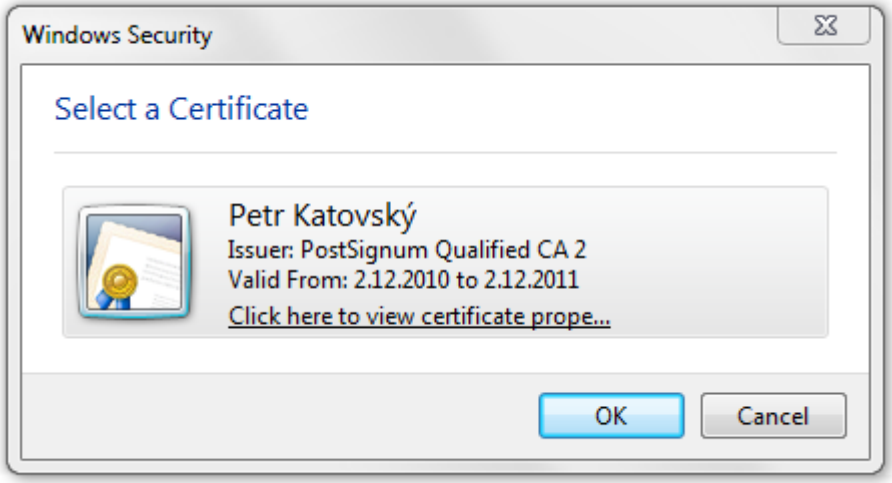
Podrobnější nastavení například umožňuje přidat elektronický podpis automaticky do všech odesílaných zpráv.



Obr. 26. Podrobnější nastavení v Outlook 2010.

Zdroj [Vlastní zpracování]

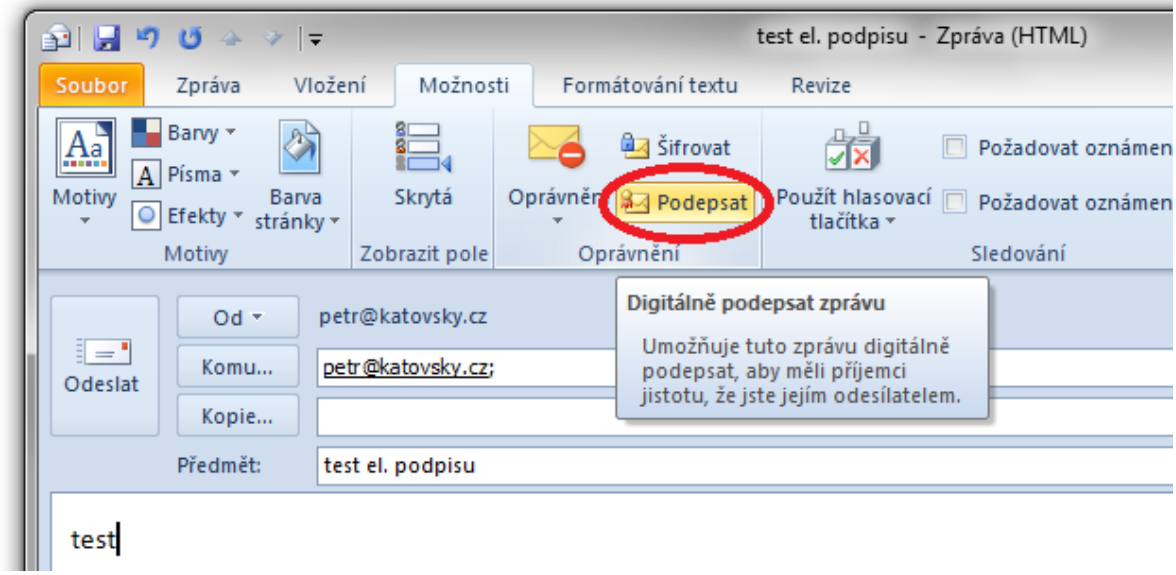
V případě, kdy je k dispozici více certifikátů je nutné vybrat jeden jako výchozí.



Obr. 27. Výběr výchozího certifikátu. Zdroj [Vlastní zpracování]

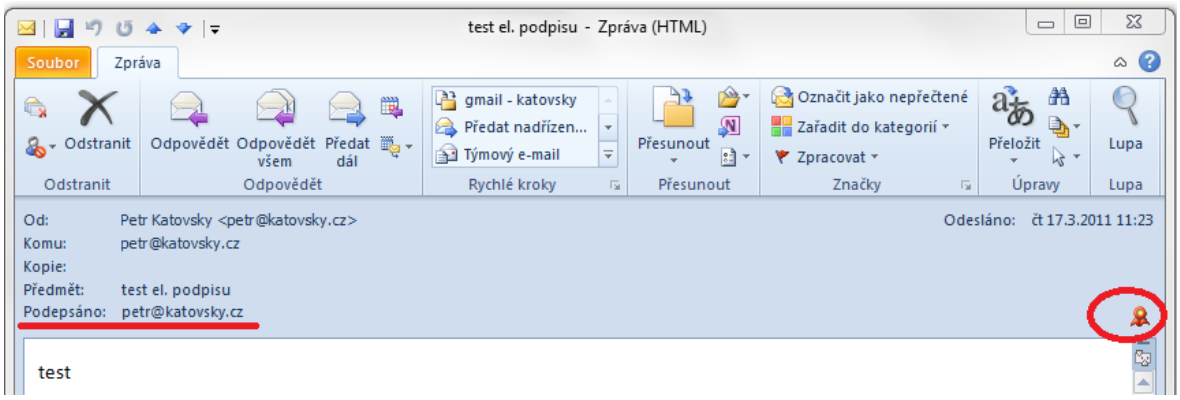
7.2 Použití certifikátu

Odeslání zprávy opatřené elektronickým podpisem je stejně jednoduché jako jakékoliv jiné zprávy. Při tvoření nové zprávy lze v menu označit, zda má být zpráva elektronicky podepsána. V zásadě tak jsou k dispozici dvě možnosti. Podepisovat veškerou odesílanou poštu automaticky nebo se při odesílání každé zprávy rozhodnout a podepsat zprávu manuálně použitím příslušné ikony.



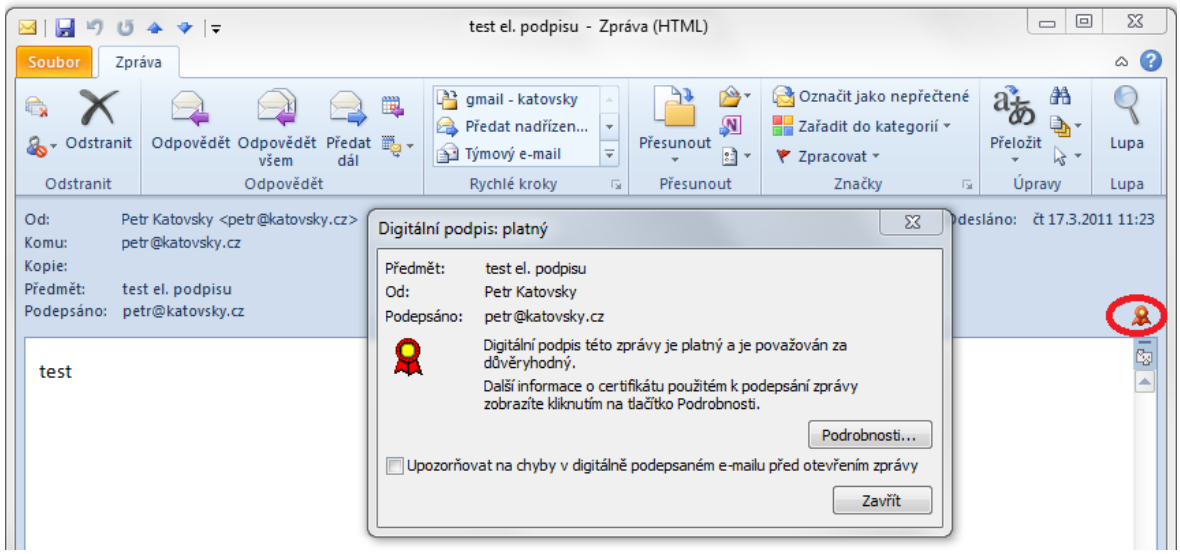
Obr. 28. Podepsání zprávy. Zdroj [Vlastní zpracování]

Příjemce zprávy obdrží podepsaný e-mail stejným způsobem jako kteroukoliv jinou zprávu. Podepsaná zpráva je v případě aplikace Outlook 2010 zobrazena specifickou ikonou.



Obr. 29. Přijatá podepsaná zpráva. Zdroj [Vlastní zpracování]

Pokud má příjemce zájem o detailnější informace o parametrech zabezpečení, kliknutím na ikonu získá další informace o bezpečnostních atributech zprávy. Tyto podrobnější informace sdělují, že elektronický podpis je platný a je považován za důvěryhodný. V podrobnostech elektronického podpisu je zároveň možné získat informace o důvěryhodné certifikační autoritě nebo o certifikátu odesilatele.



Obr. 30. Zobrazení podrobností digitálního podpisu. Zdroj [Vlastní zpracování]

Je zřejmé, že odeslání a příjem elektronicky podepsané zprávy není nic složitého. Velkou roli v celém procesu hrají moderní emailové programy jako Outlook 2010 s uživatelsky přívětivým ovládáním, které jsou na celý proces náležitě připraveny.

.

ZÁVĚR

Elektronický podpis ušel za svou historii už poměrně dlouhou cestu. Pro uživatele, orientujícího se v procedurách spojených s elektronickým podpisem je zpravidla užívání elektronického podpisu jednoduchou záležitostí. Ve spojení s vhodnou aplikací přináší mnoho výhod a zjednodušení. Celá diplomová práce je zpracována s cílem podat zevrubný přehled problematiky elektronického podpisu právě pro ty uživatele, kteří se ještě z nějakého důvodu s tímto tématem nesetkali.

První kapitola obsahuje seznámení s elektronickým podpisem a výklad klíčových pojmů.

Druhá kapitola se zabývá technologickými aspekty elektronického podpisu. Vysvětluje kryptografii založenou na symetrickém a asymetrickém podpisu, hash funkci a princip elektronicky podepsané a zašifrované zprávy.

Certifikační autority a certifikáty jsou obsahem třetí kapitoly. Kapitola popisuje druhy certifikátů, princip fungování certifikačních autorit a časová razítka.

Legislativou a aktuálním stavem využití elektronického podpisu se zaobírá čtvrtá kapitola. Je rozebrána legislativa a směrnice v EU, standardizace elektronického podpisu a zákon o elektronickém podpisu v ČR.

Praktická část diplomové práce se v kapitole pět věnuje získání a instalaci kvalifikovaného certifikátu, instalaci kořenového certifikátu a zálohování soukromého klíče.

Praktická část dále pokračuje kapitolou šest, která analyzuje certifikační autority v České republice z hlediska nabídky jejich služeb a cen.

Kapitola sedm popisuje elektronickou komunikaci v praxi v podobě nastavení a použití kvalifikovaného certifikátu v aplikaci Outlook 2010.

Hlavní přínos této práce spočívá ve vytvoření výukové pomůcky do předmětu Kriminalistické technologie a systémy, podloženou studiem odborné literatury, standardů a legislativy. V praktické části práce je možné si projít celým procesem výběru certifikační autority, získání certifikátu a podepsání elektronické zprávy. V neposlední řadě mohou tuto diplomovou práci využít všichni zájemci, kteří potřebují dobře porozumět legislativě a procesům elektronického podpisu.

ZÁVĚR V ANGLIČTINĚ

The electronic signature has covered quite a long way during its history. For users who is well informed about procedures concerning electronic signature is usually very easy to use the electronic signature. In connection with a proper application it brings many advantages and simplifications. Entire diploma work is processed with the goal to give a general review of the electronic signature topic for those users who, for some reason, have never dealt with this topic.

First chapter contains electronic signature identification and explanation of key words.

Technological aspects of electronic signature are described in the second chapter. This chapter also explains kryptography based on symetric and asymetric signature, hash function and principle of electronicly signed and coded message.

Certification authorities and certificates are contained in the third chapter. There are descriptions of various sorts of certificates, processing principles of certification authorities and time stamps.

Legislature and present status of using the electronic signature is shown in the fourth chapter. This chapter is engaged in the European legislature and procedures, electronic signature standardization and the electronic signature act in the Czech Republic.

Operative part of the diploma work – in ist fifth chapter - concerns to ways of acquirement and instalation of an competent certificate, root certificate instalation and private key backup procedures.

Certification authorities in the Czech Republic are analysed in the sixth chapter considering service and price offer range.

Electronic communication in use, which means setting up and using the competent certificate in Outlook 2010 programme.

The main contribution of this work lies in creating an educational tool for the subject Criminalistic Technology And Systems, which has to be supported by research of professional literature, standards and legislature. In the operation part of the work it is possible to go though the entire process of certification authority selection, obtaining the certificate and signing the electronic message.

This diploma work could be also useful for those, who need to understand the legislature and the electronic signature procedures.

SEZNAM POUŽITÉ LITERATURY

[1] DOSTÁLEK, Libor. VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 1. vyd. Brno: Computer Press, 2006. 536 s. ISBN: 80-251-0828-7.

[2] BOSÁKOVÁ, Dagmar. KUČEROVÁ, Alena. PECA, Jaroslav. VONDRUŠKA, Pavel. Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů. 2. vyd. Olomouc: ANAG, 2004. 141 s. ISBN 80-7263-125-X.

[3] BUDIŠ, Petr. Elektronický podpis a jeho aplikace v praxi. 1. vyd. Olomouc: ANAG, 2008. 160 s. ISBN 978-80-7263-465-1.

[4] KATZ, Jonathan. Digital Signatures. 1st ed. London: Springer, 2010. 183 s. ISBN 978-0-387-27711-0.

[5] ŠTĚDROŇ, Bohumír. E-justice. 1. vyd. Praha: Linde, 2008. 272 s. ISBN 978-80-7201-714-0.

[6] LIDINSKÝ, Vít. ŠVARCOVÁ, Ivana. BUDIŠ, Petr. LOEBL, Zbyněk. PROCHÁZKOVÁ, Barbora. eGovernment bezpečně. 1. vyd. Praha: GRADA, 160 s. ISBN 978-80-247-2462-1.

[7] Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu [online]. [cit. 2011-02-21]. Dostupný z WWW: <http://www.mvcr.cz/soubor/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmum-v-oblasti-elektronickeho-podpisu.aspx>.

[8] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms [online]. [cit. 2011-02-21]. Dostupný z WWW: <http://pda.etsi.org/exchangefolder /ts_10217601v020000p.pdf>.

[9] zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování [online]. [cit. 2011-02-5]. Dostupný z WWW: <http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=cs>.

[10] Směrnice evropského parlamentu a rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy [online]. [cit. 2011-02-14]. Dostupný z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:CS:PDF>.

[11] Zákon č.486/2004 Sb. (227/2000 Sb.): Úplné znění zákona č. 227/2000 Sb. O elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn [online]. [cit. 2011-02-11]. Dostupný z: <http://www.crypto-world.info/pravo/podpis/pravo/486_04.htm>.

[12] UNCITRAL [online]. [cit. 2011-02-14]. Dostupný z: <http://www.uncitral.org>.

[13] Komise OSN pro mezinárodní obchodní právo UNCITRAL [online]. [cit. 2011-02-14]. Dostupný z: <http://www.mpo.cz/dokument6470.html>.

[14] Elektronické podpisy a Evropská Unie [online]. [cit. 2011-02-14]. Dostupný z: <http://crypto-world.info/pinkava/clanky/zep_dsm.pdf>.

[15] The legal and market aspects of electronic signatures [online]. [cit. 2011-03-2]. Dostupný z: <http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report>.

[16] Úplné znění zákona č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů [online]. [cit. 2011-02-14]. Dostupný z: <http://www.mvcr.cz/soubor/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx>.

[17] Vyhláška č. 378/2006 Sb. o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na

ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb) [online]. [cit. 2011-02-14]. Dostupný z: <http://www.mvcr.cz/soubor/vyhlaska-c-378-2006-sb-o-postupech-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb.aspx>.

[18] Webové stránky PostSignum [online]. Dostupné z: <http://www.postsignum.cz>.

[19] Webové stránky Czech POINT [online]. Dostupný z: <http://www.czechpoint.cz/web/index.php>.

[20] Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb [online]. [cit. 2011-03-10]. Dostupný z: <http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>.

[21] První certifikační autorita, a.s. [online]. [cit. 2011-03-15]. Dostupný z: <http://www.ica.cz/cz/menu/1/obecne-informace/>.

[22] eIdentity a.s. [online]. [cit. 2011-03-16]. Dostupný z: <https://www.eidentity.cz/ServicesDescription.html>.

[23] Poskytovatelia akreditovanej certifikačnej služby správy kvalifikovaných certifikátov [online]. [cit. 2011-03-21]. Dostupný z: <http://www.nbusr.sk/sk/elektronicky-podpis/zoznam-aca/aca-spravy-kvalifikovanych-certifikatov/index.html>.

[24] Přehled udělených akreditací [online]. [cit. 2011-03-21]. Dostupný z: <http://aplikace.mvcr.cz/archiv2008/micr/scripts/detail.php_id_603.html>.

[25] Jak si vybrat certifikační autoritu [online]. [cit. 2011-03-22]. Dostupný z: <http://crypto-world.info/bridge/dokumenty/jak_vybrat_ca.pdf>.

[26] Změna v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu [online]. [cit. 2011-03-22]. Dostupný z: <http://www.mvcr.cz/clanek/zmena-v-kryptografickych-algoritmech-ktere-jsou-pouzivany-pro-vytvareni-elektronickeho-podpisu.aspx>.

[27] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy - s barevným vyznačením posledních změn [online]. [cit. 2011-04-1]. Dostupný z:

<http://www.mvcr.cz/soubor/zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy-s-barevnym-vyznacenim-zmen-provedenych-zakonem-c-190-2009-sb.aspx>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3DES	Typ algoritmu (Triple – DES).
ACAeID	Akreditovaná certifikační autorita eIdentity a.s.
AES	Typ algoritmu.
ALGO	Algorithms and Parameters for Secure Electronic Signatures.
a.s	Akciová společnost.
CA	Certifikační autorita.
CCA	Komerční Certifikační autorita.
CD	Kompaktní disk.
CRL	Seznam zneplatněných certifikátů.
ČR	Česká republika.
DES	Typ algoritmu.
DPH	Daň z přidané hodnoty.
DH	Diffie-Hellmanův algoritmus.
DSA	Digital Signature Algorithm.
ECC	Error Checking and Correcting
ETSI	Evropský ústav pro telekomunikační normy.
ES	Evropská unie.
EU	Evropská unie.
FESA	Forum of European Supervisory Authorities for Electronic Signatures.
I.SA	Registrační autorita.
IDEA	International Data Encryption Algorithm.
MD5	Message Digest 5.
MIME	Multipurpose Internet Mail Extensions.
NBÚ	Národný bezpečnostný úrad.

NTP	Network time protocol.
PVT	Soukromá společnost.
QCA	Kvalifikovaná certifikační autorita.
RC2	Typ algoritmu.
RC4	Typ algoritmu.
RFC	Request for comment.
SHA-1	Typ algoritmu.
SHA-2	Typ algoritmu.
SHA-224	Typ algoritmu.
SHA-256	Typ algoritmu.
SHA-384	Typ algoritmu.
SHA-512	Typ algoritmu.
S/MIME	Secure/Multipurpose Internet Mail Extensions.
SR	Slovenská republika.
TSA	Timestamp authority.
URL	Uniform Resource Locator.
WWW	World Wibe Web.
ZTP	Průkaz mimořádných výhod.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PŘEHLED KVALIFIKOVANÝCH POSKYTOVATELŮ CERTIFIKAČNÍCH SLUŽEB A JEJICH KVALIFIKOVANÝCH SLUŽEB

Ministerstvo vnitra zveřejňuje v souladu s § 9 odst. 2, písm. e) zákona č. 227/2000 Sb. [20]

Poř. číslo	Poskytovatelé certifikačních služeb	Kvalifikované služby	Zahájení vydávání
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	03/2002 02/2006 02/2006
2.	Česká pošta, s. p., identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	09/2005 04/2005 07/2009
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	Vydávání kvalifikovaných certifikátů; Vydávání kvalifikovaných systémových certifikátů; Vydávání kvalifikovaných časových razítek.	08/2005 08/2005 08/2010

PŘÍLOHA P II: PŘEHLED UDĚLENÝCH AKREDITACÍ

Ministerstvo vnitra zveřejňuje v souladu s § 9 odst. 2 písm. e) zákona č. 227/2000 Sb.

Ministerstvo vnitra udělilo akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb v tabulce uvedeným subjektům na základě:

- splnění všech podmínek předepsaných zákonem v souladu s § 10 odst. 4 zákona č. 227/2000 Sb., (zákon o elektronickém podpisu);
- splnění podmínek, požadavků a postupů stanovených vyhláškou č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb);
- ověření kvalifikovaných systémových certifikátů Ministerstvem vnitra podle § 9 odst. 2 písm. d) zákona o elektronickém podpisu. [24]

Poř. číslo	Udělena akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb	Akreditace udělena
1.	První certifikační autorita, a. s., identifikační číslo 26 43 93 95, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	15.3.2002
2.	Česká pošta, s. p. identifikační číslo 47 11 49 83, Olšanská 38/9, PSČ 225 99 Praha 3	15.7.2005
3.	eIdentity a. s., identifikační číslo 27 11 24 89, Vinohradská 184/2396, PSČ 130 00 Praha 3	12.9.2005

Aktualizace ke dni 21.5.2010

PŘÍLOHA P III: ZMĚNA V KRYPTOGRAFICKÝCH ALGORITMECH, KTERÉ JSOU POUŽÍVÁNY PRO VYTVÁŘENÍ ELEKTRONICKÉHO PODPISU

Na základě aktuálních poznatků v oblasti kryptografie a dokumentu ETSI TS 102 176-1 V2.0.0 (ALGO Paper) Ministerstvo vnitra stanoví:

Kvalifikovaní poskytovatelé certifikačních služeb ukončí vydávání kvalifikovaných certifikátů s algoritmem SHA-1 do 31. 12. 2009. Od 1. 1. 2010 budou tito poskytovatelé vydávat kvalifikované certifikáty podporující některý z algoritmů SHA-2.

Zároveň je od uvedeného data stanovena minimální přípustná délka kryptografického klíče pro algoritmus RSA na 2048 bitů.

Komentář ke změně v kryptografických algoritmech, které jsou používány pro vytváření elektronického podpisu.

Ministerstvo vnitra podle vyhlášky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, zveřejňuje kryptografické algoritmy a jejich parametry, které mohou být použity pro elektronický podpis ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu. Ministerstvo vnitra při stanovení zveřejňovaných algoritmů a jejich parametrů vychází jednak z dokumentů vydaných z iniciativy Evropské komise organizacemi, které k tomu EK určila (tzv. ALGO paper zveřejňovaný ETSI), a dále z aktuálního vývoje v oblasti bezpečnosti kryptografických algoritmů. V úvahu bere zároveň stanoviska významných mimoevropských institucí (např. NIST v USA) a českého Národního bezpečnostního úřadu.

V návaznosti na směrnici ES č. 1999/93/EC o zásadách Společenství pro elektronické podpisy a v ní obsažený princip vzájemného uznávání kvalifikovaných certifikátů vydaných v kterémkoliv členském státu EU je nezbytné vycházet z dokumentu ALGO paper, který stanoví, že od 1. 1. 2010 je algoritmus SHA-1 „unusable“ a je tedy nezbytné ukončit jeho používání pro oblast elektronického podpisu a zahájit přechod na bezpečnější algoritmy třídy SHA-2. Česká republika patří k těm členským státům, ve kterých je tento

přechod rozložen do delšího časového období. Je však nezbytné jej realizovat, a tak zachovat důvěru uživatelů v bezpečnost elektronického podpisu.

V případě SHA-2 se jedná o tzv. rodinu čtyř hashovacích funkcí (SHA-224, SHA-256, SHA-384 a SHA-512), které jsou součástí standardu FIPS PUB 180-2 a u kterých dosud nebyly nalezeny bezpečnostní slabiny.

Je nesporné, že tento přechod bude náročný nejen pro poskytovatele certifikačních služeb, kteří vydávají kvalifikované certifikáty, ale i pro tvůrce a provozovatele aplikací, ve kterých je elektronický podpis využíván. V praxi tato změna znamená, že:

- poskytovatelé certifikačních služeb přestanou vydávat kvalifikované certifikáty s algoritmem SHA-1 nejpozději do 31. 12. 2009;
- poskytovatelé certifikačních služeb zahájí vydávání kvalifikovaných certifikátů s hashovací funkcí třídy SHA-2 nejpozději 1. 1. 2010 (mohou tak však učinit kdykoliv dříve); tato změna se samozřejmě týká i vydávání kořenových certifikátů, kterými poskytovatel certifikačních služeb označuje jím vydané certifikáty;
- aplikace, ve kterých je elektronický podpis používán, musí podporovat nejpozději od 1. 1. 2010 všechny algoritmy třídy SHA-2;
- podpora algoritmu SHA-1 musí být v aplikacích zachována minimálně do 31. 12. 2010.

Obecně lze konstatovat, že se nejedná o nepředvídatelnou změnu. Naopak tato problematika je již několik let diskutována a byla publikována řada odborných článků a studií. Kryptografické algoritmy stejně jako jiné prvky související s informační bezpečností nejsou schopné v delším časovém horizontu odolat nejrůznějším útokům a nelze na ně plně spoléhat. Pokud jde konkrétně o algoritmy, prolomen byl dříve oblíbený algoritmus MD5 (již od roku 2004 je veřejně znám postup pro nalezení kolizního páru zpráv – tj. dvou různých zpráv se stejným hashem). Necelý rok poté byl pro SHA-1 zveřejněn objev algoritmu, který umožňuje nalézt kolizi podstatně rychleji než hrubou silou. Výpočetní náročnost s ohledem na současnou techniku je sice předmětem diskusí mezi odborníky, použití tohoto algoritmu pro elektronický podpis však nelze považovat za bezproblémové (nelze například vyloučit, že i pro tento algoritmus bude nalezen způsob generování kolizních zpráv).

Ministerstvo vnitra konzultuje uvedené změny s poskytovateli certifikačních služeb, kteří vydávají kvalifikované certifikáty (tj. Česká pošta s.p., eIdentity a.s., První certifikační autorita a.s.). Ti ve svých plánech rozvoje s přechodem na nové algoritmy počítají. Tvůrcům aplikací lze doporučit, aby případně úpravy s poskytovateli podle potřeby konzultovali.

Ministerstvo vnitra je oprávněno tuto změnu vyhlásit pouze pro oblast elektronického podpisu, avšak i pro jiné oblasti využití důrazně doporučuje, aby odpovědné osoby zvážily rizika spojená s dalším používáním hashovací funkce SHA-1. [26]

Aktualizováno dne 23. 6. 2009