



Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

ELEKTRONICKÝ PODPIS PRÁVNÝ A TECHNOLOGICKÝ POHĽAD

Diplomová práca

Autor: Martin Rublák
Vedúci: doc. RNDr. Daniel Olejár PhD.

Bratislava
apríl 2005

Čestne prehlasujem, že som túto diplomovú prácu vypracoval samostatne s použitím citovaných zdrojov.

Pod'akovanie

Chcel by som poďakovať doc. RNDr. Danielovi Olejárovi PhD. za cenné pripomienky pri písaní tejto práce.

Ďalej by som chcel poďakovať všetkým učiteľom, stredoškolským a vysokoškolským profesorom a ľuďom, ktorí mi umožnili študovať a pomáhali mi pri štúdiu.

A samozrejme rodičom a priateľom ktorí mi boli veľkou oporou.

Obsah

1 Úvod	3
2 História	5
2.1 História elektronického podpisu a asymetrickej kryptografie . .	5
2.2 Popis štandardov	6
2.3 Legislatívne riešenie elektronického podpisu	9
3 Základy kryptológie a podstaty elektronického podpisu	12
3.1 Úvod	12
3.2 Základné pojmy kryptografie	15
3.2.1 Model bezpečnosti šifrových systémov a spôsoby úto- kov na šifrovacie algoritmy	17
3.2.2 Symetrická kryptografia	19
3.2.3 Asymetrická kryptografia	20
3.2.4 Úloha kľúčov pri šifrovaní	23
3.3 Digitálny podpis	25
3.3.1 Atribúty vlastnoručného podpisu	25
3.3.2 Realizácia digitálnych podpisov	27
3.3.3 Porovnanie klasického a digitálneho podpisu	31
4 Teória a prax digitálneho podpisu	34
4.1 Administratívne problémy digitálnych podpisov	34
4.2 Infraštruktúra verejných kľúčov	34
4.2.1 Základné pojmy PKI	35
4.2.2 Úlohy certifikačnej authority	42
4.2.3 Model PKI	47
5 Legislatíva upravujúca elektronický podpis	52
5.1 Direktíva európskej únie o elektronickom podpise a Vzorový zákon UNCITRAL o elektronickom podpise	52
5.2 Vzorový zákon UNCITRAL o elektronickom podpise	53

5.2.1	Účel a história Vzorového zákona	53
5.2.2	Prehľad Vzorového zákona	54
5.3	Direktíva Európskej únie o elektronickom podpise	56
5.3.1	Účel a história Direktívy Európskej únie o elektronic- kom podpise	56
5.3.2	Prehľad Direktívy	57
5.4	Zhrnutie: čo by mal upravovať zákon o elektronickom podpise	64
5.5	Slovenský zákon o elektronickom podpise	65
5.5.1	Definície	66
5.5.2	Úlohy a povinnosti plynúce zo zákona	73
5.5.3	Typy elektronického podpisu plynúce zo zákona a pro- cedúry s nimi spojené	79
5.5.4	Právna váha elektronického podpisu a jeho spôsob vy- užitia	84
5.5.5	Novela Slovenského zákona o elektronickom podpise . .	86
5.5.6	Zhrnutie a zákona a prehľad identifikovaných požiadaviek	89
6	Záver	96

Kapitola 1

Úvod

V súčasnej dobe sme svedkami zaujímavého javu, keď stále väčšia časť komunikácie prebieha elektronicky. Prispievajú k tomu klesajúce náklady na pripojenie do Internetu ako aj zvyšujúci sa počet služieb ktoré sú poskytované prostredníctvom Internetu. Takmer každá, či už malá alebo väčšia organizácia, používa pre spracovanie údajov svojej činnosti nejaký informačný systém. Klasickú poštu v komerčných kruhoch pomaly ale isto vytláča pošta elektronická.

Komunikácia prostredníctvom počítačov je jednoduchšia, pretože elektronické dokumenty sa ľahko modifikujú, kopírujú, rýchlo prenášajú a dobre skladujú.

Ak by sme chceli aspoň čiastočne nahradiť papierové dokumenty elektronickými, musíme riešiť problémy spojené s bezpečnosťou elektronických dokumentov. Informácie v elektronickej podobe možno ľahko a nepozorovane modifikovať, je problematické určiť ich pôvodcu a ich autor preto môže ľahko poprieť, že ich vytvoril. Chýba záruka autenticity a integrity elektronického dokumentu.

Riešenie týchto problémov je rozsiahly proces, ktorý pokrýva technologické, organizačné a legislatívne otázky.

Jedným z nástrojov ako zabezpečiť autenticitu a integritu elektronických dokumentov je elektronický podpis postavený na technológii digitálneho podpisu.

Od marca 2002 má Slovensko zákon o elektronickom podpise, ktorý by mal uľahčiť elektronickú komunikáciu medzi rozličnými subjektmi. Bohužiaľ takmer za tri roky existencie zákona sa elektronický podpis nerozšíril tak rýchlo ako by niektorí ľudia očakávali.

O elektronickom podpise sa veľa diskutuje, ale väčšinou nekvalifikovane. Napáda sa zákon a hľadajú sa dôvody prečo sa elektronický podpis nepoužíva tak, ako by sa dalo očakávať. Príčinou je predovšetkým to, že používanie

elektronického podpisu si vyžaduje zmenu tradičných procesov spracovania informácie v klasickej papierovej podobe, ktorá sa nedá vykonať okamžite.

Ďalšou príčinou je aj nedostatočné pochopenie podstaty elektronického podpisu, požiadaviek, ktoré vyplývajú z legislatívy na jeho používanie a princípov fungovania potrebnej technickej infraštruktúry na presadenie týchto požiadaviek.

V tejto diplomovej práci stručne vysvetlíme pohľady na elektronický podpis z hľadiska technológie a práva. Práca je určená najmä informatikom ale aj potencionálnym záujemcom o používanie elektronického podpisu.

Z technologického pohľadu sa budeme snažiť zjednodušene objasniť základy kryptografie a podstatu elektronických podpisov, problémy spojené s používaním elektronických podpisov a spôsoby ich riešenia.

Pôvodným zámerom bolo pozrieť sa na elektronický podpis z právneho hľadiska, pričom sme chceli identifikovať, vysvetliť a zdôvodniť jednotlivé technologické a procedurálne požiadavky kladené z hľadiska legislatívy na implementáciu elektronického podpisu. Naplnenie tohto cieľa na požadovanej formálnej úrovni by znamenalo niekoľkonásobne väčší rozsah práce, preto sme sa rozhodli pre jednoduchšiu a menej formálnu analýzu zákona o elektronickom podpise.

Štruktúra práce

V kapitole 2 stručne popíšeme históriu vývoja elektronického podpisu. Uvedieme si prehľad štandardizačných orgánov a popíšeme najvýznamnejšie body legislatívneho vývoja elektronického podpisu vo svete a na Slovensku.

V kapitole 3 uvedieme základné pojmy z kryptológie a priblížime požiadavky kladené na digitálny podpis ako aj spôsob jeho realizácie. Na záver tejto kapitoly stručne zhrnieme rozdiely medzi digitálnym a vlastnoručným podpisom.

Kapitola 4 priblíži problémy implementácie digitálnych podpisov v praxi. Popíše a vysvetlí ich riešenie pomocou PKI.

Dôležitou časťou práce je kapitola 5 venujúca legislatíve upravujúcej elektronický podpis. Zaoberáme sa v nej slovenským zákonom o elektronickom podpise ako aj dôležitými dokumentmi, ktoré ovplyvnili jeho vývoj. Keďže sa veľa diskutuje o zhode slovenského zákona o elektronickom podpise s legislatívou Európskej únie, v tejto časti analyzujeme aj Direktívu Európskej únie o elektronickom podpise. Na záver sa snažíme identifikovať a objasniť jednotlivé technologické požiadavky kladené slovenským zákonom a stručne opíšeme pripravovanú novelu zákona.

Kapitola 2

História

2.1 História elektronického podpisu a asymetrickej kryptografie

Počiatky elektronického obchodu sa tradujú od začiatku 60-tych rokov minulého storočia, kedy sa začali rozmáhať počítačové siete, ktoré umožňovali vznik proprietárnych distribuovaných informačných systémov. Tieto systémy slúžili najmä na interné účely veľkých spoločností (interakcia s externým prostredím nebola prakticky možná) a preto mohli byť jednoduchšie spravované pomocou interných stanov.

V roku 1976 prišli Diffie a Hellman s teoretickou úvahou ktorá by umožňovala, okrem iného aj realizáciu podpisu v prostredí počítačov a elektronických dokumentov. O rok neskôr Ronald L. Rivest, Adi Shamir a Leonard M. Adleman prakticky realizovali myšlienku Diffieho a Hellmana (asymetrickým šifrovacím systémom RSA).

Hoci história pripisuje objavenie myšlienky asymetrickej kryptografie Diffiemu a Hellmanovi existujú dôkazy, že prvé podnety v tejto disciplíne existovali už v roku 1970. V tomto roku James Ellis, zamestnanec *The British Communications – Electronics Security Group – CSEG*, vydal publikáciu ohľadom tzv. *Non Secret Encryption*, kde dokázal, hoci len teoreticky, existenciu asymetrického šifrovacieho systému. Ďalšou indíciou dokazujúcou pred rokom 1976 existenciu asymetrických šifrových systémov bol projekt *National Security Agency – NSA STU-III*, zaoberajúci sa bezpečným telefónnym systémom založeným na certifikátoch a infraštruktúre verejných kľúčov. Tento projekt začal v prvej polovici 70-tych rokov. Certifikáty boli na verejnosti predstavené až v roku 1979.

2.2 Popis vývoja štandardizačných orgánov a jednotlivých štandardov týkajúcich sa digitálneho podpisu a informačnej bezpečnosti

S masívnym otvorením Internetu širokej verejnosti v 90-tych rokoch začala byť naliehavá otázka autentifikácie v rámci tejto siete. Internet bol v svojich počiatkoch navrhnutý najmä s ohľadom na funkcionality a výkon a aj preto neposkytuje veľké možnosti bezpečnosti. Jedným z možných riešení ako zabezpečiť autenticitu v komunikácii cez Internet bol digitálny podpis.

Aj vďaka rozšíreniu Internetu do komerčnej sféry, zažil digitálny podpis v počiatku 90-tych rokov obdobie rýchleho vývoja. Vznikalo množstvo rozličných riešení, ktoré boli častokrát nekompatibilné. Preto sa popredné štandardizačné orgány rozhodli vzhľadom na dôležitosť digitálneho podpisu v rámci globálnej komunikácie vytvoriť štandardy, podľa ktorých by sa ľudia mohli riadiť.

Štandardom rozumieme popis požiadaviek (na riešenie nejakého problému), ktorému sa prispôbujú rôzni výrobcovia za účelom zaistenia kompatibility ich produktov. Proces vývoja štandardu môže byť (a väčšinou aj býva) zložitý a zdĺhavý. Zvyčajne sa stretne skupina odborníkov, ktorá vypracuje návrh riešenia a prednesie ho na diskusiu. Po úspešnom pripomienkovaní je dokument (riešenie) zoficiálnený – kodifikovaný. Takto vytvorený štandard je potom presadzovaný v praxi¹.

Štandard vzniká väčšinou pod záštitou jednej či viac organizácií zaoberajúcich sa štandardizačným procesom. V závislosti od štatútu týchto organizácií delíme štandardy nasledovne.

Štandard, ktorý bol kodifikovaný uznávanou štandardizačnou inštitúciou sa stáva štandardom *de jure*. Jeho záväznosť pre výrobcov a používateľov býva odlišná v závislosti od jeho vydavateľa, resp. právneho štatútu daného štandardu.

Štandardy môžu vznikať aj z podnetu súkromných firiem či výrobcov. Tie zvyčajne nemajú možnosť vydávať oficiálne normy záväzné pre iných výrobcov. Ak je však aj napriek tomu ich riešenie prebraté inými výrobcami, stávajú sa tieto štandardy *štandardmi de facto*.

Medzi najväčších tvorcov štandardov patrí Medzinárodná organizácia pre normalizáciu (International Organization for Standardization – **ISO**). ISO je organizácia zastrešujúca národné štandardizačné orgány v rámci 148 krajín medzi ktorými je aj Slovensko.

¹Veľakrát sa stáva, že štandard hoci ešte nedokončený (draft), je už presadzovaný v praxi.

Táto inštitúcia vyvinula množstvo noriem týkajúcich sa širokého spektra technológií, okrem iných aj informačných. V roku 1988 vyvinula štandard, ktorý je úzko spätý s používaním digitálnych podpisov a dalo by sa povedať, že je jedným z najdôležitejších v tejto oblasti. Názov tohto štandardu je **X.509** a zaoberá sa certifikátmi verejných kľúčov. Tento štandard prešiel niekoľkými zmenami a verziami. Momentálne najpoužívanejšia verzia je *X.509 v3*, ktorá bola schválená v roku 1996. Neskôr v roku 2000 bola vydaná zatiaľ posledná verzia tohto štandardu.

Medzinárodná elektrotechnická komisia² – IEC je celosvetová organizácia zastrešujúca národné elektrotechnické organizačno-standardizačné výbory. IEC bola založená v roku 1906. Cieľom IEC je podporovať medzinárodnú spoluprácu v otázkach elektrotechnickej a elektronickej normalizácie. IEC úzko spolupracuje najmä s ISO ale aj s ETSI. Množstvo štandardov a noriem ktoré vydala IEC v spolupráci s ISO je vysoké a ich vybraný zoznam môže čitateľ nájsť v [1].

Dalšou významnou inštitúciou je **National Institute for Standard and Technology – NIST**, ktorý bol založený v roku 1901 v USA. Hlavnou úlohou NIST-u je vyvíjať štandardy a technológie (nielen v oblasti informatiky ale aj v oblasti chémie, elektroniky, fyziky a iných). Napriek tomu, že ide o národnú štandardizačnú organizáciu, jej normy a odporúčania sú využívané aj v medzinárodnom kontexte.

Medzi najvýznamnejšie štandardy v oblasti informačnej bezpečnosti vyvinuté touto inštitúciou patria: *Digital Signature Standard – DSS*, *Data Encryption Standard – DES*, *Advanced Encryption Standard – AES* a mnoho iných napr. požiadavky na kryptografické moduly, manažment kľúčov, či implementáciu infraštruktúry verejných kľúčov.

European Telecommunications Standards Institute – ETSI je dôležitý štandardizačný orgán Európskej únie pre oblasť telekomunikácií. Medzi inými ETSI vydal dokumenty týkajúce sa formátu elektronického podpisu, profilu kvalifikovaných certifikátov a formátu časových pečiatok.

Európsky výbor pre normalizáciu³ – CEN je európska organizácia, ktorej cieľom je podporovať technickú harmonizáciu v Európe. Členmi CEN sú národné štandardizačné organizácie z krajín Európskej únie a Európskeho združenia voľného obchodu. V roku 1997 bola touto organizáciou založená pracovná skupina CEN/ISSS⁴. CEN/ISSS používa pri tvorbe noriem postup kombinujúci formálnu štandardizáciu s rýchlym komerčne orientovaným prístupom. Proces prijímania štandardov je založený na priamej účasti výro-

²The International Electrotechnical Commission

³European Committee for Standardization

⁴European Committee for Standardization / Information Society Standardization System

cov s ohľadom na záujmy spotrebiteľa a otvorenosť tohto procesu. Aktivity CEN/ISSS v odvetví elektronického podpisu sa týkajú oblasti zabezpečenia informačných systémov využívaných poskytovateľmi certifikačných služieb vydávajúcich kvalifikované certifikáty, požiadaviek kladených na bezpečné zariadenia ktoré pomáhajú pri tvorbe elektronického podpisu ako aj procesom, ktoré sú spojené s vytváraním elektronického podpisu.

European Electronic Signature Standardisation Initiative – EESSI je organizácia, ktorej účelom je iniciovať a koordinovať prípravu a prijímanie štandardov týkajúcich sa elektronického podpisu. Najdôležitejším dokumentom publikovaným EESSI je *Direktíva EU o elektronickom podpise*. Tento dokument stanovuje stratégiu riešenia problematiky elektronického podpisu z legislatívneho hľadiska v rámci Európskej únie. EESSI úzko spolupracuje s ETSI a CEN/ISSS.

V roku 1999 bol založený Európskou úniou projekt **New European Schemes for Signatures, Integrity and Encryption – NESSIE**. Jeho cieľom bolo navrhnuť portfólio silných kryptografických primitív rozličných typov. Hlavnou úlohou projektu bolo udržať silnú pozíciu európskeho výskumu kryptografie a posilniť pozíciu európskeho kryptografického priemyslu. Projekt NESSIE počas svojich troch rokov existencie organizoval štyri konferencie, ktorých cieľom bolo:

- Publikovať kryptografické primitívy a testovacie metodiky.
- Vybrať doporučenú množinu kryptografických primitív.
- Vytvoriť konsenzus s priemyselným odvetvím.
- Predložiť výsledky svojej práce európskym a svetovým štandardizačným orgánom.

V roku 2003 bol tento projekt ukončený a bola vydaná správa NESSIE Security Report, v ktorom bola zosumarizovaná práca na tomto projekte.

Okrem národných a medzinárodných inštitúcií ISO, NIST, EESSI, ETSI, IEC vydávajúcich štandardy de jure, existovala iniciatíva aj mimo týchto orgánov. V roku 1993 vznikli *RSA Public Key Cryptographic Standards – PKCS*, de facto štandardy pokrývajúce šifrovací systém RSA, Diffieho–Hellmanov protokol na výmenu kľúčov, certifikáty verejných kľúčov, algoritmy na šifrovanie, dešifrovanie, podpisovanie a na tvorbu digitálnych odťahov. PKCS vydali RSA Laboratories, ktoré sú súčasťou súkromnej firmy RSA Security vlastniacej patent na šifrovací systém RSA.

Iným prístupom k tvorbe de facto štandardov je tvorba **RFC**⁵ dokumentov. Tieto dokumenty podliehajú verejnej diskusii, ktorú zastrešuje Internet

⁵Request For Comments

Engineering Task Force (IETF). RFC dokumenty nie sú však iba štandardy. Sú to aj návody, vysvetlenia či stanoviská a názory.

Tvorba dokumentov RFC je rýchla a vzniknuté dokumenty bývajú často-krát jednoduchšie na pochopenie ako napr. dokumenty z dielne ISO. Aj z toho dôvodu bývajú dokumenty RFC dobrým štartovacím bodom, pri tvorbe neskorších oficiálnych štandardov, či pri ich dočasnom, alebo stálom nahrazení vo forme de facto štandardov.

V súčasnosti existuje okolo 4000 RFC dokumentov. Väčšina z nich sa zaoberá problematikou počítačových sietí, komunikačných protokolov a informačnej bezpečnosti. Medzi najpodstatnejšie RFC z hľadiska digitálneho podpisu patria tie, ktoré sa zaoberajú problematikou certifikátov a komunikačných protokolov. Týchto dokumentov je veľmi mnoho, preto ak má čitateľ záujem, nájde prehľad vybraných v [1].

Štandardizačných organizácií zaoberajúcich sa problematikou informačnej bezpečnosti je mnoho. Ich vzťahy bývajú zložité. Niekedy sa dokážu dohodnúť pomerne rýchlo, inokedy rozhodovanie trvá neúmerne dlho. Tento fakt často negatívne vplyva na proces vývoja štandardu a jeho zapracovanie do praxi. Určité riešenie ponúkajú medzinárodné dohody a legislatívne úpravy, ktoré umožňujú zjednotiť riešenia diskutovanej problematiky.

2.3 Legislatívne riešenie elektronického podpisu

Vďaka rýchlemu rozvoju informačných technológií sa začalo vyvíjať nové odvetvie obchodu – elektronický obchod. Elektronický obchod je založený na komunikácii prostredníctvom počítačových sietí a teda aj Internetu. Hoci otázku zabezpečenia a zjednotenia tejto komunikácie riešili štandardizačné orgány, pre úplnú funkčnosť elektronického obchodu bolo potrebné stanoviť aj legislatívne pravidlá, tak aby bola zachovaná rozumná miera jeho bezpečnosti a zároveň nebola ohrozená funkčnosť elektronického obchodu.

Základným článkom obchodu je zmluva medzi poskytovateľom služby a kupujúcim. Pre zaručenie schopnosti preukázať nárok na službu, tovar, či peniaze býva táto dohoda obvykle podpísaná. Podpis symbolizuje súhlas s obsahom zmluvy a pomáha identifikovať podpísanú osobu. Preto aj pri tvorbe legislatívy upravujúcej elektronický obchod bolo potrebné okrem iného definovať aj pojmy elektronického dokumentu, podpísaného elektronického dokumentu a stanoviť ich právnu účinnosť a procedúry a povinnosti spojené s ich vytváraním a používaním.

Prvým dôležitým právnym dokumentom upravujúcim problematiku pod-

pisu v prostredí počítačov a elektronickej komunikácie bol *UTAH Digital Signature Act* prijatý v roku 1995 v Spojených Štátoch Amerických.

Európa nasledovala až po USA v roku 1997, keď svoj zákon ako prvá krajina schválilo Nemecko. Nemecko sa tak stalo prvou krajinou, ktorá zákonom upravila rámcové požiadavky pre overenie platnosti digitálneho podpisu a používanie nevyhnutných kryptografických prostriedkov. Prínos nemeckého zákona spočíval aj v tom, že nebol obmedzený len na národné štandardy a ponechával možnosť integrácie systému do medzinárodného kontextu. Nemecký zákon sa stal vzorom pre mnohé európske štáty.

Prvou dôležitou nadnárodnou iniciatívou bol *Vzorový zákon Komisie Organizácie Spojených Národov pre Medzinárodné Obchodné Právo (The United Nations Commission on International Trade Law – UNCITRAL)* – 1997. V tomto dokumente sa po prvý krát objavila snaha vytvoriť abstraktný prístup k elektronickému podpisu, t.j. prístup ktorý by bol technologicky nezávislý.

Štáty EU sa tiež dohodli na spoločnom postupe v otázke legislatívneho riešenia problematiky elektronického podpisu. V apríli 1997 sa začal vývoj *Direktívy EU o elektronickom podpise*, ktorá bola po dvoch rokoch schválená Európskou komisiou dňa 31.12.1999, pričom sa štáty EU zaviazali, že uvedú do praxe princípy a požiadavky tohto dokumentu do 19.7.2001. Smernica bola vypracovaná tak aby zachovala nasledujúce princípy:

- technologická neutralita,
- interoperabilita elektronického podpisu v rámci krajín EU aj mimo nich,
- legislatívne upravenie platnosti elektronických podpisov tak aby bola zaručená ekvivalencia s vlastnoručným podpisom.

Legislatívny vývoj na Slovensku sa začal v roku 1998, keď sa Ministerstvo spravodlivosti SR začalo zaujímať o zabezpečenie elektronickej komunikácie. Bohužiaľ tento záujem nebol pretavený do žiadnej konkrétnej aktivity zo strany ministerstva. V roku 1999 vznikla skupina pri Ministerstve hospodárstva pripravujúca zákon o elektronickom obchode. Elektronický obchod však vyžaduje podstatnú mieru bezpečnosti, ktorej jednou z realizácií je aj elektronický podpis. Preto (a aj na základe Direktívy EU o elektronickom podpise) začal vznikať zákon o elektronickom podpise. Začiatkom roku 2000 uzrel svetlo sveta vládny návrh zákona z dielne MH SR založený na Direktíve EU o elektronickom podpise, českom zákone o elektronickom podpise a z časti na Vzorovom zákone UNCITRAL. Bohužiaľ tento návrh obsahoval množstvo nedostatkov tak technických ako aj legislatívnych. Ďalším problémom vládneho návrhu bolo zaostávanie prípravy zákona za časovým harmonogramom.

Slovenská Informatická Spoločnosť – SIS, ktorá sa počas predchádzajúcich rokov aktívne zúčastňovala na procese vývoja slovenského zákona o elektronickom podpise, v roku 2000 vytvorila odbornú skupinu, ktorá pripravila alternatívny návrh zákona.

Pre urýchlenie legislatívneho procesu si osvojil poslanec František Šebej tento návrh zákona a predložil ho do NRSR ako poslanecký návrh. Ako sa neskôr ukázalo vládny návrh mal neopraviteľné nedostatky a nemal šancu na úspech v NRSR, preto zostal v aktívnom legislatívnom konaní len poslanecký návrh. Poslanecký návrh zákona sa začal prerokovávať vo výboroch NR SR, ale pre nedostatky formálno-legislatívneho charakteru bol predkladateľom vrátený na prepracovanie. Prepracovaný poslanecký návrh bol v decembri 2001 podaný do parlamentu kde bol zaradený na januárovú schôdzu. Konečne v roku 2002 parlament schválil poslanecký návrh. V tom istom roku *Národný bezpečnostný úrad – NBÚ* vydal aj niekoľko vyhlášok, ktoré špecifikujú technické požiadavky, štandardy a formáty späté s elektronickým podpisom ako aj jeho používanie v obchodnom a administratívnom styku.

Podobne ako Slovenská republika aj Česká republika (vzhľadom na jej pripravovaný vstup do EU) bola zaviazaná Direktívou EU o elektronickom podpise prijať právne predpisy pre dosiahnutie súladu s Direktívou. Tak ako na Slovensku aj v Čechách vznikali spočiatku dva návrhy. Jeden bol z dielne *Úřadu pro státní informační systém – ÚSIS* a druhý bol pôvodom poslanecký (iniciovaný *Sdružením pro informační společnost – SPIS*). Takisto aj tu bol jeden z problémov čas. Poslanecký návrh zákona, hoci podľa niektorých expertov menej kvalitný, dostal prednosť pred vládny, najmä z dôvodu reálnejšieho časového plnenia. 26–27.3.2000 sa uskutočnilo rokovanie v Třešti kde sa ako ÚSIS tak aj SPIS dohodli na kompromisoch v návrhu. V apríli roku 2000 sa zákon predložil na prerokovanie do poslaneckej snemovne a neskôr v tomto roku bol aj prijatý. V roku 2002 a neskôr v 2004 bol zákon po dlhšej diskusii novelizovaný.

Kapitola 3

Základy kryptológie a podstata elektronického podpisu

3.1 Úvod

Dôvodov zabezpečenia digitálnej komunikácie je viacero. V prvom rade je jednoduchšie komunikovať cez verejné počítačové siete ako vytvárať súkromné – chránené siete. Toto riešenie je prakticky nemožné pre obyčajných ľudí a je realizovateľné len vojenskými úradmi, vládnyimi orgánmi, či rozsiahlymi organizáciami. Komunikácia cez nezabezpečené zdroje je preto oveľa častejšia.

Na prepojenie jednotlivých uzlov siete možno používať rozličné technológie. V závislosti od použitej technológie má útočník zjednodušenú alebo sťaženú pozíciu pri odchyťovaní či modifikovaní komunikácie. Každopádne pri použití bežných technológií ako sú káblové siete, satelitné či mikrovlnné spojenie je nerozumné predpokladať, že útočník nemôže manipulovať s našou komunikáciou. Preto je potrebné aby sme našu komunikáciu cez nezabezpečený kanál adekvátne chránili.

Kým pri využívaní služieb počítačových sietí na súkromné účely¹ nám mnohokrát nezáleží na bezpečnosti našej komunikácie, pri komunikovaní v rámci komerčnej, zdravotníckej, vojenskej či politickej sféry je potrebné zabezpečiť, aby táto komunikácia ostala konzistentná a utajená. Z odchytenia, pozmenenia či zadržania dôležitej komunikácie môže profitovať konkurencia, podvrtné živly, informačné služby alebo iné nepovolané osoby.

Okrem týchto protivníkov existuje aj prirodzený nepriateľ – príroda. Vplyvom rozličných šumov a technických porúch je komunikácia prirodze-

¹Napr. pri posielaní elektronickej pošty, ktorá neobsahuje citlivé údaje, napr. vtipy priateľom.

ne rušená. Riešením týchto problémov sa zaoberá teória kódovania. Ďalej v tejto práci budeme preto abstrahovať od tohto problému a budeme predpokladať, že vonkajšie vplyvy na komunikačné kanály neexistujú.

Existujú isté základné predpoklady, ktoré musí bezpečná komunikácia spĺňať. Tieto predpoklady sa odvíjajú od základných atribútov údajov vyskytujúcich sa v našej komunikácii, ktoré musia byť zachované a chránené. Medzi tieto atribúty patria:

Dôvernosť – stav, v ktorom je informácia utajená, známa iba vymedzenému okruhu subjektov; strata tohto atribútu znamená, že informácia je prezradená (únik informácie), teda že sa stane známou mimo vymedzeného okruhu subjektov.

Integrita – informácia je celistvá, v pôvodnom, nezmenenom stave, je neporušená; strata tohto atribútu znamená, že informácia je neúplná, nie je v pôvodnom stave, bola neoprávnene zmenená.

Autentickosť – stav, v ktorom je informácia pravdivá, skutočná, zodpovedajúca skutočnosti, nespochybniteľného pôvodu, teda je správnou reprezentáciou toho, čo je úmyslom, aby reprezentovala; strata tohto atribútu znamená, že údaj je nesprávny, nezodpovedá skutočnosti, ktorú by mal reprezentovať, je "falošný" (sfalšovaný).

Dostupnosť – stav, v ktorom je informácia k dispozícii, schopná bezprostredného použitia na nejaký účel; strata tohto atribútu znamená, že údaj nie je tam, kde je očakávaný, nie je schopný okamžitého použitia.

Pre lepšie pochopenie uvedených atribútov uvedieme teraz pár príkladov. Dôvernosť je asi prvý atribút komunikácie, čo každému človeku príde na rozum. Napríklad v komunikácii s osobným lekárom je nevhodné, aby sa jej obsah dostal do nepovoláných rúk, pretože by nás neskôr mohol kompromitovať alebo spôsobiť určitú diskrimináciu voči našej osobe. Ešte lepším príkladom môže byť vojenská komunikácia v ktorej sa snaží strana spojencov utajiť svoje plány pred nepriateľom. Strata tohto atribútu je v tomto prípade kritická a môže viesť k zlyhaniu celej operácie resp. misie.

Atribút integrity by sme mohli ilustrovať na príklade internetového bankovníctva. Predpokladajme, že chceme previesť istú čiastku z nášho účtu na účet príjemcu. Z hľadiska komfortu je pohodlné, ak máme tú možnosť, previesť túto operáciu z domu pomocou Internetu a služby, ktorú nám naša banka ponúka. Vyplníme platobný príkaz a odošleme ho našej banke. V prípade, že by bol niekto schopný tento dokument neoprávnene modifikovať, mohol by zmeniť buď číslo účtu alebo výšku prevodu. Tým by nám spôsobil finančnú ujmu.

Atribút autenticity sa síce na prvý pohľad podobá atribútu integrity, ale ako vidieť na nasledovnom príklade, nie je tomu tak. V niektorých prípadoch autenticita znamená, že subjekt ktorý s nami komunikuje (t.j. posiela správy), je naozaj ten za ktorý sa vydáva a s obsahom správ je uvedený a súhlasí s ním. Príklad kde je zachovaný atribút integrity, ale atribút autenticity je porušený môže vyzeráť nasledovne. Opäť si predstavme, že pomocou služby internetového bankovníctva uhradíme prevodom istú sumu. Útočník odchyť správu, ktorú posielame banke a neskôr ju opäť pošle². Ak by takáto správa neobsahovala nejaké ďalšie atribúty zaručujúce autenticitu ako napr. dátum a čas, banka ju nedokáže rozlíšiť od našej autentickej správy a preto ju považuje za korektnú (atribút integrity nebol porušený) a príkaz na prevod akceptuje. Opäť sa dostávame do situácie, keď nám útočník spôsobil finančnú ujmu.

Na ilustrovanie atribútu dostupnosti si možno vybrať konkurenčný boj v súkromnej sfére. Predpokladajme, že isté dve firmy prevádzkujú platený internetový portál poskytujúci napríklad spravodajské informácie. Jedna z firiem sa rozhodla, že zníži svoje náklady a tým aj ceny tak, že zruší prevádzku "hot backup" serverov. Druhá firma túto informáciu nejakým spôsobom zistila a rozhodne sa ju využiť vo svoj prospech. Najme si skupinu ľudí, ktorí sú schopní na čas znemožniť hlavnej serverovej farme konkurenčnej firmy prevádzkyschopnosť. Keďže konkurenčná firma zrušila zálohovacie servery nie je schopná poskytovať ani základné služby. Týmto činom stratí konkurenčná firma zákazníkov, pretože sa naštříb ich dôvera v jej služby. Toto sa môže stať najmä ak by sa táto situácia opakovala častejšie alebo vyskytla v momente keď sú informácie poskytované informačným portálom extrémne dôležité.

Hoci útoky na tieto atribúty vo svete počítačov sledujú zväčša tie isté ciele ako útoky v klasickom svete, spôsoby prevedenia bývajú iné. Útočník je mnohokrát vo výhode z nasledovných príčin:

Automatizácia útoku – Jednou zo zásadných výhod útočníka je možnosť ľahko opakovať a modifikovať útoky. Jednoduchým príkladom využitia tejto výhody je tzv. *Denial of Service* – *DoS* resp. *Distributed Denial of Service* – *DDoS* útok. V prípade tohto útoku útočník posiela na cieľ či už zmysluplné alebo nezmyselné správy tak, aby zaťažili poskytovateľa služieb natoľko, že nebude môcť svoje služby poskytovať ostatným subjektom.

Útok zo vzdialeného miesta – Výhoda útočníka spočíva aj v ľahšom ukrytí a ťažšom postihu za jeho zločiny. Predstavme si situáciu, keď je útočník fyzicky prítomný v nejakej krajine tretieho sveta s nie príliš

²Tento spôsob útoku nazývame aj útok opakovaním.

rozvinutou legislatívou (prípadne slušne rozvinutou korupciou). Takýto zločinec sa môže stať pomerne ťažko vystopovateľným a postihnuteľným.

Zverejnenie spôsobu útoku – Mnohokrát sa stáva, že útok môže byť ľahko realizovateľný (pomocou špeciálneho softvéru) aj laickej verejnosti a nielen odborníkom venujúcim sa danej oblasti. Preto aj zverejnenie spôsobu útoku, prípadne daného softvéru, môže byť potenciálnym bezpečnostným rizikom.

Obrana voči počítačovej kriminalite je rozsiahly proces počnúc návrhom informačného systému, jeho prevádzkou, auditom a tvorbou špecifických opatrení. Jedným zo základných článkov obrany systému je kryptológia.

3.2 Základné pojmy kryptografie

Kryptológia je veda zaoberajúca sa skúmaním zabezpečenia komunikácie. Kryptológia sa skladá z dvoch vedných disciplín – *kryptografie* a *kryptoanalýzy*. Kryptografia sa zaoberá návrhom algoritmov a protokolov slúžiacich na ochranu komunikácie. Kryptoanalýza skúma možnosti útokov na tieto konštrukcie – kryptosystémy.

Hlavným cieľom kryptografie je ochrana informácie. Pod informáciou môžeme rozumieť údaje resp. správy. Tieto sa zvyčajne posielajú v nejakej kódovanej forme³.

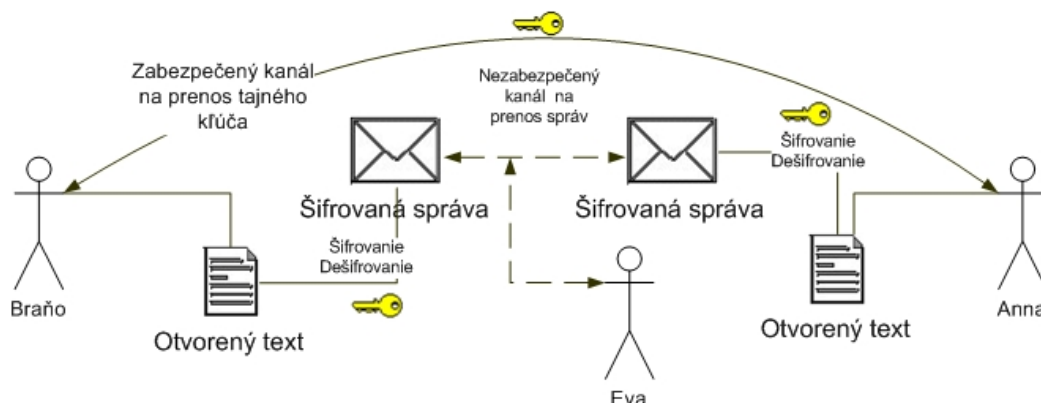
Pre úspešné pochopenie tejto kapitoly je nutné si definovať niekoľko základných pojmov.

Komunikácia je proces, v priebehu ktorého si účastníci komunikácie vymieňajú správy. Tento proces je upravený presnými pravidlami (určujúcimi napríklad postupnosť správ, maximálny čas medzi správami apod.), ktoré sa nazývajú komunikačným protokolom.

V komunikácii vystupujú vždy aspoň dve entity – odosielateľ a príjemca. Budeme ich označovať *Anna* a *Braňo*. Ich cieľom je, aby žiadna tretia strana (označme ju *Eva*) nemohla odpočúvať ani modifikovať ich komunikáciu.

V prípade že *Eva* komunikáciu modifikuje, opakovane alebo oneskorene posielá správy, prípadne predstiera falošnú identitu hovoríme o *aktívnom protivníkovi* a v prípade že ju len odpočúva hovoríme o *pasívnom protivníkovi*.

³Rozdiel medzi kódovaním a šifrovaním je, že informácia je kódovaná s cieľom vylepšenia atribútov prenosu – napr. možnosť opravy chyby alebo zmenšenia objemu prenášaných dát a je ľahko dekodovateľná bez dodatočnej informácie. Naopak šifrovanie má za cieľ znemožniť dešifrovanie správy bez tajnej informácie.



Obrázok 3.1: Model komunikačného kanála Anny a Braňa

Šifrovaním nazveme operáciu vykonanú na informácii za účelom znemožnenia zistenia obsahu informácie bez znalosti tajnej informácie – *kľúča*. *Dešifrovaním* nazveme reverznú operáciu, kde za pomoci kľúča šifrovanú správu opäť transformujeme do čitateľného stavu. Nešifrovanú informáciu budeme tiež nazývať *otvoreným textom*, označujeme ju M resp. P . Šifrovanú informáciu nazveme *šifrovým textom* a označujeme C . Teraz sme schopní uviesť prvú definíciu.

Definícia 3.2.1 *Šifrovací systém* je päťica $(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$ pričom:

1. \mathcal{P} je konečná množina možných **otvorených textov**.
2. \mathcal{C} je konečná množina možných **šifrových textov**.
3. \mathcal{K} je konečná množina možných **kľúčov**.
4. \mathcal{E} a \mathcal{D} sú množiny šifrovacích a dešifrovacích operácií pričom:
5. $\forall k \in \mathcal{K} \exists e_k \in \mathcal{E}, d_k \in \mathcal{D}$ sú operácie $e_k : \mathcal{P} \rightarrow \mathcal{C}$ a $d_k : \mathcal{C} \rightarrow \mathcal{P}$ také že $\forall x \in \mathcal{P} : d_k(e_k(x)) = x$

Poznámka 3.2.1 V podstate platí, že e a d sú funkcie pričom obe sú definované nasledovne: $e : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{C}$ a $d : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{P}$

V bežnej praxi (najmä v komerčnej sfére) sa nezvykne utajovať spôsob šifrovania a dešifrovania – kryptosystém. To čo musí ostať tajné je šifrovací kľúč. Problematike kryptografických kľúčov sa budeme venovať v sekcii 3.2.4.

Na základe rôzneho pochopenia úlohy kryptografického kľúča sa diferencujú kryptosystémy na symetrické a asymetrické. Vo všeobecnosti by sa

dalo zjednodušať povedať, že symetrické systémy používajú jeden tajný kľúč a asymetrické systémy používajú pár kľúčov verejný a súkromný. Kým v symetrických systémoch slúži tajný kľúč na šifrovanie aj dešifrovanie, v asymetrických systémoch sú tieto operácie rozdelené medzi pár kľúčov. Pomocou súkromného kľúča sa obsah správy dešifruje a tento kľúč je utajený. Pomocou verejného kľúča sa obsah správy šifruje a tento kľúč je prístupný širokej verejnosti. O symetrickom a asymetrickom spôsobe šifrovania sa čitateľ dozvie viac v sekciách 3.2.2 a 3.2.3.

Bez ohľadu nato či ide o symetrický alebo asymetrický šifrovací systém, tento systém slúži na ochranu a utajenie údajov pred nepovolanou osobou. V prípade, že táto osoba sa napriek tomu, že údaje nie sú pre ňu určené, snaží k nim dostať, prípadne ich modifikovať, nazveme ju útočníkom. V nasledovnej časti sa pozrieme nato aké možnosti má tento útočník a z akého uhla pohľadu sa možno pozeráť na zabezpečenie údajov.

3.2.1 Model bezpečnosti šifrových systémov a spôsoby útokov na šifrovacie algoritmy

Cieľom útoku na šifrovací systém je obvykle nájdenie otvoreného textu k danému šifrovanému textu, prípadne odhalenie tajného kľúča či vytvorenie falošnej správy.

Spôsoby útokov na šifrovacie algoritmy sa líšia v závislosti od prostriedkov útočníka a množstva získaných informácií o parametroch systému. Vo všeobecnosti sa predpokladá, že útočník pozná algoritmus ktorým bola správa šifrovaná. Dôvodom tohto predpokladu je, že v prípade využitia algoritmu v praxi je vysoká hrozba jeho reverse engineering-u. Tento predpoklad sa ukázal ako správny v mnohých prípadoch. Len pre zaujímavosť mnoho šifrových systémov, ktoré sa spoliehali na utajenie algoritmu bolo pomerne rýchlo rozbitých. Ako príklad by sme mohli uviesť RC4 použité na šifrovanie komunikácie mobilných telefónov, CSS algoritmus pre šifrovanie DVD a šifrovací algoritmus Firewire.

Útok na základe šifrovaného textu. Cipher Text Only Attack (COA). Útočník má k dispozícii len šifrový text. Na základe tejto znalosti, prípadne znalosti šifrovacieho a dešifrovacieho algoritmu sa snaží nájsť otvorený text, či súkromný kľúč, ktorý sa používa na dešifrovanie alebo šifrovanie. Väčšina moderných algoritmov je voči tomuto útoku odolná, ale ak má útočník k dispozícii enormnú výpočtovú silu, špeciálne vybavenie či iné neštandardné výhody, môže byť aj tento typ útoku serióznou hrozbou.

Útok na základe znalosti otvoreného textu. Known Plaintext Attack (KPA). Útočník má k dispozícii niekoľko šifrovaných textov a k nim zodpovedajúcich otvorených textov. Jeho cieľom je získať kľúč. V prípade znalosti kľúča sme schopní dešifrovať ostatné šifrované texty šifrované pomocou daného kľúča. Hoci sa na prvý pohľad tento spôsob útoku môže zdať nepravdepodobným a zbytočným, je v mnohých prípadoch ľahko realizovateľný. Ako príklad realizácie môže poslúžiť existencia štandardných hlavičiek súborov editora Word. Všetky tieto súbory začínajú rovnakými 100 bajtmi. V prípade že protivník je schopný získať kľúč na základe tejto znalosti môže prečítať celý dokument. KPA sa použil aj počas druhej svetovej vojny na rozbitie nemeckého šifrového systému *Enigma*.

Útok na základe vybraného otvoreného textu. Chosen Plaintext Attack (CPA). Protivník si môže vybrať sám aký otvorený text chce zašifrovať tajným kľúčom. Jeho cieľom je opäť získať kľúč. K takémuto útoku môže prísť, keď sa útočník dočasne zmocní⁴ šifrovacieho zariadenia a môže vytvárať šifrované správy.

Útok na základe vybraného šifrovaného textu. Chosen Cipher Text Attack (CCA). Protivník má možnosť dešifrovať niekoľko málo šifrovaných textov. Tento útok nie je veľmi pravdepodobný.

Tak ako existuje viac typov útokov (líšiacich sa v závislosti od možností útočníka) existuje aj viacero pohľadov na bezpečnosť v kryptografii. Dôvodom existencie týchto rôznorodých pohľadov je široké spektrum využitia kryptografie v reálnom živote, pričom požiadavky na bezpečnosť, rýchlosť a dostupnosť konkrétneho riešenia sa menia od aplikácie k aplikácii. Z týchto názorov teraz uvedieme len tie všeobecnejšie a najviac uznávané.

Nepodmienená bezpečnosť (absolútna bezpečnosť). Útočník nemôže na základe šifrovaného textu, bez ohľadu na jeho výpočtovú silu a poskytnutý čas, nič presnejšie o otvorenom texte ani o kľúči zistiť. Vernamova šifra spĺňa kritérium absolútnej bezpečnosti avšak pre prax je takmer nepoužiteľná. Vyžaduje totiž dĺžku kľúča ekvivalentnú dĺžke otvoreného textu⁵, pričom každý kľúč je možné použiť iba raz na šifrovanie jednej správy, t.j. nemôžeme šifrovať viacero správ jedným

⁴Napríklad sa vláme do kancelárie a dočasne sa zmocní počítača používaného na šifrovanie údajov.

⁵Je teda jasné, že ak sme schopní preniesť bezpečne kľúč, ktorého dĺžka je rovnaká ako dĺžka utajovanej informácie, sme schopní preniesť aj utajovanú informáciu. Výhodou je však možnosť si tento kľúč "predgenerovať" a potom preniesť.

kľúčom. Napriek tomuto obmedzeniu sa Vernamova šifra používala najmä v diplomatických či vojenských sférach. Kľúč sa vygeneroval vopred, distribuoval sa bezpečným spôsobom medzi zúčastnené strany a uzamkol sa niekde v trezore, kde čakal na svoje použitie.

Výpočtová bezpečnosť. V praxi sa zvyčajne stretávame s protivníkmi ktorých zdroje tak časové ako aj výpočtové sú obmedzené. Z hľadiska teórie zložitosti sa ukazuje ako vhodná trieda algoritmov trieda pravdepodobnostných algoritmov bežiacich v polynomiálnom čase⁶. Znamená to, že existuje horný odhad dĺžky trvania výpočtu algoritmu pomocou ktorého útočíme, ktorý je ohraničený polynómom pričom polynomický by mal byť vzhľadom na dĺžku vstupu. Šifrovací algoritmus je výpočtovo bezpečný ak takýto algoritmus nevieme nájsť.

”Dokázateľná“ bezpečnosť. Existujú dve interpretácie tohto modelu. Prvou interpretáciou dokázateľnej bezpečnosti je, ak rozbitie šifrovacieho algoritmu je ekvivalentné s riešením nejakého ťažkého matematického problému⁷. Ďalšou možnou interpretáciou dokázateľnej bezpečnosti je, ak šifrový algoritmus je dokázateľne odolný voči istej technike kryptoanalýzy (napr. diferenciálna alebo lineárna kryptoanalýza).

Praktická bezpečnosť. V tomto modeli sa šifrovací algoritmus považuje za bezpečný, pokiaľ rozbitie šifry vyžaduje viac nákladov, ako je hodna informácia ktorú ochraňujeme.

Bezpečnosť na základe histórie. Bezpečnosť šifrovacieho algoritmu môže byť posudzovaná aj na základe počtu kryptoanalytikov a spôsobov útokov neúspešne vyskúšaných na rozbitie daného algoritmu. Hoci sa tento pohľad na bezpečnosť kryptosystému v laických kruhoch považuje za presvedčivý, jeho hodnota je neurčitá. Problémom ostáva overiť kto a koľko prostriedkov venoval rozbájaniu algoritmov.

3.2.2 Symetrická kryptografia

Symetrický spôsob šifrovania zodpovedá definícii kryptosystému v ktorom existuje len jeden utajený kľúč, ktorý sa používa zároveň na šifrovanie aj dešifrovanie. Tento kľúč si Anna a Braňo vymenia pomocou zabezpečenej

⁶Polynomiálne algoritmy sú v dnešnej dobe a dostatočne blízkej budúcnosti efektívne realizovateľné.

⁷Medzi takéto problémy patria napríklad problém faktorizácie alebo problém diskrétného logaritmu.

komunikácie (napríklad sa môžu osobne stretnúť a odovzdať si kľúč na diske, alebo ho pošlú za pomoci dôveryhodnej kuriérskej služby). Neskôr na základe tohto tajného kľúča môžu posilať informácie v zašifrovanom stave takým spôsobom, že Eva bude mať sťaženú resp. znemožnenú možnosť odpočúvania, falšovania či modifikovania komunikácie. Symetrické šifrovacie algoritmy môžeme ďalej rozdeliť na *blokové* a *prúdové*.

Blokové šifrovacie algoritmy rozdelia otvorený text na bloky rovnakej dĺžky na ktoré aplikujú šifrovaciu transformáciu. Dešifrovanie prebieha analogicky. Šifrový text sa opäť rozdelí na bloky a na ne sa aplikujú dešifrovacie algoritmy. Medzi najznámejšie blokové šifrovacie algoritmy patria *DES*, *3DES*, *AES – Rijndael* a *IDEA*.

Prúdové šifrovacie algoritmy otvorený text rozdelia tiež na bloky (hoci aj 1 bitové), pričom sa snažia k otvorenému textu pripočítať postupnosť "náhodných"⁸ bitov generovaných na základe kľúča prípadne tzv. inicializačného vektora a otvoreného textu. Dešifrovanie prebieha inverzným procesom na prijímajúcej strane, kde sa vygeneruje na základe tajného kľúča, príp. šifrovaného textu a inicializačného vektora tá istá "náhodná" postupnosť bitov ako pri šifrovaní a na základe šifrovaného textu a tejto postupnosti získame opäť pôvodný otvorený text. Výhodou prúdových šifrovacích algoritmov je ich rýchlosť a dobrá hardvérová implementácia. Dva príklady prúdových šifrovacích algoritmov sú *SNOW* a *RC4*.

3.2.3 Asymetrická kryptografia

Istou nevýhodou symetrických systémov je potreba zdieľania tajného kľúča medzi každou komunikujúcou dvojicou. Predstavme si, že máme n subjektov, ktoré chcú medzi sebou komunikovať posielaním šifrovaných správ. V tomto prípade potrebujeme kľúč pre každú dvojicu účastníkov, teda $\binom{n}{2}$ kľúčov. Zrejme počet kľúčov potrebných na uskutočnenie takejto zabezpečenej komunikácie rastie kvadraticky s počtom účastníkov tejto komunikácie.

Tento fakt spôsobuje množstvo problémov týkajúcich sa distribúcie a správy tajných kľúčov. V prvom rade je nutné rozdistribúovať enormné množstvo kľúčov medzi jednotlivých účastníkov komunikácie. Ak sa nám tento problém podarí preklenúť, zostáva nám vyriešiť správu tajných kľúčov účastníkmi. Jednotlivé subjekty musia tieto kľúče bezpečne uložiť. Po čase je potrebné proces distribúcie kľúčov zopakovať s novými kľúčmi, aby sa predišlo ich uhádnutiu (periodická zmena kľúčov). No a v prípade pridania nového účastníka do rámca našej komunikácie je potrebné vytvoriť n nových

⁸Proces generovania týchto bitov je deterministický a tak aj táto postupnosť nie je náhodná. Dá sa zrekonštruovať. Podstatné je aby útočník nebol schopný efektívne uhádnuť bez znalosti kľúča podstatnú časť tejto postupnosti.

tajných kľúčov a tie rozposlať bezpečným spôsobom medzi ostatných účastníkov komunikácie. Tento akt si v prípade, že sú osoby geograficky vzdialené, môže vyžadovať služby dôveryhodnej tretej strany.

Čiastočné riešenie týchto problémov umožňujú kryptosystémy založené na asymetrickej kryptografii. Vďaka svojej podstate, asymetrické systémy umožňujú ľahšie distribuovať kľúče medzi účastníkmi komunikácie.

Asymetrické šifrovacie systémy sú založené na existencii dvoch transformácií e_k a d_k štandardne známych ako šifrovacia a dešifrovacia transformácia, pričom ale platí, že zo znalosti šifrovacej transformácie e_k **nie je efektívne možné** zistiť dešifrovaciu transformáciu d_k . V praxi sa to rieši pomocou dvojice kryptografických kľúčov označovaných ako *súkromný* ($k_{private}$) a *verejný* (k_{public}).

V prípade, že Anna chce poslať šifrovanú správu Braňovi, použije jeho verejný kľúč na zašifrovanie otvoreného textu. Braňo obdrží šifrový text a dešifruje na základe jeho súkromného kľúča. Proces teda prebieha nasledovne:

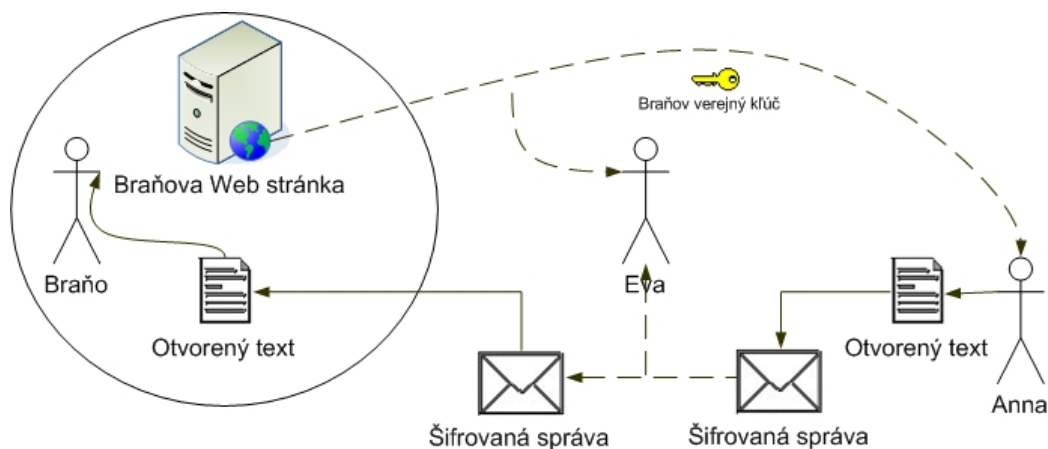
- 1) Anna získa Braňov verejný kľúč, $K_{B_{public}}$ z dôveryhodného zdroja⁹.
- 2) Anna za pomoci šifrovej transformácie e , otvoreného textu P a kľúča $K_{B_{public}}$ vytvorí šifrový text. $C = e_{K_{B_{public}}}(P)$.
- 3) Anna pošle cez nezabezpečený kanál šifrový text C .
- 4) Braňo obdrží šifrový text C od Anny.
- 5) Braňo použije svoj súkromný kľúč $K_{B_{private}}$, dešifrovaciu transformáciu d a šifrový text na obnovenie pôvodného otvoreného textu, $P = d_{K_{B_{private}}}(C)$.

Za zmienku stojí, že asymetrické šifrovacie systémy nemôžu byť absolútne bezpečné. Útočníkovi stačí vyskúšať všetky možné otvorené texty zašifrovať na základe znalosti verejného kľúča a porovnávať, kým nenájde také x že $y = e_k(x)$. Vo všeobecnosti by sa dali vlastnosti asymetrického šifrovacieho systému zhrnúť do troch bodov.

1. **korektnosť** – Dešifrovanie šifrovaného textu musí šifrový text opäť transformovať do pôvodného otvoreného textu.

$$\forall P \in \mathcal{P} : d_{k_{private}}(e_{k_{public}}(P)) = P$$

⁹Podstatné je aby Eva nemohla podvrhnúť Anne svoj verejný kľúč. Inak by Anna zašifrovala správu pomocou Evinho kľúča a poslala Braňovi. Eva by šifrovanú správu odchytila a pomocou svojho súkromného kľúča extrahovala pôvodný šifrový text. Ten by potom mohla (no nemusela) poslať Braňovi zašifrovaný pomocou Braňovho verejného kľúča (ku ktorému má prístup lebo je verejný).



Obrázok 3.2: Model šifrovanej komunikácie Anny a Braňa pomocou asymetrického kryptosystému

2. **efektívnosť** – Šifrovacie, dešifrovacie a inicializačné¹⁰ algoritmy musia byť efektívne realizovateľné.
3. **bezpečnosť** – Je ťažké zo znalosti transformácie e_k nájsť transformáciu d^* tak že pre dostatočne veľa šifrovaných textov C platí $d^*(C) = d_k(C)$. Inak povedané funkcia e_k je ťažko invertovateľná, tiež hovoríme o funkcii e_k že je *jednosmerná* alebo *one-way*.

Výhodou asymetrických kryptosystémov ako sme už spomenuli je jednoduchší manažment kľúčov. Ich nevýhodou je vyššia výpočtová zložitosť. V praxi sa preto častokrát používa tzv. *hybridné šifrovanie*. Otvorený text sa zašifruje pomocou náhodne zvoleného kľúča k nejakým symetrickým šifrovacím algoritmom. Kľúč k sa potom zašifruje pomocou asymetrického systému a pripojí k správe. Výhodou tohto postupu je oveľa nižšie množstvo údajov šifrovaných pomocou asymetrického systému (z čoho vyplýva vyššia rýchlosť šifrovania) a nevýhodou je, že takýto systém je tak silný ako slabší z dvojice asymetrického a symetrického systému použitého pri šifrovaní.

Medzi najznámejšie asymetrické kryptosystémy zaraďujeme *RSA* a *El Gamal*. O týchto šifrovacích schémach je možné sa dozvedieť viac v [3, str. 203] a [5].

¹⁰Algoritmy generujúce kľúče prípadne iné parametre šifrovacieho systému.

3.2.4 Úloha kľúčov pri šifrovaní

Jednou z najjednoduchších ciest ako porovnať silu šifrovacích algoritmov je dĺžka kľúča.

Dĺžka kľúča reprezentuje veľkosť priestoru odkiaľ kľúče vyberáme. Napr. ak je kľúč dĺžky 32 bitov, znamená to, že kľúčom môže byť jedno z čísel $\{0, \dots, 2^{32} - 1\}$, teda počet možných rôznych kľúčov je cca. 4 miliardy¹¹.

Vo všeobecnosti platí tvrdenie, že algoritmus používajúci krátky kľúč je zlý, neplatí však, že algoritmus s dlhým kľúčom musí byť dobrý.

Jedným zo spôsobov ako Eva môže zistiť obsah šifrovanej správy, v prípade že nebol použitý absolútne bezpečný šifrovací systém, je vyskúšať každý možný kľúč¹². V prípade že dĺžka kľúča je n bitov, možných kľúčov je 2^n . Takže v prípade že kľúč je dlhý 40 bitov existuje približne miliarda možných kľúčov. Čo znamená, že počítač schopný vyskúšať miliardu kľúčov za sekundu by bol schopný nájsť správny kľúč za približne 18 minút.

Útok pomocou hrubej sily je vysoko neefektívny pretože s počtom výpočtovej sily rastie lineárne t.j. keď máme dvakrát toľko počítačov sme schopní vyskúšať dvakrát toľko kľúčov. Ale vzhľadom na dĺžku kľúča rastie exponenciálne t.j. pridaním jedného bitu k dĺžke kľúča sa priestor kľúčov rozšíri dvojnásobne.

Z týchto vlastností pramení dôvod výberu správnej dĺžky kľúča. Pre momentálne potreby a potreby blízkej budúcnosti (najbližších 10 rokov) sa považujú za dostatočné dĺžky kľúčov 1024 bitov pre algoritmus RSA a 96 bitov pre algoritmus 3DES. Dokonca pre kľúč dĺžky 2048 bitov RSA algoritmu najlepší známy spôsob rozbitia tohto šifrovacieho systému¹³ dosahuje limity adresného priestoru 64-bitových procesorov.

Proces rozbitia kryptosystému, je väčšinou zdĺhavý, náročný na financie aj ľudské zdroje a mnohokrát prakticky nerealizovateľný. Preto sa protivník orientuje viac na inú zraniteľnosť kryptosystémov, na odhalenie tajných parametrov – kryptografických kľúčov. Z hľadiska útočníka existuje viacero spôsobov ako sa dostať ku kľúču. Tieto závisia od životného cyklu kľúča skladajúceho sa z: generovania kľúča, bezpečného skladovania kľúča, korektného používania kľúča a jeho odstránenia.

Počas generovania kľúča je nutné zabezpečiť aby bol kľúč dostatočne odolný voči rôznym útokom kryptoanalytikov, unikátny (najmä v oblasti asymetrickej kryptografie) a dobre utajený. Požívateľ si môže kľúč (pár

¹¹V praxi toto tvrdenie neplatí, pretože niektoré kľúče nie sú dostatočne kryptograficky silné a nemali by byť preto použité. Týchto kľúčov však nebýva príliš veľa a preto môžeme brať mohutnosť množiny odkadiaľ kľúč vyberáme ako dobrý odhad počtu kľúčov.

¹²Tento spôsob útoku sa nazýva útok *hrubou silou* resp. *brute-force attack*.

¹³General Number Field Sieve algoritmus [8].

klúčov) vygenerovať buď sám, alebo môže prenechať túto činnosť nejakej dôveryhodnej tretej strane. Každý z týchto postupov má svoje výhody a nevýhody.

V prípade generovania kľúča používateľom, používateľ nie je schopný zabezpečiť plnú kontrolu nad týmto procesom. Vždy musí prejsť kus dôvery či už tvorcom softvéru alebo hardvéru. V otázke generovania kľúčov by sa používateľ nemal spoliehať na bezpečnosť svojho počítača. Lepším riešením je v tomto prípade čipová karta dodaná dôveryhodným výrobcom s dobrou reputáciou. Výhody kvalitne navrhutej čipovej karty spočívajú v nemožnosti jednoducho manipulovať s citlivými údajmi na nej uloženými. Naopak v prípade osobného počítača používateľ častokrát nemôže vylúčiť infekciu vírusom, prítomnosť trójskeho koňa alebo iného zákerného programu.

V prípade, že kľúč je generovaný dôveryhodnou treťou stranou je tento proces zdĺhavejší a drahší. Navyše používateľ musí dôverovať vo vysokej miere danej inštitúcii. Na druhú stranu týmto spôsobom generovaný kľúč má mnoho výhod. Inštitúcia môže zaručiť unikátnosť vydaných kľúčov a je schopná vytvoriť kľúče dostatočnej kryptografickej sily. Bolo by vhodné keby táto inštitúcia používala hardvérové vybavenie odolné voči nežiaducej manipulácii (*tamper-proof device*). Týmto spôsobom zaručí zákazníkom, že ich kľúče neboli kompromitované aj v prípade, ak bol niektorý z operátorov podvodník. Vhodnou vlastnosťou karty je aj notifikácia upozorňujúca na prvé použitie kľúča. Slúži ako poistka že zákazníkov kľúč nebol použitý skôr.

Bezpečné skladovanie kľúča a jeho korektné používanie je fáza nasledujúca po vygenerovaní kľúča a jeho odovzdaní do rúk používateľa. Opäť sa odporúča používať čipové karty (alebo iné tamper-proof zariadenia), ktoré neumožňujú neautorizovanú manipuláciu s kryptografickým kľúčom.

Nebezpečným útokom v tejto časti životného cyklu kryptografického kľúča, je útok, ktorý zneužíva ľudskú dôveru. Útok nie je zameraný voči prístrojom ktoré uchovávajú kľúč, ani voči kryptosystému, ale spolieha sa na nedostatočnú osvetu resp. neexistenciu bezpečnostných smerníc v rámci existujúceho informačného systému alebo komunikácie. Hlavná myšlienka celého útoku spočíva v kontakte používateľa s útočníkom, ktorý predstiera falošnú identitu – napr. správca siete. Na základe tejto identity vymámi od používateľa informácie, ktoré vedú k odhaleniu kľúča alebo schopnosti dešifrovať šifrovanú komunikáciu.

Opísaný útok nie je jediný spôsob ako sa dostať ku kľúču inak než rozbitím kryptosystému. Kľúč je možné ukradnúť, alebo získať pomocou vydierania.

Aby sa predišlo úspešnému útoku majú šifrovacie kľúče obmedzenú dobu platnosti. Je zrejmé, že po ukončení doby vymedzenej na používanie šifrových kľúčov je potrebné ich bezpečné uskladnenie alebo likvidácia. V prípade, ak

by sa útočník dostal k starým šifrovacím kľúčom, vedel by dešifrovať naše dáta, ktoré sme pred ním chceli ochrániť¹⁴.

3.3 Digitálny podpis

Asymetrické šifrovacie systémy nás síce zbavili problému správy kľúčov, avšak predstavili nový a závažný problém. Pri symetrickom systéme šifrovania si mohol byť Braňo istý, že komunikuje s Annou a nie Evou, pretože len on a Anna poznali tajný kľúč. Pri asymetrickom systéme môže Eva ľahko zašifrovať pomocou Braňovho verejného kľúča správu, ktorú chce Braňovi podhodiť a vydávať sa za Annu. Podobný problém môže vzniknúť aj pri symetrickom šifrovaní v prípade, že Braňo by chcel vytvoriť falošnú správu od Anny. Anna by nemohla dokázať že správu nevytvorila resp. Anna môže poprieť autorstvo správy ktorú vytvorila. Dôvodom týchto závažných nedostatkov komunikácie je chýbajúca autentizácia dokumentu. Riešenie tohto problému prináša elektronický podpis. Elektronický podpis je abstraktná konštrukcia, ktorá umožňuje realizáciu aktu podpisovania v digitálnom svete počítačov¹⁵. Elektronický podpis môže byť realizovaný rôznymi spôsobmi. Od použitej realizácie závisí dostupnosť, cena ale hlavne bezpečnosť riešenia. Jednou z realizácií, ktorá spĺňa kľúčové podmienky kladené na elektronický podpis, je dostupná a zaručuje rozumnú mieru bezpečnosti, sú digitálne podpisy.

3.3.1 Atribúty vlastnoručného podpisu

Aby sme boli schopní pochopiť konštrukciu elektronického podpisu musíme si najprv stanoviť požiadavky, ktoré chceme aby spĺňal. Na elektronický podpis musia byť kladené rovnaké resp. aspoň podobné požiadavky ako na klasický, rukou písaný podpis. Vlastnoručný podpis aspoň čiastočne spĺňa nasledovné požiadavky.

Zviazanosť s dokumentom: Pre úspešnú autentifikáciu dokumentu je nutné aby bol dokument nejako zviazaný s podpisom. Teda aby nebolo možné podpis kopírovať, falšovať ani nijak inak s ním neoprávnene manipulovať.

¹⁴Hoci tieto údaje môžu byť v čase odhalenia kľúča už neaktuálne, môžu pomôcť útočníkovi pri odvodení aktuálnych dát, kompromitovať nás alebo nám inak poškodiť.

¹⁵V praxi to znamená, že elektronický podpis musí byť schopný zabezpečiť aspoň identifikáciu podpisovateľa a schopnosť rozpoznať porušenie integrity podpisu a dokumentu.

Integrita dát: Úzko súvisí so zviazanosťou s dokumentom. Podobne ako sme požadovali skôr nemanipulovať s podpisom, teraz žiadame nemanipulovať s dokumentom.

Autentifikácia: Podpis dokumentu by mal umožniť overiť identitu osoby, ktorá dokument podpísala.

Nepopierateľnosť: Je dôležité, aby autor bol schopný preukázať pravosť podpisu dokumentu (napr. pri súde). Z tohto dôvodu je nutné aby podpisovateľ nebol schopný poprieť podpísanie dokumentu.

Hoci vlastnoručný podpis nesie horeuvedené atribúty, je možné ich relatívne ľahké falšovanie. Závisí na schopnosti a zručnosti overovateľa resp. falšovateľa, či a do akej miery je schopný odhaliť falšovanie podpísaného dokumentu resp. dokument falšovať.

Napr. atribúty zviazanosti s dokumentom a integrity dokumentu je možné falšovať nasledovne. Predstavme si, že máme dokument, ktorý je korektne podpísaný. Chceme v ňom zmeniť časť, ktorá pojednáva o výške sumy, ktorú sa nám osoba podpisujúca dokument zaviazala vyplatiť. Najprv dokument skopírujeme a potom miesto, kde je stanovená výška sumy vybielime pomocou kancelárskeho bielidla. Následne napíšeme novú sumu, ktorá nám vyhovuje. Takto modifikovaný dokument opäť niekoľkokrát skopírujeme, tak aby zmizla na odkopírovanom dokumente stopa použitia bielidla¹⁶. Na záver využijeme notársku službu overovania fotokópií. Ak sa nám podarí presvedčiť pracovníčku notárskeho úradu aby dokument overila máme platne podpísaný dokument¹⁷. Analogicky sa dá manipulovať aj s podpisom a preniesť ho z jedného dokumentu na druhý.

Samozrejme toto nie je jediný spôsob ako falšovať papierové dokumenty. Preto sa v praxi pri podpisovaní dôležitých dokumentov využíva štatút svedka. Táto osoba (dôveryhodná tretia strana napr. notár) potom môže dosvedčiť, že obe strany boli s obsahom dokumentu oboznámené a že ho podpísali z vlastnej vôle.

Elektronický podpis realizovaný pomocou digitálneho podpisu za vhodných podmienok poskytuje vyššiu úroveň zabezpečenia dokumentu a lepšiu zviazanosť s jeho podpisovateľom ako vlastnoručný popis. Aj preto sa pozrieme v nasledujúcej časti bližšie nato ako fungujú digitálne podpisy.

¹⁶Proces kopírovania papierového dokumentu je stratový. Znamená to, že detaily ako jemné okraje a textúry zanechané bielidlom sa neodkopírujú úplne presne a postupným opakovaním kopírovania úplne zmiznú.

¹⁷Z vlastnej skúsenosti môžem povedať, že pracovníčky notárskeho úradu sa príliš nezaťažovali overením obsahu fotokópií mojich vysvedčení ...

3.3.2 Realizácia digitálnych podpisov

Digitálne podpisy sú kryptografické konštrukcie ktorých cieľom je zabezpečiť vlastnosti klasického podpisu v digitálnom svete počítačov.

Na rozdiel od papierových dokumentov je kopírovanie digitálnych dokumentov jednoducho realizovateľné. Preto digitálny podpis nesmie závisieť len na identite podpisujúceho ale aj na obsahu dokumentu. Inak by bolo možné digitálny podpis falšovať jednoduchým kopírovaným z jedného dokumentu do druhého. Z hľadiska realizácie by mali digitálne podpisy spĺňať nasledovné kritériá:

1. **efektívnosť** – Používateľ je schopný efektívne vytvoriť podpis digitálneho dokumentu, za pomoci digitálneho dokumentu, vstupných parametrov podpisového algoritmu a algoritmu samotného. Používateľ môže pritom využiť rôzne technologické prostriedky, ktoré mu proces podpisovania zjednodušia prípadne umožnia znížiť pravdepodobnosť úspešného falšovania podpisu.
2. **dostupnosť** – Overovateľ je schopný overiť platnosť podpisu, za pomoci dokumentu, jeho podpisu, vstupných parametrov overovacieho algoritmu a algoritmu samotného. Podobne ako pri podpisovaní aj tu môže používateľ využiť rôzne technologické prostriedky.
3. **bezpečnosť** – Nikto nie je schopný efektívne falšovať digitálny podpis, za predpokladu že má k dispozícii len ohraničené prostriedky a nezíska prístup k súkromným (tajným) vstupným parametrom, ktoré používa tvorca digitálneho podpisu.

Pre splnenie týchto kritérií sa v súčasnosti používajú tzv. *podpisové schémy*. Podpisová schéma je zvyčajne založená na asymetrickom šifrovacom systéme. Obsahuje *overovací* – $ver_{K_{public}}(x)$ algoritmus a *podpisový* – $sig_{K_{private}}(x)$ algoritmus.

Formálne sa dá opísať podpisová schéma nasledovne:

Definícia 3.3.1 *Podpisová schéma* je päťica $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ pričom:

1. \mathcal{P} je konečná množina možných **otvorených textov**.
2. \mathcal{A} je konečná množina možných **podpisov**.
3. \mathcal{K} je konečná množina možných **kľúčov**.
4. \mathcal{S} a \mathcal{V} sú množiny odkiaľ vyberáme podpisový resp. overovací algoritmus pričom:

5. Pre každé $K_{private}, K_{public} \in \mathcal{K}$ existuje **podpisový algoritmus** $sig_{K_{private}} \in \mathcal{S}$ a korešpondujúci **overovací algoritmus** $ver_{K_{public}} \in \mathcal{V}$. Pričom
- $$sig_{K_{private}} : \mathcal{P} \rightarrow \mathcal{A}$$
- $$ver_{K_{public}} : \mathcal{P} \times \mathcal{A} \rightarrow \{0, 1\}$$
- a pre každý otvorený text $x \in \mathcal{P}$ a každý podpis $y \in \mathcal{A}$ platí
- $$ver_{K_{public}}(x, y) = \begin{cases} 1 & \text{ak } y = sig_{K_{private}}(x), \\ 0 & \text{ak } y \neq sig_{K_{private}}(x). \end{cases}$$

Keďže na realizáciu podpisovej schémy sa zväčša používajú asymetrické šifrovacie systémy, ani tu nie je možné dosiahnuť absolútnu bezpečnosť. Eva je schopná vyskúšať všetky možné podpisy y pre danú správu x a hľadať taký podpis ktorý by vyhovoval. Takže v prípade neobmedzeného času a prostriedkov Eva dokáže sfaľšovať Braňov podpis. Naším cieľom je znemožniť Eve efektívny spôsob útoku a tak zabezpečiť že podpisová schéma bude výpočtovo bezpečná.

Hašovacie funkcie – Digitálny odtlačok

Vzhľadom na to že sa v podpisových schémach používajú asymetrické kryptosystémy, ktoré sú výpočtovo zložité, podpisovanie (šifrovanie) celého dokumentu by bolo neefektívne. V skutočnosti sa namiesto dokumentu podpisuje jeho *digitálny odtlačok*.

Digitálny odtlačok H je obraz dokumentu M zobrazený pomocou *hašovacej funkcie* h : $H = h(M)$. Zvyčajne sú hašovacie funkcie definované na potencionálne nekonečnej množine pričom obor hodnôt býva konečný.

Z hľadiska bezpečnosti je nutné aby hašovacia funkcia bola *jednosmerná*. V praxi to znamená že funkcia h je ťažko invertovateľná t.j. k danému H nevieme efektívne nájsť M tak aby platilo $H = h(M)$.

Bolo by príjemné keby každý odtlačok jednoznačne určoval správu. Zabránilo by to možnosti nájsť správu s rovnakým odtlačkom a tak predstierať odtlačok inej správy. Táto vlastnosť je ale pri našich požiadavkách na hašovaciu funkciu nerealizovateľná¹⁸. Preto požadujeme o čosi slabšiu ale v praxi postačujúcu vlastnosť – *odolnosť voči kolíziám*. V prípade že nevieme efektívne nájsť M_1 a M_2 tak, že $h(M_1) = h(M_2)$ hovoríme o funkcii h , že je odolná voči kolíziám.

Na záver je potrebné dodať, že očakávame že funkcia h bude efektívne algoritmicky realizovateľná.

Je ľahko vidieť, že takto definovaná funkcia h zachováva výpočtovú bezpečnosť týkajúcu sa integrity dokumentu.

¹⁸Injektívne zobrazenie z množiny s väčšou mohutnosťou do množiny s menšou mohutnosťou neexistuje.

Podpisovanie a overovanie správy M prebieha nasledovne:

- 1) Braňo vytvorí správu M
- 2) Použije h na vytvorenie odtlačku Z : $M \xrightarrow{h} Z$
- 3) Z podpíše pomocou podpisového algoritmu $Z \xrightarrow{sig_{K_{private}}} S$
- 4) Braňo pošle Anne dvojicu (M, S)
- 5) Anna prijme správu
- 6) Pre overenie Anna vytvorí $Z' = h(M)$ a overí že $ver_{K_{public}}(Z', S) = 1$.

Výhoda využitia hašovacej funkcie spočíva nielen v zrýchlení procesu podpisovania a overovania dokumentu ale aj v zvýšení bezpečnosti. Viac sa o tejto tematike čitateľ môže dočítať v [3], [5] a v prílohe.

Príklad realizácie podpisovej schémy

Jedným z príkladov vyhovujúcim špecifikácii podpisových schém založených na asymetrických kryptosystémoch, je podpisová schéma založená na šifrovacom systéme RSA. V stručnosti teraz popíšem princíp fungovania schémy. Ak by mal čitateľ záujem o presnú definíciu schémy a detaily implementácie, môže ich nájsť v prílohe.

Braňov proces podpisovania prebieha nasledovne:

- 1) Braňo si vyberie dokument M , ktorý chce podpísať.
- 2) Braňo pomocou svojho súkromného kľúča zašifruje digitálny odtlačok tohto dokumentu. Teda. $C = e_{K_{B_{private}}}(h(M))$ ¹⁹.
- 3) C je teraz platný podpis dokumentu M .
- 4) Braňo pošle Anne dvojicu (M, C) , ktorá reprezentuje podpísaný dokument M .

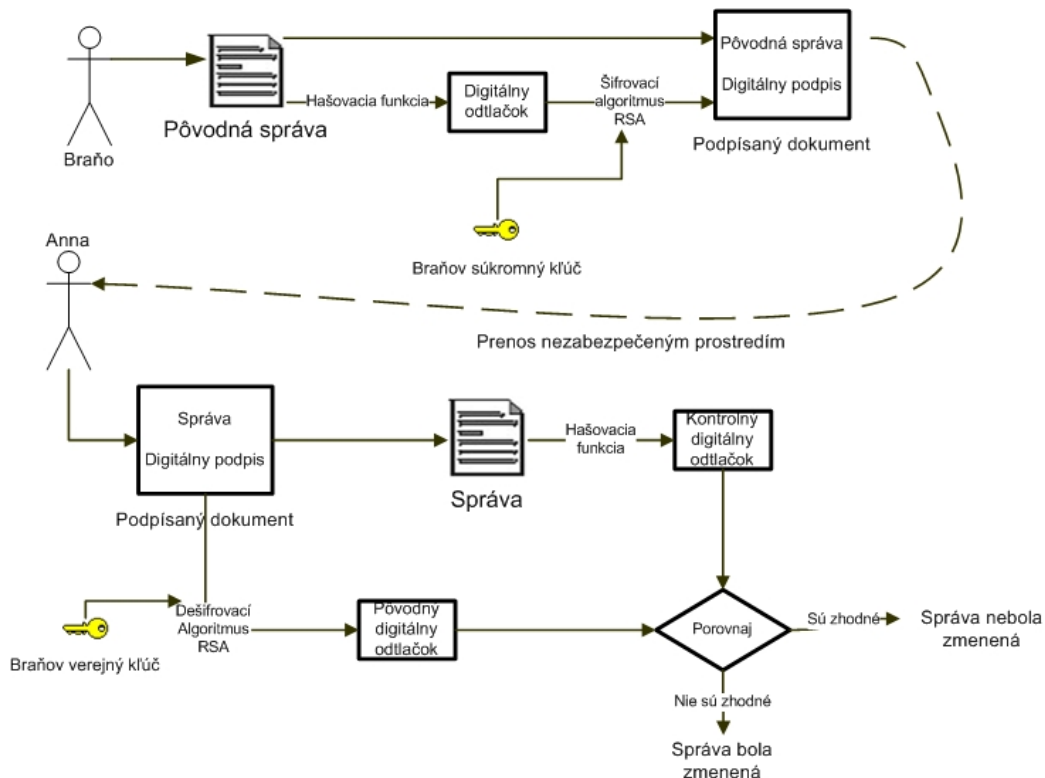
Annin proces overovania prebieha nasledovne:

- 1) Anna prijíme podpísaný dokument (M, C) .
- 2) Anna získa z dôveryhodného zdroja Braňov verejný kľúč – $K_{B_{public}}$.

¹⁹Dá sa povedať, že šifrová transformácia kryptosystému RSA nám teraz slúži ako podpisový algoritmus a súkromný kľúč slúži ako tajný vstupný parameter tohto algoritmu.

- 3) Anna vypočíta $H' = d_{K_{B_{public}}}(C)$, t.j. dešifruje²⁰ pomocou Braňovho verejného kľúča správu C .
- 4) Následne overí či $H' = h(M)$. Ak áno podpisu dôveruje, ak nie podpis vyhlási za falzifikát.

Tieto procesy sú ilustrované na obrázku 3.3.



Obrázok 3.3: Model procesu podpisovania a overovania dokumentu pri použití podpisovej schémy založenej na kryptosystéme RSA

Je zrejmé, že táto realizácia podpisovej schémy spĺňa podmienky, ktoré sme si uviedli na začiatku tejto sekcie. Efektívnosť a dostupnosť priamo plynú z efektívnosti a dostupnosti kryptosystému RSA. Čo sa týka bezpečnosti, tá je zaručená tým, že Braňo používa svoj súkromný kľúč na vytvorenie podpisu. Keďže transformácie šifrovania a dešifrovania sú v kryptosystéme RSA navzájom inverzné, bezpečnosť tohto riešenia je ekvivalentná bezpečnosti dešifrovania (v prípade ak používame kryptosystém RSA na šifrovanie

²⁰Dá sa povedať, že dešifrovanie pomocou RSA nám teraz slúži ako časť overovacieho algoritmu a verejný kľúč slúži ako jeho vstupný parameter.

komunikácie). Táto je všeobecne uznávaná ako dostatočná, t.j. ak Anna posla šifrovanú správu Braňovi, tak za predpokladu, že protivník neodhalil jeho tajný kľúč, prípadne nemá k dispozícii neobmedzené množstvo prostriedkov, protivník nie je schopný túto správu dešifrovať.

3.3.3 Porovnanie klasického a digitálneho podpisu

Spôsob podpisovania

Spôsob vytvorenia vlastnoručného a digitálneho podpisu je značne rozdielny proces.

Vlastnoručný podpis nesie biometrické charakteristiky podpisujúceho, a takto umožní spojenie podpisujúcej osoby a dokumentu. Proces jeho tvorby je triviálny a zaberie len málo času.

Naopak proces tvorby digitálneho podpisu je podstatne zložitejší. Napriek tomu sú situácie keď vytvorenie digitálneho podpisu je oveľa výhodnejšie a podstatne urýchli komunikáciu²¹.

Digitálny podpis nenesie biometrické charakteristiky podpisujúceho a môže ho vytvoriť hocikto kto pozná súkromný kľúč. Preto je potrebné zabezpečiť zviazanie podpisovateľa s dokumentom iným spôsobom.

Metóda podpisovania použitá pri digitálnej forme podpisu vyžaduje špeciálny hardvér alebo aspoň osobný počítač. Keby prišlo k súdnemu procesu tak argument typu "Ja som nepodpísal tento dokument to moje pero." by pravdepodobne vyvolal skôr všeobecné pobavenie. Napriek tomu argument "Ja som nepodpísal tento dokument to môj počítač" znie oveľa zmyslupľnejšie a dôveryhodnejšie. Existujú vírusy, trójske kone a iné škodlivé programy, ktoré sú schopné za istých predpokladov²² vytvoriť platný podpis dokumentu, o ktorom používateľ nevie a s obsahom dokumentu nemusí súhlasiť. Týmto hrozbám je z časti venovaný článok [9].

Spôsob overovania

Súdny znalci grafológie bežne pri overovaní porovnávajú viac vzoriek platných podpisov a hľadajú známky falšovania ako napr.

- Podpisy napísané rýchlosťou ktorá je podstatne nižšia ako pri originálnych podpisoch.

²¹Napr. použitie elektronickej pošty.

²²Použitie obyčajného osobného počítača bez špeciálnych zariadení určených na vytvorenie digitálneho podpisu, neaplikovanie bezpečnostných záplat na tento počítač, absencia aktualizovaného antivírusu na tomto počítači, ...

- Častá zmena tlaku pera na podpisovaný dokument.
- Tupé konce a začiatky liniek.
- Rozdielne vedenie písmen, ich spojov, diakritických znamienok a spôsobu kladenia interpunkcie.
- Manipulácia s dokumentom: retušovanie, zmazanie časti dokumentu.
- Neočakávané zastavenie písma kde by malo byť spojité.

Postup znalca pri analýze dokumentu sa nesmie opierať o tvar písma (to to zvyčajne býva prvoradá vec falšovateľa) ale musí sa sústrediť najmä na tlak písma, veľkosť písma, hustotu písmen, rozdeľovanie slov a mnoho iných vlastností písma. Viac o spôsobe overovania podpisov a grafológii je možné nájsť v [10].

Ako vidno posudzovanie platnosti rukou písaného podpisu závisí vo veľkej miere na technických schopnostiach človeka overujúceho podpis. Určite je možné pre experta úspešne sfalšovať rukou písané dokumenty. Napriek tomu sa klasické podpisy naďalej používajú. Pre prípady vyžadujúce vyššiu bezpečnosť je možné proces podpisovania zviazať za pomoci očitých svedkov.

Na rozdiel od klasických podpisov overenie digitálneho podpisu nezávisí od schopnosti overovateľa a je to čisto technická záležitosť. Overovanie digitálneho podpisu je proces založený na presných matematických procedúrach. Výhodou je, že sfalšovať digitálny podpis je oveľa ťažšie. Nevýhodou je nemožnosť rozlíšenia falšovaného a originálneho podpisu. V prípade že podpis bol falšovaný, neexistuje expert ktorý by to zistil, tzn. že podpis je falšovaný dokonale.

Problémy implementácie digitálnych podpisov

Z implementačného hľadiska má digitálny podpis ďalšiu nevýhodu. Z hľadiska dlhodobej archivácie digitálneho dokumentu sa vynárajú tieto problémy:

- Poškodenie média na ktorom je dokument uložený.
- Zastaranosť formátu dokumentu.
- Vývoj kryptografických algoritmov a štandardov.

Prvý problém nie je až taký závažný. V prípade že sú médiá uložené v ideálnych podmienkach vydržia okolo sto rokov (čo je síce menej ako papier ale z hľadiska zvyšných dvoch problémov postačujúce).

Problém s formátom by sa mohol odstrániť využívaním len jednoduchých textových dokumentov. Tento formát vydržal už dlhý čas vďaka svojej jednoduchosti. Na rozdiel od formátov, ktoré síce ponúkajú (mnohokrát zbytočnú) vyššiu funkcionality, nepodlieha časovej skaze. Jasným príkladom sú dokumenty vytvorené zastaranými textovými procesormi pod operačným systémom *DOS*, ktoré sú v súčasnosti mnohokrát nečitateľné z dôvodu chýbajúceho softvéru alebo hardvéru.

Druhý spôsob ako tento problém riešiť je periodická konverzia formátov. Avšak po konverzii je nutné dokument opäť podpísať čo býva nepohodlné a často aj nemožné.

Tak ako formáty dokumentov aj podpisové algoritmy a hašovacie funkcie časom zastarajú. Pred nedávnom sa našli kolízie v hašovacej funkcii *MD5*²³ ktorá sa aj napriek upozorneniam odborníkom naďalej dosť používa. Existuje aj možnosť odhalenia podpisového kľúča či už pomocou rozbitia algoritmu alebo iným spôsobom (ukradnutie, vydieranie, ...). Riešením týchto a iných problémov sa budeme zaoberať v nasledujúcej kapitole.

²³http://cryptophy.hyperlink.cz/2004/kolize_hash.htm

Kapitola 4

Teória a prax digitálneho podpisu

4.1 Administratívne problémy digitálnych podpisov

Okrem technických problémov spojených s používaním digitálneho podpisu sa vynárajú aj administratívne problémy. Predstavme si, že Braňo chce komunikovať s Annou. Braňo podpíše dokument a pošle ho. Teraz Braňo musí zverejniť svoj overovací kľúč. Následne vzniká problém: "Ako zistiť či je zverejnený kľúč naozaj Braňov? ".

Existuje mnoho spôsobov zverejnenia verejného kľúča napr. zverejnenie na internetovej stránke, poslanie pomocou elektronickej pošty prípadne osobné doručenie. Tieto spôsoby sú však buď ťažko realizovateľné (osobné dodanie) alebo ľahko manipulovateľné Evou. Navyše v prípade, že Anna Braňa nepozná ako môže určiť či zverejnená internetová stránka je naozaj Braňova? A nakoniec v prípade kompromitácie súkromného kľúča je nutné oboznámiť širokú verejnosť s týmto faktom. Toto je pre Braňa prakticky nerealizovateľné.

V stručnosti by sa dali tieto problémy zhrnúť do troch bodov:

1. Spoľahlivá distribúcia verejných kľúčov.
2. Prepojenie verejného kľúča a identity jeho držiteľa.
3. Kompromitácia súkromného kľúča.

4.2 Infraštruktúra verejných kľúčov

Riešenie týchto problémov je ťažké. Vyžaduje si vybudovať infraštruktúru ktorá umožní identifikovať používateľov, spojiť ich s ich verejnými kľúčmi,

spoľahlivo distribuovať údaje o používateľoch, archivovať tieto údaje a v neposlednom rade riešiť problémy s kompromitáciou relevantných údajov. Vzhľadom na to, že táto infraštruktúra sa týka najmä verejných kľúčov používateľov, budeme ju nazývať *infraštruktúrou verejných kľúčov* – *Public Key Infrastructure* – *PKI*.

4.2.1 Základné pojmy PKI

V tejto časti sa budeme venovať základným pojmom vyskytujúcich sa v PKI. Cieľom je priblížiť ich funkciu a opísať procesy s nimi spojené. Z dôvodu rozsiahlosti tejto tematiky sa nebudeme venovať presnej syntaxi a formátom jednotlivých dokumentov. Tie môže čitateľ nájsť v prílohe.

Certifikát

Na spojenie identity podpisovateľa a jeho verejného kľúča slúži *certifikát*. Certifikát je vydávaný *certifikačnou autoritou*.

Držiteľ je v certifikáte identifikovaný pomocou mena, adresy, elektronickej pošty prípadne iných informácií. Certifikačná autorita by mala overiť platnosť týchto údajov, napr. tak že bude žiadať nejaký doklad na overenie totožnosti žiadateľa. Používateľ môže požiadať aj o anonymný certifikát, kde bude identifikovaný na základe pseudonymu. Certifikačná autorita mu môže takýto certifikát vydať za predpokladu, že vo vydanom certifikáte jasne uvedie, že ide o pseudonym a za predpokladu, že bude poznať skutočnú identitu žiadateľa.

Každý certifikát má unikátne sériové číslo (v rámci certifikačnej autority), a identifikátor certifikačnej autority, ktorá ho vydala.

Certifikát je digitálne podpísaný patričnou certifikačnou autoritou. Dôvodom je potreba zachovať integritu údajov obsiahnutých v certifikáte. Ak je podpis certifikačnej autority platný, overovateľ si môže byť istý, že údaje na certifikáte sú pravé a že neboli nikým manipulované. Vzhľadom na možnosť použiť rôzne podpisové schémy, je nutné pripojiť aj informáciu o algoritme použitom certifikačnou autoritou pri podpisovaní certifikátu.

Overovanie platnosti podpisu certifikátu prebieha na základe verejného kľúča certifikačnej autority. Táto zverejní kľúč na viacerých nezávislých miestach (napr. na svojej internetovej stránke, v tlači alebo ho vyteše na základný kameň svojej budovy ☺), aby nebolo možné kľúč zameniť.

Ako už bolo spomenuté, asymetrické šifrovacie systémy nie sú absolútne bezpečné, preto je potrebné aby platnosť certifikátu bola obmedzená. Tento údaj musí byť súčasťou certifikátu.

Dokumenty podpísané súkromným kľúčom prislúchajúcim k verejnému kľúču uvedenému na certifikáte po dobe vypršania tohto certifikátu sú neplatné. Týmto spôsobom sa zaručí preventívna ochrana¹, pred vypočítaním resp. uhádnutím súkromného kľúča zodpovedajúceho verejnému kľúču, ktorý je uvedený v certifikáte.

V prípade, že si používateľ želá, aby bolo možné overiť platnosť podpisu dokumentu aj po vypršaní platnosti certifikátu je dobré aby využil službu certifikačnej autority, ktorá pripojí k dokumentu časovú pečiatku. Služba časových pečiatok slúži na zviazanie dokumentu a dátumu resp. času kedy bol dokument vytvorený.

Samozrejme certifikát obsahuje aj verejný kľúč prislúchajúci k súkromnému kľúču používateľa.

Okrem týchto základných informácií, certifikát obsahuje aj nepovinné pole – rozšírenia (extenzie). Extenzie sa dajú vo všeobecnosti rozdeliť na kritické a nekritické. Extenzia, ktorá je označená ako kritická musí byť korektne spracovaná a vyhodnotená², inak nesmie byť certifikát použitý.

Extenzie môžu určovať napríklad na aký účel sa môže používať súkromný kľúč ku ktorému prislúcha verejný kľúč uvedený v certifikáte³, môžu špecifikovať reťaz dôvery – postupnosť certifikačných autorít, môžu určovať akým spôsobom a odkiaľ je možné získať zoznam revokovaných certifikátov a môžu určovať mnoho iných atribútov spätých s používaním certifikátu, alebo s identitou vydavateľa alebo s identitou držiteľa.

Všetky tieto informácie sú uložené v štandardnom formáte *X.509*, ktorého štruktúru ilustrujem na obrázku 4.1. Bližšiu špecifikáciu formátu certifikátov a ich obsahu možno nájsť v prílohe. Proces spojený so žiadosťou o vydanie a samotným vydávaním certifikátov bude opísaný v sekcii 4.2.2.

Zoznamy zneplatnených certifikátov

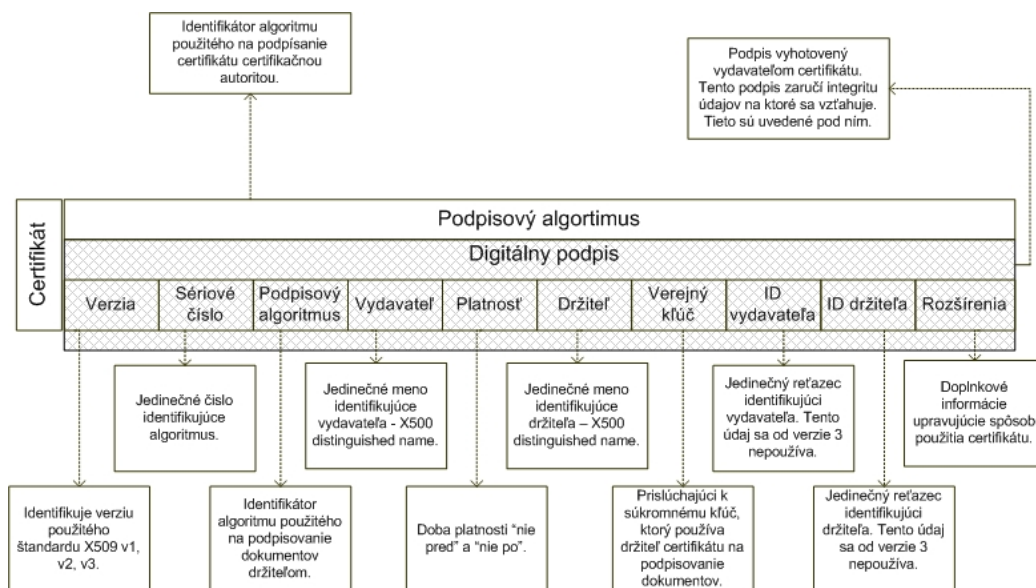
Platnosť certifikátu sa môže skončiť prirodzeným vypršaním času na ktorý bol certifikát vydaný, alebo predčasným zneplatnením certifikátu. Dôvodov kedy je nutné zneplatniť certifikát je viacero:

- Certifikát nebol vydaný v súlade s platnou legislatívou.

¹Predpokladáme, že útočník nebude schopný uhádnuť kľúč skôr ako skončí platnosť certifikátu. Z tohto dôvodu je platnosť certifikátu pomerne krátka – cca. 1 rok.

²Aplikáciou, ktorá prichádza do styku s certifikátom, napr. poštový klient pri overovaní digitálneho podpisu prijatej pošty.

³Koncový používateľ môže využiť súkromný kľúč v podstate len na vytváranie digitálnych podpisov alebo na šifrovanie. Pokiaľ ide o poskytovateľov certifikačných služieb – CA, tie môžu použiť súkromný kľúč aj na zaručenie integrity nejakej služby napr. podpísanie CRL, časovej pečiatky, alebo vydaných certifikátov.



Obrázok 4.1: Štruktúra formátu certifikátu X.509

- Certifikát bol vydaný na základe nepravdivých údajov.
- Vlastník certifikátu explicitne požiada o jeho zrušenie napr. z dôvodu zmeny údajov uvedených na certifikáte.
- V prípade úmrtia držiteľa certifikátu.
- V prípade kompromitácie súkromného kľúča patriaceho k verejnemu kľúču uvedenému na certifikáte.

Keď príde k predčasnému zneplatneniu certifikátu, je povinnosťou certifikačnej authority, ktorá certifikát vydala, upovedomiť používateľov certifikačných služieb o revokácii certifikátu. Existuje viacero možností ako zabezpečiť túto službu. V praxi sa používajú dva základné spôsoby – "on-line" a "off-line".

"On-line" spôsob umožňuje takmer v reálnom čase overiť či certifikát nebol revokovaný. Táto schopnosť závisí od hardvéru, pomocou ktorého je služba poskytovaná, infraštruktúry podniku ktorý službu poskytuje a čerstvosti informácií ktoré sú k dispozícii.

Príkladom takejto "on-line" služby je implementácia Online Certificate Status Protocol – OCSP.

Treba poznamenať, že OCSP neurčuje či bol v danom čase certifikát platný, ale hovorí len o tom či bol v danom čase certifikát revokovaný alebo nie.

Je na používateľovi aby overil či platnosť certifikátu nevypršala, či bola zachovaná reťaz dôvery medzi certifikačnými autoritami, či neboli porušené kritické obmedzenia kladené na certifikát a či je podpis vydavateľa platný.

Problémom pri implementácii OSCP je potreba aby služba bola stále dostupná. Z toho dôvodu je OSCP náchylný na rôzne formy *DoS* útokov a *replay* útokov⁴. Preto je potrebné, aby v prípade výpadku služby bolo k dispozícii záložné riešenie.

Jednoduchšie riešenie, menej náročné na zabezpečenie a prevádzku je *off-line* služba vydávania zoznamu zneplatnených certifikátov – Certificate Revocation List – CRL. Táto služba je poskytovaná certifikačnou autoritou, ktorá je zodpovedná za revokáciu príslušných certifikátov. Zoznam zneplatnených certifikátov je vydávaný periodicky. Interval ako často vydáva certifikačná autorita CRL je stanovený jej certifikačným poriadkom.

Zoznam musí byť podpísaný príslušnou certifikačnou autoritou aby sa predišlo jeho neautorizovanej manipulácii a musí byť dostupný za akýchkoľvek podmienok všetkým používateľom.

CRL podobne ako certifikát má svoj štandardný formát. Každé CRL musí obsahovať meno vydavateľa, dátum a čas týkajúci sa vydania CRL, ako aj dátum a čas vydania najbližšieho plánovaného CRL. Vydavateľ CRL musí vydať najbližšie CRL najneskôr pred uplynutím tohto dátumu.

Po týchto údajoch nasleduje najpodstatnejšia časť CRL – zoznam zrušených certifikátov. Každá položka tohto zoznamu povinne obsahuje sériové číslo certifikátu a dátum a čas zrušenia certifikátu. Voliteľne môže obsahovať neprázdny zoznam rozšírení, ktoré upresňujú dôvod zrušenia certifikátu.

CRL obsahuje zoznam rozšírení (extenzií), podobne ako je to pri certifikáte. Medzi tieto extenzie patria napr. poradové číslo CRL, rámec pôsobnosti CRL⁵ (CRL scope), zoznam entít pre ktoré je dané CRL určené, atribút indikujúci či ide o prírastkové CRL, a iné.

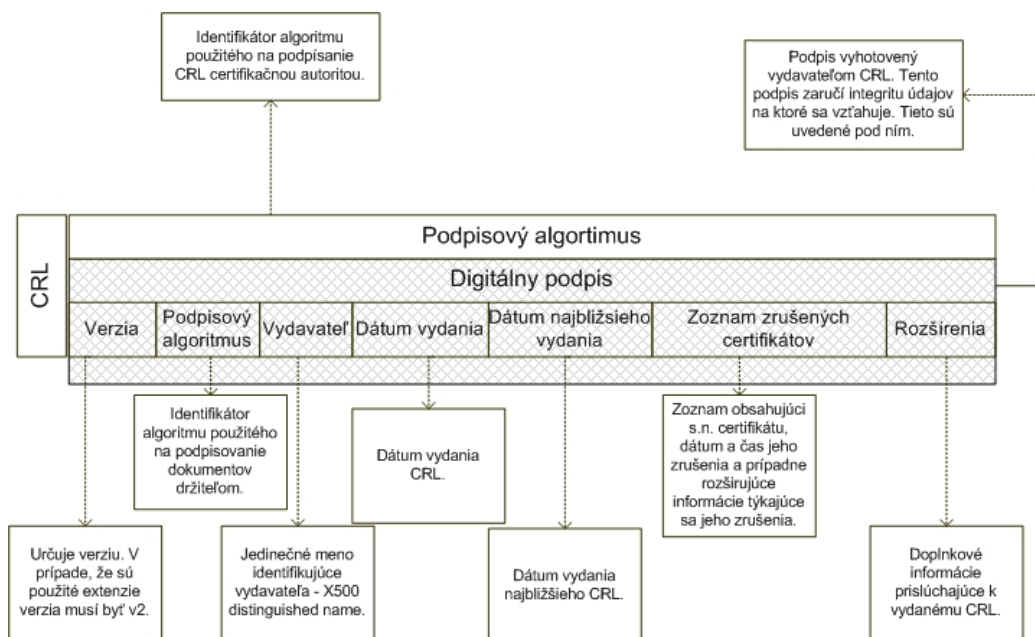
Vzhľadom na možnú rozsiahlosť zoznamu zrušených certifikátov existujú dva základné typy CRL: úplný a prírastkový.

Úplné CRL obsahuje zoznam všetkých certifikátov, ktoré boli zneplatnené a nevypršala im doba platnosti. Výhodou tohto riešenia je, že máme všetky zneplatnené certifikáty spolu a nemusíme spravovať viacero zoznamov. Nevýhodou môže byť zložitá distribúcia takéhoto zoznamu, v prípade veľkého množstva zrušených certifikátov.

Naopak prírastkové CRL obsahuje len zoznam certifikátov, ktoré boli zrušené po vydaní predchádzajúceho CRL a nevypršala im doba platnosti. Prí-

⁴Pozri [18].

⁵Táto extenzia slúži na potencionálne štruktúrovanie vydaných CRL na základe rôznych kritérií, napr. sériových čísel certifikátov, dôvodu ich zneplatnenia, apod.



Obrázok 4.2: Štruktúra formátu CRL

rastkové CRL musí mať vo svojej extenzii nastavený atribút, ktorý indikuje, že ide o prírastkové CRL. Tento atribút musí byť označený ako kritický.

Proces vydávania CRL bude opísaný v sekcii 4.2.2. Bližšie informácie o formáte a obsahu CRL možno nájsť v prílohe.

Časová pečiatka

Predstavme si situáciu keď Braňo chce od Anny získať niečo cenné za čo je ochotný zaplatiť resp. ponúknuť nejakú protislužbu. Braňo môže svoju vôľu potvrdiť elektronickým dokumentom, ktorý digitálne podpíše. Anna Braňovi uverí a službu poskytne. Následne Braňo požiada svoju certifikačnú autoritu o revokovanie certifikátu z dôvodu kompromitácie súkromného kľúča. Teraz Anna nemôže dokázať, že dokument ktorý obdržala od Braňa bol podpísaný v čase keď bol ešte Braňov certifikát platný. Riešením sú *časové pečiatky* – *time stamps*.

Ďalším dôvodom využitia časových pečiatok je možnosť preukázať platnosť digitálneho podpisu aj po uplynutí doby platnosti k nemu prislúchajúcemu certifikátu. V tomto prípade je možné dôveryhodne preukázať, že dokument bol podpísaný v deklarovanom čase a teda nemohol byť neskôr falšovaný útočníkom.

Časová pečiatka T slúži na dokázanie:

1. **aktuálnosti** – T bola vytvorená v časovom okamžiku t_1 .
2. **existencie** – T bola vytvorená pred časom t_2 .
3. **poradia** – časová značka T bola vytvorená pred časovou značkou S .

Časovú pečiatku vydáva autorita nato určená – obvykle certifikačná autorita. Časová pečiatka je informácia spojená s dokumentom za účelom presnej identifikácie dátumu a času vytvorenia dokumentu a spĺňa nasledovné kritériá:

- Je vytvorená na základe dôveryhodného zdroja času, ktorý je synchronizovaný s nejakým oficiálnym zdrojom času.
- Je vytvorená len na základe platnej žiadosti.
- Je vytvorená v súlade s politikou časových pečiatok.
- Je s dokumentom jasne zviazaná.

Zachovanie integrity časovej pečiatky zaručí jej vydavateľ (CA) tak, že ju digitálne podpíše. Vydavateľ musí zverejniť príslušný certifikát, aby umožnil overiť platnosť pečiatky.

Proces vydávania časových pečiatok bude opísaný v sekcii 4.2.2. Viac o časových pečiatkach možno nájsť v [2], prípadne [22].

Certifikačná autorita

Inštitúcia vydávajúca certifikáty verejných kľúčov, zabezpečujúca ich distribúciu a revokovanie sa nazýva *certifikačná autorita* – CA.

CA je tzv. *dôveryhodnou treťou stranou*, čo znamená, že Anna a Braňo veria že certifikáty, ktoré CA vydala a podpísala obsahujú len pravdivé, úplné a aktuálne údaje.

Certifikačná autorita hraje významnú úlohu v rámci infraštruktúry verejných kľúčov. Certifikačná autorita musí poskytnúť klientom množstvo služieb spätých so správou certifikátov. Vzhľadom na rozsiahlosť tejto témy jej budeme venovať samostatnú časť 4.2.2.

Registračná autorita

Registračná autorita – RA slúži na zabezpečenie kontaktu medzi CA a (potencionálnymi) držiteľmi certifikátov, ktoré táto CA vydala (vydá).

Dalo by sa povedať, že RA je akási "pobočka" CA, kde sa vybavujú formality spojené s registráciou, obnovovaním a revokovaním certifikátov.

Každá certifikačná autorita má niekoľko zmluvne zaviazaných registračných autorít, ktorých hlavným cieľom je komunikácia s koncovým používateľom. Medzi najbežnejšie činnosti registračnej autority patria:

- Prijímanie žiadosti o vydanie certifikátu.
- Overenie totožnosti používateľa.
- Overenie znalosti súkromného kľúča (v prípade že pár kľúčov nie je generovaný príslušnou certifikačnou autoritou).
- Odovzdanie vygenerovaných certifikátov, prípade zariadení ktoré ich uschovávajú (napr. čipové karty alebo USB tokeny).
- Prijímanie žiadostí o zrušenie certifikátu.
- Komunikácia s príslušnou certifikačnou autoritou.

Registračná autorita je zodpovedná za pravdivosť údajov obsiahnutých v žiadostiach o vydanie certifikátu, prípadne jeho zneplatnenie. Tieto žiadosti potom posíla na spracovanie príslušnej certifikačnej autorite.

Za účelom overenia digitálneho podpisu v budúcnosti, môže byť dôležité zistiť ako vznikol príslušný certifikát. Registračná autorita by preto mala archivovať žiadosti pre vytvorenie resp. revokáciu certifikátov.

Držitelia, overovatelia a podpisovatelia

Žiadateľ o certifikát je osoba, ktorá podá žiadosť o vytvorenie certifikátu. Túto žiadosť môže podať priamo certifikačnej autorite, alebo registračnej autorite. Žiadateľ o certifikát je zodpovedný za pravdivosť údajov, ktoré poskytne registračnej alebo certifikačnej autorite.

V niektorých implementáciách PKI je možné aby si používateľ mohol sám generovať kľúče. V tomto prípade je zodpovedný za použitie dostatočne silných algoritmov a vhodného hardvéru.

Držiteľ certifikátu ručí za správne uloženie súkromného kľúča, prislúchajúceho k verejnému kľúču uvedenému na certifikáte, ktoré zabráni jeho kompromitácii. V prípade, že ku kompromitácii súkromného kľúča dôjde, je jeho vlastník zodpovedný za okamžité upovedomenie príslušnej certifikačnej alebo registračnej autority.

Po vypršaní platnosti certifikátu držiteľ certifikátu musí požiadať registračnú autoritu o vydanie nového⁶.

⁶ Samozrejme len v prípade, že bol spokojný s certifikačnými službami a chce ich aj naďalej používať.

Overovateľ digitálneho podpisu je zodpovedný za kontrolu platnosti certifikátu verejného kľúča, slúžiaceho na overenie podpisu dokumentu. Pri tomto akte je povinný sa riadiť smernicami a obmedzeniami⁷, určenými certifikačnou autoritou, ktorá príslušný certifikát vydala. V prípade, že je tento certifikát platný, môže na základe verejného kľúča, ktorý je v ňom uvedený overiť digitálny podpis dokumentu.

Podpisovateľ je osoba, ktorá zodpovedá za vytvorenie digitálneho podpisu. Podpis vytvára pomocou súkromného kľúča, ktorý prislúcha k verejnému kľúču uvedenému v certifikáte. Počas tvorby podpisu sa musí podpisovateľ riadiť certifikačným poriadkom⁸, ktorý vydala príslušná certifikačná autorita.

4.2.2 Úlohy certifikačnej autority

Od typu certifikačnej autority závisí miera plnenia povinností a výška poskytovaných záruk. Je samozrejmé, že národná certifikačná autorita, komerčná certifikačná autorita, či certifikačná autorita ktorá sa stará o školské certifikáty bude mať rozdielnú ponuku služieb a teda aj zodpovedností.

V tejto časti si v hlavných črtách popíšeme procedúry týkajúce sa správy certifikátov, ako aj iné povinnosti, ktoré by mala certifikačná autorita splniť, bez ohľadu na jej typ. Prirodzene miera plnenia týchto povinností sa bude líšiť v závislosti od typu.

Vydávanie certifikátov

Jedna z hlavných úloh certifikačnej autority je vydávanie certifikátov. Pre splnenie tejto funkcie je potrebné:

1. **Identifikovať používateľa** – Certifikačná autorita potrebuje poznať identifikačné údaje žiadateľa bez ohľadu na to či je generovaný certifikát anonymný alebo nie. Komunikáciu so žiadateľom môže certifikačná autorita delegovať na jej registračnú autoritu.

Certifikačná autorita musí prideliť každému novému certifikátu sériové číslo, ktoré bude jednoznačne identifikovať certifikát v rámci certifikačnej autority.

⁷Medzi tieto obmedzenia môžu patriť napr. obmedzenia kladené na spôsob použitia verejného kľúča.

⁸Na jeho základe môžu byť obmedzené prostriedky, ktoré môže podpisovateľ používať napr. môže použiť len bezpečné zariadenia na vytvorenie digitálneho podpisu certifikované nejakým výrobcom alebo spĺňajúce nejaké normy, môže byť obmedzená procedúra ako sa má podpis vytvoriť, apod.

2. **Overiť atribúty kľúča** – Certifikačná autorita musí skontrolovať jedinečnosť páru kľúčov (aspoň v rámci certifikačnej autority), aby sa predišlo kompromitácii súkromného kľúča. V prípade, že už existuje certifikát vydaný s daným verejným kľúčom certifikačná autorita odmietne vydať nový certifikát a existujúci certifikát zneplatní. Samozrejme certifikačná autorita upovedomí držiteľa o zneplatnení certifikátu a vydá mu nový.

Certifikačná autorita by tiež mala overiť či používateľ pozná súkromný kľúč prislúchajúci k verejnému kľúč. Overenie tejto znalosti môže byť založené napr. na podpise nejakého ľubovoľného dokumentu ktorý predloží certifikačná autorita. Samozrejme, že táto kontrola je nutná len v prípade, ak si používateľ generuje kľúče sám.

3. **Zmluvne potvrdiť záväzky** – Na záver je potrebné zmluvne podchytiť existenciu spojenia medzi používateľom a jeho certifikátom. Inak by používateľ bol schopný poprieť svoj digitálny podpis, prípadne by nebol viazaný certifikačným poriadkom vydaným certifikačnou autoritou.

Certifikačná autorita musí pri generovaní nového certifikátu oboznámiť používateľa s certifikačným poriadkom ako aj s certifikačnými politikami a obmedzeniami kladenými na používanie certifikátu. Zároveň je vhodné aby používateľa oboznámila aj so základnými procedúrami vytvárania digitálnych podpisov ako aj s legislatívou s tým spojenou.

Zrušovanie certifikátov

Ako sme už skôr uviedli dôvodov pre revokovanie certifikátov môže byť viacero. Certifikačná autorita musí umožniť dostupnosť služby zrušovania certifikátov 24 hodín denne. Zneplatniť certifikát musí certifikačná autorita **ihneď** po obdržaní autentickej žiadosti o jeho revokovanie. Táto žiadosť zvyčajne býva iniciovaná registračnou autoritou alebo priamo používateľom. Autentickosť žiadosti musí byť bezpodmienečná aby sme predišli *DoS* útokom.

Žiadosť o zrušenie certifikátu možno podať napr. telefonicky, pomocou pošty alebo elektronicky napr. na základe vyplnenia formulára dostupného na internetovej stránke certifikačnej autority. Autenticita žiadosti môže byť v každom z týchto prípadov vyriešená zadaním tajného hesla, ktoré držiteľ certifikátu uviedol v žiadosti o vydanie nového certifikátu.

Certifikačná autorita je povinná viesť dokumentáciu o úspešných aj neúspešných pokusoch o revokovanie certifikátov. Táto dokumentácia musí obsahovať najmä presný dátum a čas prijatia žiadosti o revokáciu certifikátu

resp. zistenia dôvodu pre zrušenie certifikátu, dôvod na zrušenie certifikátu a údaje určujúce osobu ktorá zrušenie certifikátu iniciovala.

Distribúcia zoznamu revokovaných certifikátov

Certifikačná autorita je zodpovedná za distribúciu zoznamu revokovaných certifikátov. CRL musia byť publikované periodicky⁹ a certifikačná autorita musí zabezpečiť aby informácie obsiahnuté CRL boli čo najaktuálnejšie.

Používatelia obvykle získavajú aktuálne CRL z internetovej stránky príslušnej certifikačnej autority. Certifikačná autorita môže navyše poskytovať službu prehľadávania CRL založenú na adresárovej architektúre.

CRL musia byť dostupné širokej verejnosti. Vzhľadom na to, že CRL sú certifikačnou autoritou podpísané, je táto inštitúcia povinná zverejniť svoj príslušný certifikát na **viacerých** miestach, tak aby bolo isté, že bude vždy dostupný.

Podobne ako certifikáty, aj zoznamy zneplatnených certifikátov musia byť zálohované a archivované.

Distribúcia a manažment certifikátov

Certifikačná autorita je zodpovedná za publikovanie verejných certifikátov na adresárovom servri. Nepovinnou službou certifikačnej autority môže byť distribúcia certifikátov priamo k používateľovi. Adresárový server musí byť prístupný pre všetkých používateľov, najmä služba prehliadania zoznamu revokovaných certifikátov, ktorá by mala byť dostupná stále.

Certifikačná autorita tiež prevádzkuje doplnkové služby manažmentu certifikátov. Mala by upozorniť vlastníka certifikátu nejaké obdobie pred prirodzeným vypršaním platnosti certifikátu. Certifikačná autorita tiež musí zálohovať certifikáty pre prípad zlyhania adresárového servra.

Vzhľadom na to, že certifikáty sú certifikačnou autoritou podpísané, je táto inštitúcia povinná zverejniť svoj príslušný certifikát na **viacerých** miestach tak aby bolo isté, že bude vždy dostupný.

Služba časových pečiatok

V niektorých situáciách môže byť dôležité stanoviť kedy vznikol podpis dokumentu. Ide najmä o situácie keď:

1. v priebehu platnosti certifikátu bol tento certifikát zneplatnený. V tomto prípade je potrebné zistiť, či bol podpis vytvorený pred okamžikom zneplatnenia, alebo

⁹Za postačujúcu periódu sa považuje časové rozpätie 12–24 hodín.

2. doba platnosti certifikátu vypršala a je potrebné určiť či podpis vznikol pred vypršaním tejto doby, alebo
3. právne predpisy vyžadujú určenie okamžiku kedy bol dokument podpísaný.

Z horeuvedených dôvodov vidieť, že je potrebné aby certifikačná autorita poskytovala svojim zákazníkom službu vydávania časových pečiatok.

V nasledujúcej časti zjednodušene ilustrujeme proces poskytovania tejto služby. Ak by mal čitateľ záujem, detaily spojené s vydávaním časových pečiatok môže nájsť v [19].

Proces vydávania časovej pečiatky prebieha nasledovne:

1. Žiadateľ o časovú pečiatku vytvorí digitálny odtlačok dokumentu, ktorý chce podpísať.
2. Žiadateľ pošle tento digitálny odtlačok spolu s inými parametrami¹⁰ autorite vydávajúcej časové pečiatky.
3. Certifikačná autorita overí či je formát žiadosti v poriadku. Ak nie, proces vydávania časovej pečiatky ukončí a časovú pečiatku nevydá. O tomto akte neskôr žiadateľa informuje.
4. Ak je formát žiadosti v poriadku, certifikačná autorita vytvorí časovú pečiatku. Zo spoľahlivého zdroja času zistí aktuálny čas a ten spolu s digitálnym odtlačkom zakóduje. Túto správu potom podpíše nato určeným súkromným kľúčom. K tomuto kľúču musí byť vydaný verejne dostupný certifikát, aby bolo možné overiť autenticitu a integritu vydanej časovej pečiatky. Takto podpísanú správu potom odošle žiadateľovi. Táto správa reprezentuje časovú pečiatku.

Dokumentácia, certifikačný poriadok a technická podpora

Vzhľadom na rozsiahlu činnosť certifikačnej autority je potrebné viesť dokumentáciu. Podkladový materiál pozostáva z prevádzkovej dokumentácie, bezpečnostných pravidiel a interných smerníc určujúcich procesy certifikačnej činnosti.

¹⁰Napríklad identifikátor použitej hašovacej funkcie, identifikátor politiky časových pečiatok, "príležitostné slovo – nonce", prípadne iné informácie. Presný formát žiadosti môže čitateľ nájsť v [19]

Prevádzková dokumentácia popisuje pravidlá, na základe ktorých sú riadené procesy spojené s vydávaním a správou certifikátov. V rámci prevádzkovej dokumentácie sú stanovené zodpovednosti, ktoré na seba prevezmú subjekty¹¹ vyskytujúce sa v procesoch súvisiacich s certifikačnými službami.

Najdôležitejšou časťou prevádzkovej dokumentácie je certifikačný poriadok, ktorý popisuje najmä:

- Pre koho a za akých podmienok sú certifikačné služby určené.
- Obmedzenia pri poskytovaní služieb.
- Typy certifikátov poskytovaných certifikačnou autoritou.
- Práva a povinnosti používateľov.
- Pravidlá používania a zneplatňovania certifikátov a procedúry s nimi spojené.
- Spôsob spracovania údajov a ich ochrany.
- Spôsob a rozsah zverejnenia informácií súvisiacich s certifikačnými službami (adresa certifikačnej autority, príslušné certifikáty certifikačnej autority a iné).

Bezpečnostné pravidlá stanovujú mieru zabezpečenia procesov spojených s výkonom certifikačných služieb. Na ich základe si môže zákazník vybrať, či daná certifikačná autorita spĺňa jeho požiadavky na bezpečnosť. Ak certifikačná autorita spracováva citlivé (napr. osobné) údaje, bezpečnostné pravidlá musia spĺňať kritériá určené štátom. Dodržiavanie týchto pravidiel kontroluje štát.

Aj na základe týchto dokumentov je určená právna zodpovednosť certifikačnej autority. Ak nastane problém a certifikačná autorita sa chce vyhnúť postihu, musí dokázať, že sa správala podľa zákona a týchto pravidiel. Aj preto je povinnosť certifikačnej autority viesť dokumentáciu zakotvená v zákone.

Pre zvýšenie svojej konkurencieschopnosti môže certifikačná autorita v rámci centra podpory zriadiť "callcentrum" alebo "helpdesk", ktoré rieši problémy spojené s vytváraním a overovaním digitálnych podpisov. Okrem týchto voliteľných služieb musí poskytnúť aj 24 hodinovú linku, kde môžu držitelia certifikátov svoje certifikáty zneplatniť v prípade potreby.

¹¹Certifikačná autorita, registračná autorita, žiadateľ o certifikát, držiteľ certifikátu, ...

Archivácia

Certifikačná autorita je povinná viesť archív v ktorom bude uchovávať dostatočne dlhú dobu informácie o prevádzkovej dokumentácii certifikačnej autority, podpisových politikách, politikách časových pečiatok, zozname vydaných časových pečiatok, záznamy o synchronizácii času a všetkých výnimočných udalostiach v systéme ako aj archívy vydaných certifikátov a zoznamu zneplatnených certifikátov.

Archív je užitočný pri overovaní podpísaných dokumentov, ktorých príslušné certifikáty už nie sú platné. Archív môže byť využitý aj pri internej alebo externej kontrole.

4.2.3 Model PKI

Pre správne fungovanie PKI nebude stačiť jedna certifikačná autorita. Takto navrhnutá infraštruktúra je nerealizovateľná tak technicky ako aj legislatívne. V prípade, že by sme mali jedinú certifikačnú autoritu, musela by zvládnuť požiadavky širokého spektra používateľov. Tieto by sa menili v závislosti od nárokov na cenu, bezpečnosť a kvalitu riešenia. Certifikačná autorita by preto musela vytvoriť viacero produktov, čo by mohlo byť náročné na technické aj personálne zdroje. Ďalším dôvodom prečo potrebujeme viacero certifikačných autorít je vytvorenie konkurenčného prostredia. Ak by sme mali jedinú inštitúciu poskytujúcu certifikačné služby, mohla by svoje monopolné postavenie zneužívať. No a na záver je potrebné dodať, že ak by išlo o naozaj rozsiahlu PKI, jediná certifikačná autorita by nebola schopná stopercentne poskytovať svoje služby všetkým používateľom.

Ako riešenie sa ponúka vytvoriť viac certifikačných autorít, ktoré budú následne prepojené. Certifikačné autority možno založiť na rozličných princípoch: národné, organizačné, na základe komunít či úrovne zabezpečenia.

Otázka dôvery v certifikát (a teda aj v údaje ktoré sú v ňom uvedené) je dôležitá pre overenie podpisu. Ak certifikát ktorý prislúcha k súkromnému kľúču, pomocou ktorého bol vytvorený podpis nie je pre nás dôveryhodný, ani vytvorený podpis nemôže byť pre nás dôveryhodný. Naša dôvera v certifikát je podmienená dôverou¹² k certifikačnej autorite, ktorá ho vydala.

V prípade keď certifikát ktorý používame pri overení podpisu pochádza od certifikačnej autority, ktorej dôverujeme¹³ a máme jej verejný kľúč postupujeme nasledovne: Overíme si platnosť certifikátu, t.j. overíme si či je podpis na certifikáte platný (pomocou verejného kľúča certifikačnej autori-

¹²Tá môže byť založená na tom, že daná certifikačná autorita spĺňa podmienky na vykonávanie certifikačných služieb uložené zákonom.

¹³Napr. je to certifikačná autorita ktorej služby sami využívame.

ty ktorá ho vydala), overíme si, že certifikát nebol revokovaný, neuplynula doba jeho platnosti a že neboli porušené obmedzenia, ktoré naň uvalil jeho vydavateľ.

V prípade keď je potrebný certifikát vydaný inou certifikačnou autoritou, ktorá je nám neznáma, potrebujeme overiť aj certifikát ktorý prislúcha k súkromnému kľúču, ktorý použila certifikačná autorita na jeho podpísanie. Tento proces sa môže líšiť v závislosti od architektúry prepojenia a modelu dôvery medzi jednotlivými certifikačnými autoritami.

Stromová (hierarchická) architektúra

V prípade stromovej štruktúry PKI, existuje tzv. *koreňová certifikačná autorita* – KCA , ktorá vydáva certifikáty len iným certifikačným autoritám a nie koncovým používateľom. Tie môžu ďalej poskytovať certifikačné služby buď koncovým používateľom alebo iným podriadeným autoritám. Táto architektúra sa dá opísať stromom pričom uzly sú certifikačné autority a listy sú používatelia. Každý používateľ a každá certifikačná autorita pozná verejný kľúč KCA . Na jeho základe možno overiť ľubovoľný certifikát v rámci architektúry.

Väzba medzi CA_i a CA_j spočíva v existencii koreňovej certifikačnej autority CA_r , ktorá je nadradená tak CA_i ako aj CA_j . Anna – klient CA_i vlastní verejný kľúč CA_r a pomocou neho môže overiť certifikát CA_j ktorej klientom je Braňo. Po overení certifikátu CA_j možno overiť aj Braňov certifikát. Reťaz overovania je znázornená na obrázku 4.3.

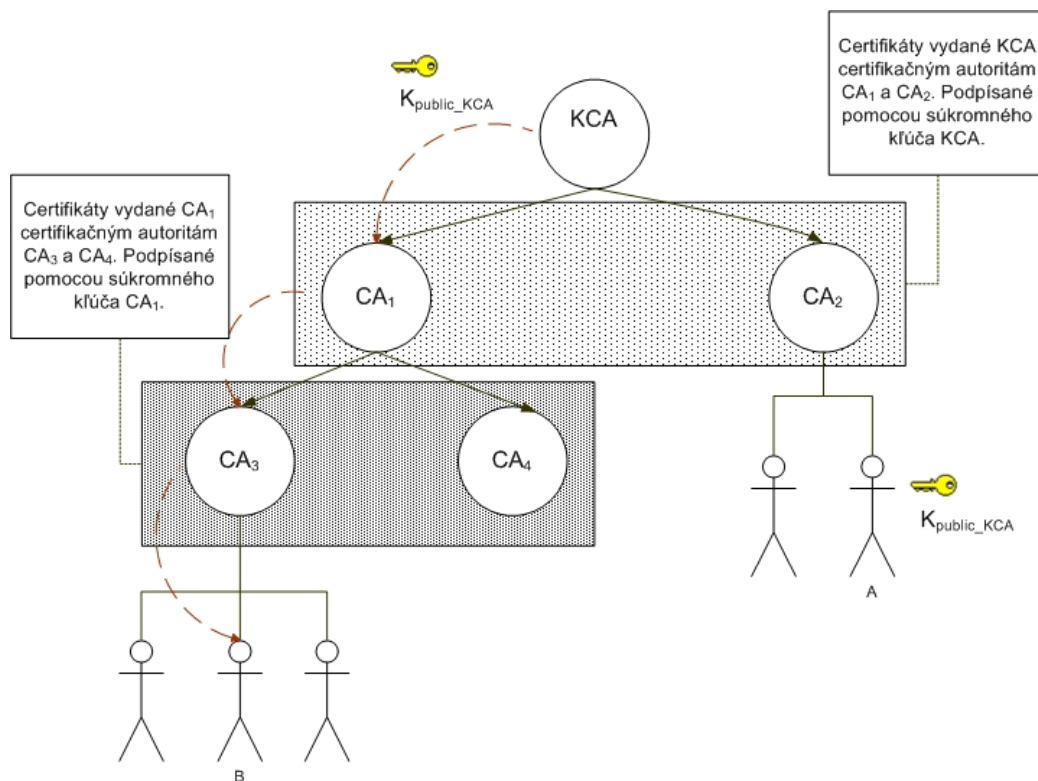
Sieťová (mesh) architektúra

Sieťová architektúra modeluje infraštruktúru ako jednoduchý neorientovaný graf. Jednotlivé certifikačné autority vytvárajú medzi sebou väzbu tak, že si **navzájom** vydávajú certifikáty. Tento proces sa nazýva *krížová certifikácia*.

Väzba medzi CA_i a CA_j vznikne práve vtedy keď medzi nimi existuje cesta v grafe PKI. Takýchto ciest môže existovať viacero. Spôsob overovania je znázornený na obrázku 4.4.

Architektúra a prax

Každá z uvedených architektúr má svoje výhody aj nevýhody. Kým pri hierarchickej architektúre je vydávanie certifikátov iným certifikačným autoritám obmedzené len na bezprostredných "potomkov", v sieťovej architektúre sa môžu vydávať ľubovoľne. Z toho vyplýva, že počet vydaných certifikátov iným certifikačným autoritám v hierarchii je $n - 1$, kým v sieti to môže byť až



Obrázok 4.3: Reťaz overovania Braňovho certifikátu na základe verejného kľúča koreňovej certifikačnej autority

$\binom{n}{2}$. Na druhej strane, v sieťovej architektúre v prípade kompletného grafu možno overiť platnosť certifikátu priamo¹⁴.

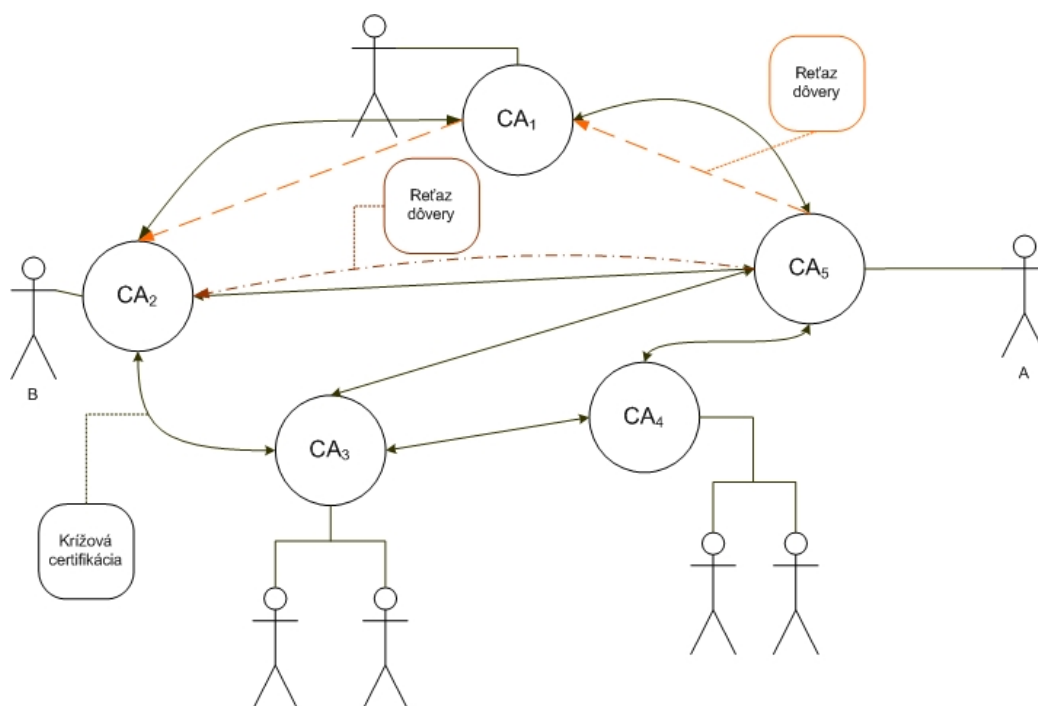
Pri hierarchickej štruktúre sa predpokladá že nadradená CA vydá certifikát len takej CA ktorá spĺňa jej bezpečnostné politiky. Pri sieťovej architektúre možno predpokladať, že sa proces krížovej certifikácie uskutoční len ak obe CA majú porovnateľnú úroveň zabezpečenia.

Pri prepojení už existujúcich PKI možno využiť rôzne prístupy. Možno použiť od počiatku sieťovú architektúru. Na prvý pohľad by sa toto riešenie mohlo pozdávať. Umožňuje vznik najkratších ciest pre overovanie certifikátov¹⁵. Bohužiaľ v prípade krížovej certifikácie väčšieho počtu certifikačných autorít vznikajú problémy s obnovovaním krížových certifikátov ako aj s ich manažmentom. Ďalšou nevýhodou je nejednoznačnosť spočívajúca v potenciálnej existencii viacerých možných ciest medzi jednotlivými CA.

Je možné použiť hybridnú architektúru kde sa budú krížovo certifikovať

¹⁴Vzhľadom na to, že každá certifikačná autorita je krížovo certifikovaná s každou.

¹⁵V prípade použitia kompletného grafu.

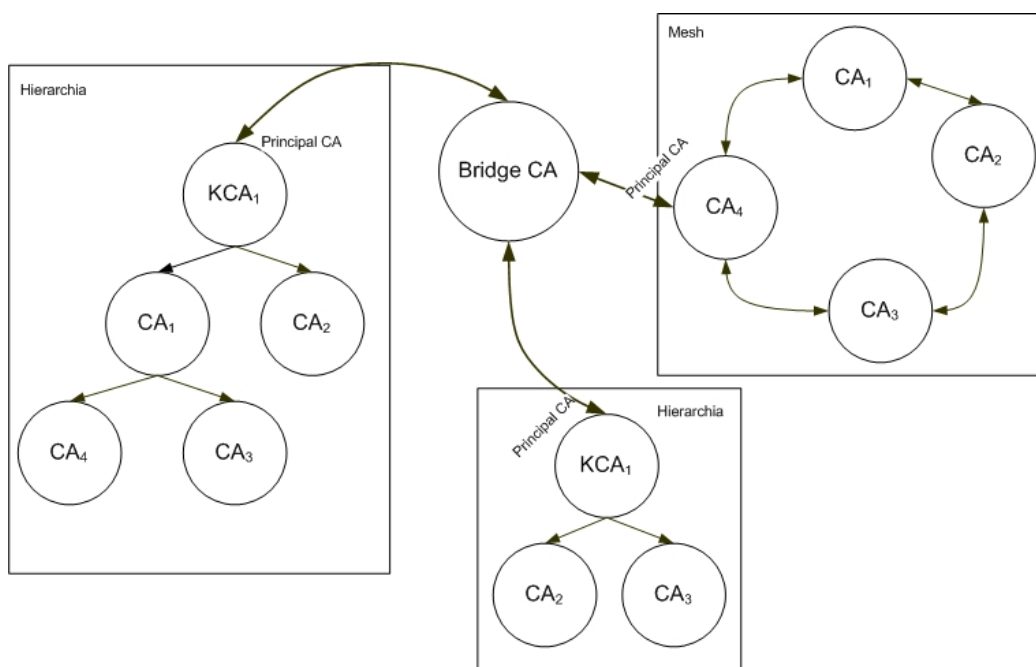


Obrázok 4.4: Možné prepojenie medzi Braňom a Annou na základe mesh architektúry.

koreňové certifikačné autority jednotlivých hierarchických PKI. Výhodou je ľahšia realizácia tak z technického ako legislatívneho hľadiska. Táto štruktúra umožňuje ľahkú kontrolu v rámci jednotlivých komponentov PKI.

Pre lepšiu orientáciu by bolo teoreticky možné vytvoriť novú koreňovú certifikačnú autoritu pri spájaní jednotlivých KCA. Toto riešenie naráža na problém technický (nutnosť vytvoriť bezpečnostné politiky vyhovujúce všetkým KCA ktoré ideme prepojiť) ako aj legislatívny resp. politický (existencia nadnárodných infraštruktúr môže byť ťažko uskutočniteľná).

Na záver možno použiť tzv. *premostujúcu (bridge) certifikačnú autoritu*. Premostujúca CA je navrhnutá špeciálne na prepojenie už existujúcich architektúr PKI nezávisle na ich štruktúre. Na rozdiel od sieťovej štruktúry bridge CA nevydáva certifikáty priamo používateľom. V prípade že bridge CA spája hierarchickú architektúru vytvorí vzťah s jej koreňovou CA. V prípade že pripojená architektúra má byť sieťová, tak sa bridge CA spojí (krížovo certifikuje) s práve jednou certifikačnou autoritou. V každom z predchádzajúcich prípadov CA ktorá sa spojila s bridge CA je nazvaná *hlavná (principal) CA*.



Obrázok 4.5: Možné prepojenie existujúcich PKI pomocou bridge CA.

Kapitola 5

Legislatíva upravujúca elektronický podpis

V predchádzajúcej kapitole sme opísali administratívne a implementačné problémy a riešenia spojené s používaním digitálneho podpisu v praxi. V tejto kapitole sa budeme venovať základným pojmom a definíciám uvedeným v slovenskom zákone o elektronickom podpise ako aj jeho jednoduchému výkladu.

5.1 Direktíva európskej únie o elektronickom podpise a Vzorový zákon UNCITRAL o elektronickom podpise

Vzorový zákon komisie Organizácie spojených národov pre medzinárodné obchodné právo¹ o elektronickom podpise (ďalej len Vzorový zákon) a Direktíva Európskej únie o elektronickom podpise² (ďalej len Direktíva) majú veľa spoločného. Obidva dokumenty boli vytvorené na základe nadnárodnej iniciatívy za účelom zjednodušenia procesu prijímania národných zákonov o elektronickom podpise a ich lepšej interoperability. Vzhľadom na to že tieto dva dokumenty boli podstatnými pomôckami pri tvorbe slovenského zákona o elektronickom podpise budem sa nimi zaoberať podrobnejšie.

¹The United Nations Commission on International Trade Law – UNCITRAL

²Directive of the European Parliament and of the Council on digital signatures

5.2 Vzorový zákon UNCITRAL o elektronickom podpise

5.2.1 Účel a história Vzorového zákona

Vzorový zákon slúži ako právny text, ktorý sa odporúča zapracovať do národnej legislatívy³. Implementujúci štát má možnosť niektoré časti zákona vynechať prípadne modifikovať tak, aby vzniknutý zákon bol v súlade s existujúcou národnou legislatívou. Toto je zásadný rozdiel medzi vzorovým zákonom a medzinárodným dohovorom pri ktorom je možnosť odchýliť sa od textu veľmi obmedzená.

Cieľom Vzorového zákona je:

- Vytvoriť legislatívny rámec za účelom zníženia rizika príliš veľkej odlišnosti jednotlivých národných zákonov ktoré upravujú problematiku elektronického podpisu.
- Prispiieť k pochopeniu problematiky elektronického podpisu.
- Pomôcť k rozšíreniu používania elektronického podpisu.
- Umožniť zrovnoprávnenie elektronického podpisu s vlastnoručným podpisom.
- Zabezpečiť technologickú neutralitu ako aj nezávislosť od vybranej implementácie elektronického podpisu.
- Zaistiť konzistenciu s existujúcim Vzorovým zákonom UNCITRAL o elektronickom obchode.

UNCITRAL bol založený v roku 1966. Jeho hlavnou úlohou je odstraňovanie prekážok medzinárodného obchodu. Po vytvorení Vzorového zákona UNCITRAL o elektronickom obchode sa komisia v roku 1996 rozhodla, že sa začne zaoberať problematikou digitálnych podpisov. Účastníci sa zhodli na vytvorení uniformných pravidiel zaoberajúcich s otázkami legislatívnej úpravy certifikačných procesov, digitálnej autentifikácie ako aj rozdelením rizík a zodpovedností medzi používateľov a poskytovateľov certifikačných služieb. V roku 1998 bola komisii predstavená pracovná verzia pravidiel, ktoré boli

³ Pôvodne mal byť text priamo odvodený od článku 7 Vzorového zákona UNCITRAL o elektronickom obchode. Otázkou zostávalo akou formou by mal byť tento dokument realizovaný: zmluvné pravidlá, legislatívne opatrenia, či smernica. Nakoniec sa komisia rozhodla pre formu legislatívnych pravidiel s komentárom.

neskôr niekoľkokrát revidované v roku 1999. Pracovná skupina ukončila vývoj pravidiel v septembri roku 2000. 5. júla 2001 komisia schválila Vzorový zákon.

5.2.2 Prehľad Vzorového zákona

Vzorový zákon sa skladá z dvanástich článkov upravujúcich využitie elektronického podpisu v rámci komerčných aktivít. Presné znenie Vzorového zákona ako aj jeho podrobný popis možno nájsť v [23], popíšeme preto Vzorový zákon len jednoducho, pričom sa budeme snažiť vysvetliť o čom jednotlivé články pojednávajú.

Článok 1

Vymedzuje hranice pôsobnosti Vzorového zákona, pričom kladie dôraz nato, že Vzorový zákon nesmie anulovať žiadny zo zákonov na ochranu spotrebiteľa.

Článok 2

Článok 2 sa venuje definíciám pojmov známych z PKI⁴ ako aj pojmu elektronického podpisu, dátovej správy a údajov na tvorbu podpisu.

Článok 3

Rovnoprávnosti elektronických podpisov a technologickej neutralite sa venuje článok 3. Je v ňom explicitne uvedené, že žiadna metóda vytvárania elektronického podpisu nesmie byť diskriminovaná v prípade, že spĺňa požiadavky ustanovené článkom 6.

Článok 4

Cieľom článku 4 je poskytnúť návod na interpretáciu Vzorového zákona súdnymi tribunálmi, súdmi, národnými a lokálnymi administratívnymi autoritami. Uvádza, že napriek lokálnemu charakteru zákona je potrebné, aby bol vysvetľovaný s ohľadom na medzinárodnú komunitu aby sa zabezpečila uniformná interpretácia Vzorového zákona.

⁴Ako sme už spomenuli Vzorový zákon je technologicky neutrálny dokument a teda sa neobmedzuje na používanie digitálnych podpisov. Vzorový zákon si však z časti vypomáha istými riešeniami známymi z PKI. Sú to najmä certifikáty, poskytovateľ certifikačných služieb, podpisovateľ a iné.

Článok 6

Článok číslo 6 tvorí jadro Vzorového zákona, pretože vymedzuje právnu účinnosť elektronického podpisu. Článok slúži na zrovnoprávnenie vlastnoručných a elektronických podpisov a sú v ňom opísané nasledovné požiadavky kladené na elektronický podpis:

- a) údaje na tvorbu podpisu sú v kontexte ich použitia spojené s podpisovateľom a s nikým iným,
- b) údaje na tvorbu podpisu sú v čase podpisovania pod kontrolou podpisovateľa a nikoho iného,
- c) je možné zistiť akúkoľvek zmenu elektronického podpisu vykonanú po čase podpísania,
- d) v prípade, že účelom zákonnej požiadavky na podpis je poskytnúť záruky integrity informácii, ku ktorým sa vzťahuje, je možno zistiť akúkoľvek zmenu týchto informácii.

Článok 7

Článok 7 umožňuje príslušným národným autoritám rozhodnúť, ktoré implementácie elektronických podpisov spĺňajú nariadenia článku 6, pričom ale zároveň požaduje konformnosť s medzinárodnými štandardmi. Umožňuje vytvárať elektronické podpisy rôznej váhy. Článok 7 by nemal byť mylne vykladaný ako podpora diskriminácie cudzozemných elektronických podpisov.

Články 8,9,10,11

Články 8 a 11,9,10 pojednávajú o povinnostiach a právach používateľov, poskytovateľov certifikačných služieb a uvádzajú podmienky za ktorých je možné poskytovateľom certifikačných služieb dôverovať. Tieto články vo veľkej miere kopírujú požiadavky kladené na poskytovateľov certifikačných služieb (certifikačné authority, registračné authority). Používateľ by mal pri výbere poskytovateľa certifikačných služieb na základe Vzorového zákona zohľadniť najmä:

- finančné a ľudské zdroje,
- kvalitu softvéru a hardvéru,
- postupy a politiky spracovania certifikátov,

- dostupnosť informácií pre podpisovateľov uvedených v certifikátoch a pre spoliehajúce sa osoby (osoby overujúce resp. inak dôverujúce podpisom)
- pravidelnosť a rozsah auditu nezávislým orgánom
- existenciu vyhlásenia štátu, akreditačného orgánu alebo poskytovateľa certifikačných služieb o súlade s horeuvedenými podmienkami.

Tieto požiadavky priamo plynú z povinností jednotlivých entít v PKI, ktoré sme opísali v predošlej kapitole.

Článok 12

Napokon článok číslo 12 upravuje uznávanie zahraničných certifikátov a elektronických podpisov. Stanovuje nezávislosť elektronického podpisu od geografického umiestnenia jeho vzniku. Podstatná je miera jeho spoľahlivosti. Pri určovaní miery spoľahlivosti by mali zaväziť národné a medzinárodné štandardy, medzinárodné dohody, a iné podstatné skutočnosti.

5.3 Direktíva Európskej únie o elektronickom podpise

5.3.1 Účel a história Direktívy Európskej únie o elektronickom podpise

Direktíva je právny dokument, ktorý síce nemá priamu právnu účinnosť v členských štátoch, ale štáty majú povinnosť ju implementovať do svojich legislatívnych poriadkov. Slovensko sa v roku 2004 stalo členom Európskej únie, a preto muselo zosúladiť svoju legislatívu s európskou. Z toho dôvodu bolo potrebné aby Slovenský zákon o elektronickom podpise spĺňal požiadavky kladené Direktívou

Direktíva kladie požiadavky, ktoré majú byť splnené poskytovateľmi služieb vzťahujúce sa na elektronický podpis ako aj spojené s podpisujúcou a overujúcou stranou a práva, ktoré tieto strany majú. Komisia stanovila za základné ciele Direktívy nasledovné body:

- Vytvoriť legislatívny rámec upravujúci používanie elektronického podpisu.
- Zabezpečiť zrovnoprávnenie elektronického a vlastnoručného podpisu.

- Zabezpečiť technologickú neutralitu realizácie elektronických podpisov.
- Pomôcť k rozšíreniu používania elektronických podpisov.
- Zaistiť kompatibilitu jednotlivých národných zákonov v rámci Európskej únie za účelom plného využitia potenciálu elektronického podpisu.
- Podporiť rozvoj elektronického obchodu.
- Umožniť obmedzenie využitia istých typov elektronických podpisov na určité účely.
- Podporiť využívanie elektronických podpisov v už existujúcich systémoch.

V roku 1997 sa štáty Európskej únie dohodli na jednotnom postupe riešenia problému elektronického podpisu. Direktíva bola schválená 13.12.1999 a zákonodarné orgány jednotlivých členských krajín mali za úlohu zosúladiť svoju legislatívu s Direktívou najneskôr do 19.7.2001.

5.3.2 Prehľad Direktívy

Úvod

Podobne ako Vzorový zákon aj Direktíva v úvode vymedzuje rámec pôsobnosti a ciele Direktívy⁵.

Definície

Definície uvedené v Direktíve sú rozsiahlejšie aj obsiahlejšie ako vo Vzorovom zákone. Uvedieme len najpotrebnejšie, plné znenie Direktívy možno nájsť v prílohe.

Elektronický podpis sú údaje v elektronickej podobe, ktoré sú pripojené alebo logicky spojené s inými elektronickými údajmi a ktoré slúžia ako metóda autentizácie.

Zaručený elektronický podpis je elektronický podpis, ktorý:

- a) je výlučne spojený s podpisujúcim (výhradne priradený podpisujúcemu),
- b) umožňuje identifikovať podpisujúceho,
- c) je vyhotovený prostriedkami, ktoré môže podpisujúci udržiavať výlučne pod svojou kontrolou,

⁵Preambula a článok 1 Direktívy

- d) je takým spôsobom spojený (zviazaný) s údajmi, na ktoré sa vzťahuje, že možno zistiť akúkoľvek neskoršiu zmenu údajov.

Certifikát je elektronické potvrdenie, ktoré spája údaje na overenie podpisu s osobou a potvrdzuje totožnosť tejto osoby.

Kvalifikovaný certifikát je certifikát, ktorý obsahuje nasledovné údaje:

- a) údaj (označenie), že certifikát je vydaný ako kvalifikovaný certifikát
- b) označenie poskytovateľa certifikačných služieb a štátu, v ktorom má sídlo,
- c) meno podpisujúceho alebo pseudonym, ktorý sa má ako taký identifikovať,
- d) priestor (miesto) pre špecifický atribút (charakteristický znak) podpisovateľa, ktorý bude zaradený na certifikát podľa toho, či to vyžaduje účel certifikátu,
- e) údaje na overenie podpisu, ktoré zodpovedajú údajom na vytvorenie podpisu, nad ktorými má podpisujúci kontrolu,
- f) označenie začiatku a konca doby platnosti certifikátu,
- g) identifikačný kód certifikátu,
- h) zaručený elektronický podpis poskytovateľa certifikačných služieb, ktorý certifikát vydal,
- i) prípadne obmedzenia rozsahu použitia certifikátu,
- j) prípadne obmedzenia hodnoty transakcií, na ktoré sa má certifikát použiť

a poskytuje ho poskytovateľ certifikačných služieb ktorý je akreditovaný resp. spĺňa požiadavky prílohy 2 Direktívy.

Poskytovateľ certifikačných služieb (PCS) je inštitúcia (úrad) alebo právnická osoba alebo fyzická osoba, ktorá vyhotovuje (vystavuje) certifikáty alebo poskytuje iné služby súvisiace s elektronickým podpisom.

Dobrovoľná akreditácia je povolenie stanovujúce práva a povinnosti pre poskytovanie certifikačných služieb udelené na základe žiadosti príslušného poskytovateľa certifikačných služieb verejnou alebo súkromnou inštitúciou, ktorá je príslušná stanoviť práva a povinnosti a vykonávať dozor nad ich dodržiavaním, pričom poskytovateľ certifikačných služieb nie je oprávnený vykonávať práva vyplývajúce z povolenia skôr, ako dostane rozhodnutie tohto orgánu.

Bezpečné zariadenie pre vytváranie elektronického podpisu je prostriedok na vytvorenie podpisu, ktorý spĺňa nasledovné podmienky:

1. Bezpečné zariadenia na tvorbu podpisov musia vhodnými technickými prostriedkami a postupmi prinajmenšom zaručiť že:
 - a) údaje na vytvorenie podpisu použité na zhotovenie podpisu sa môžu prakticky vyskytnúť iba jedenkrát a ich utajenie je dostatočne zabezpečené,
 - b) údaje na vytvorenie podpisu použité na zhotovenie podpisu nemôžu byť s dostatočnou istotou odvodené a že podpis je za použitia súčasne dostupnej technológie chránený pred falšovaním,
 - c) údaje na vytvorenie podpisu použité na zhotovenie podpisu môžu byť spoľahlivo chránené oprávneným podpisujúcim pred použitím inými osobami.
2. Bezpečné zariadenia nesmú pozmeniť podpisované údaje a nesmú zabrániť tomu, aby sa tieto údaje zobrazili podpisovateľovi pred podpisovaním.

Direktíva ďalej definuje ďalšie pojmy spojené s vytváraním elektronického podpisu. Sú to: *údaje na vytvorenie podpisu, údaje na overenie podpisu, zariadenie pre overovanie elektronického podpisu* a iné.

Právna účinnosť elektronického podpisu plynúca z Direktívy

V podstate by sme mali rozdeliť elektronické podpisy ako ich pozná Direktíva na dva základné typy: "obyčajný" elektronický podpis a "kvalifikovaný" elektronický podpis. Tieto dva typy majú z Direktívy plynúcu rôznu právnu váhu.

"Obyčajný" elektronický podpis slúži najmä na metódy autentizácie (nemusí slúžiť na zaručenie integrity).

"Kvalifikovaný" elektronický podpis zaručí tak autentizáciu podpisovateľa ako aj integritu dokumentu. "Kvalifikovaný" elektronický podpis musí spĺňať nasledovné podmienky:

- a) Je to zaručený elektronický podpis.
- b) Je založený na kvalifikovanom certifikáte.
- c) Bol vytvorený pomocou bezpečného zariadenia na vytvorenie elektronického podpisu.

"Kvalifikovaný" elektronický podpis má na základe Direktívy rovnakú právnu váhu ako vlastnoručný podpis⁶.

⁶Článok 5 odsek 1 Direktívy

Direktíva kladie za povinnosť členským štátom neupierať právnu účinnosť elektronickým podpisom len z dôvodu, že elektronický podpis⁷:

- je v elektronickej forme, alebo
- nie je založený na kvalifikovanom certifikáte, alebo
- nie je založený na kvalifikovanom certifikáte vydanom akreditovaným poskytovateľom certifikačných služieb, alebo
- nebol vytvorený za pomoci bezpečného zariadenia na vytváranie elektronických podpisov.

Tu je podstatné uvedomiť si rozdiel medzi ekvivalentnosťou s vlastnoručným podpisom a neupretím právnej účinnosti. Totiž elektronickému podpisu ktorý nie je "kvalifikovaný", nemôže byť upretá právna účinnosť⁸, ale nikde nie je povedané, že právna účinnosť musí byť ekvivalentná s účinnosťou vlastnoručného podpisu. Je teda na rozhodnutí príslušných právnych štruktúr akú váhu priradia danému elektronickému podpisu. Tento proces sa môže líšiť od prípadu k prípadu v závislosti od schopnosti preukázať jednotlivé bezpečnostné atribúty elektronického podpisu.

Elektronické podpisy majú pomerne širokú škálu využitia. V závislosti od použitia je určená aj požadovaná bezpečnosť na elektronický podpis. Z tohto dôvodu existujú horeuvedené kategórie. Slovenská legislatívna úprava definuje pojem *elektronického podpisu* a *zaručeného elektronického podpisu*. Tieto dva pojmy by sa dali prirovnať k "obyčajnému" a "kvalifikovanému" elektronickému podpisu. Aj preto sa v tabuľke 5.1 venujem najzávažnejším rizikám, ktoré sú spojené s využitím elektronických podpisov a ich riešeniu v závislosti od typu použitého elektronického podpisu. Táto tabuľka umožní ilustrovať a odôvodniť požiadavky kladené na "kvalifikovaný" podpis.

⁷Článok 5 odsek 2 Direktívy

⁸Článok 5 odsek 2 Direktívy

Tabuľka 5.1: Porovnanie riešenia rizík "kvalifikovaným"
a "obyčajným" elektronickým podpisom

Riziko	Kvalifikovaný podpis	Obyčajný podpis
<p>PCS si ponechal kópie vydaných údajov potrebných pre vyhotovenie podpisu. Tie to môžu byť zneužitú napr. na vytváranie falšných podpisov alebo na narušenie dôvery v podpis určitého používateľa.</p> <p>PCS nepoužíva štandardné a dostatočne silné kryptosystémy na podpisovanie certifikátov, alebo nestanovuje pravidlá ktoré by vylučovali použitie takýchto kryptosystémov (aj v rámci používateľov).</p> <p>PCS nemá dostatočne kvalifikovaný personál, a preto neposkytuje certifikačné služby v požadovanom rozsahu alebo v dostatočnom časovom limite (napr. službu revokovania certifikátov).</p>	<p>Je založený na kvalifikovanom certifikáte vydanom poskytovateľom certifikačných služieb, ktorý musí spĺňať podmienky uvedené v prílohe 2 Direktívy.</p> <p>Riziko je teda prenesené na orgán ktorý vykonával akreditáciu, prípadne kontrolu splnenia požiadaviek Direktívy a na samotného PCS, ktorý sa zodpovedá kontrolnému úradu.</p>	<p>Používateľ musí sám overiť spoľahlivosť PCS, čo môže byť náročné, až nemožné.</p>
<p>Podpisovateľ tvrdí, že certifikát verejného kľúča bol v čase vytvorenia podpisu (pomocou zodpovedajúceho súkromného kľúča) neplatný (napríklad z dôvodu kompromitácie údajov potrebných pre vytvorenie podpisu).</p>	<p>Vydavateľ kvalifikovaného certifikátu je povinný zaručiť, že dátum a čas vydania a zneplatnenia certifikátu je možné určiť presne. Toto je možné zabezpečiť pomocou vydávania CRL resp. OSCP.</p> <p>Pre zviazanie dokumentu s dátumom a časom jeho podpísania je navyše nutné použiť službu časových pečiatok poskytovanú akreditovaným poskytovateľom certifikačných služieb.</p>	<p>Používateľ nie je schopný preukázať platnosť podpisu bez využitia služby časových pečiatok.</p>

Tabuľka 5.1: Pokračovanie

Riziko	Kvalifikovaný podpis	Obyčajný podpis
Kvalifikovaný certifikát bol použitý aplikáciou, ktorá nepovoľuje využitie kvalifikovaných certifikátov (používateľ si neuvedomil, že používa kvalifikovaný certifikát a vytvoril "kvalifikovaný podpis"). Prípadne používateľ predpokladá použitie kvalifikovaného certifikátu ale daný certifikát kvalifikovaný nebol.	Kvalifikovaný certifikát musí obsahovať údaj o tom, že bol vydaný ako kvalifikovaný certifikát.	—
Podpisovateľovi sa pred podpísaním nezobrazil podpisovaný dokument správne, dokument bol podpísaný svojvoľne (nezámerne), údaje ktoré sú potrebné pre vytvorenie podpisu boli kompromitované, podpis nie je dostatočne kryptograficky silný,	"Kvalifikovaný" podpis je vytvorený pomocou bezpečného zariadenia na vytvorenie elektronického podpisu. Toto zariadenie zabezpečuje aby uvedené riziká boli minimalizované na najnižšiu možnú úroveň – pozri definíciu týkajúcu sa bezpečných zariadení pre vytváranie elektronického podpisu.	Používateľ musí zabezpečiť korektnú procedúru podpisovania. V prípade použitia osobného počítača je pri najmenšom potrebné nainštalovať najnovšie aktualizácie antivírusov, bezpečnostné záplaty a zaistiť že na počítači nie je spustený žiadny nevyžiadaný program (spyware, malware, ...). Takisto je potrebné sa presvedčiť, že dokument je prezentovaný správne t.j. je zobrazený celý (vrátane písmen ktoré sú malé, alebo napísané "bielou farbou na bielom podklade" ...).

Právna zodpovednosť poskytovateľov certifikačných služieb

Vydavateľ kvalifikovaných certifikátov ručí za správnosť a úplnosť informácií uvedených v certifikáte⁹, registráciu a revokáciu certifikátov. Vydavateľ kvalifikovaných certifikátov si musí overiť či údaje určené pre vytvorenie podpisu sú vo výhradnom vlastníctve podpisovateľa a či údaje pre vytvorenie a overenie podpisu korešpondujú¹⁰ (v praxi to znamená overiť či overovací kľúč prislúcha k podpisovému kľúču).

Poskytovateľ certifikačných služieb má právo indikovať isté obmedzenia vzhľadom na vydaný kvalifikovaný certifikát. Tieto obmedzenia musia byť jasne definované a musia sa vzťahovať na spôsob použitia certifikátu¹¹. Poskytovateľ certifikačných služieb potom nie je zodpovedný za škody, ktoré boli spôsobené použitím kvalifikovaného certifikátu v nesúlade s obmedzeniami.

Poskytovateľ certifikačných služieb, ktorý vydal kvalifikovaný certifikát je zodpovedný za škody spôsobené fyzickej alebo právnickej osobe, ktorá naň spoliehala, pokiaľ nie je schopný dokázať, že škody nevznikli jeho nedbalosťou.

Ostatné opatrenia

Direktíva zaväzuje členské štáty k uznávaniu kvalifikovaných certifikátov vydaných v iných členských krajinách. Tieto certifikáty musia mať rovnakú váhu ako certifikáty vydané v danej krajine za podmienok že:

- a) vydavateľ certifikátu spĺňa podmienky uložené Direktívou a bol akreditovaný v inom členskom štáte, alebo
- b) poskytovateľ certifikačných služieb zriadený v rámci Spoločenstva, ktorý spĺňa požiadavky ustanovené Direktívou sa zaručil za certifikát, alebo
- c) certifikát resp. poskytovateľ certifikačných služieb je uznaný na základe bilaterálnej alebo multilaterálnej zmluvy medzi Spoločenstvom a tretími krajinami alebo medzinárodnými organizáciami.

Direktíva ďalej udáva povinnosť poskytovateľa certifikačných služieb ochraňovať osobné údaje, vytvára nový orgán – "Výbor pre Elektronický podpis" a stanovuje jej povinnosti.

⁹Je treba podotknúť že tak ako celá Direktíva aj táto časť sa venuje len otvoreným (nie uzavretým) systémom.

¹⁰Článok 6 Direktívy

¹¹Príkladom takéhoto obmedzenia môže byť cenový strop, ktorý nesmie podpísaná transakcia presiahnuť.

5.4 Zhrnutie: čo by mal upravovať zákon o elektronickom podpise

Zákon o elektronickom podpise musí jasne definovať svoj rámec pôsobnosti.

Vzhľadom na svoj technický podtón by mal Zákon o elektronickom podpise obsahovať potrebné definície uvádzajúce nové pojmy do legislatívy. Medzi tieto patria pojmy popisujúce: elektronický podpis, digitálny dokument, údaje potrebné pre vytvorenie resp. overenie elektronického podpisu, (bezpečné) zariadenie potrebné pre vytvorenie resp. overenie podpisu, certifikačné služby, pojem poskytovateľa certifikačných služieb a pojem akreditácie. Táto časť zákona je kritická pre jeho správny výklad, flexibilitu, a účinnosť v praxi.

Pre zaručenie dostatočnej bezpečnosti by zákon mal upravovať spôsob použitia elektronického podpisu. Mal by definovať procedúry a podmienky, za ktorých je vytvorený elektronický podpis platný ako aj podmienky pre správne overenie platnosti podpisu. V tomto popise môže byť uvedené kedy je potrebné využívať bezpečné zariadenie pre vytvorenie podpisu, službu časových pečiatok, aký formát podpisu možno využívať, za akých podmienok je certifikát platný a za akých podmienok môže (by mal) poskytovateľ certifikačných služieb certifikát zneplatniť.

Účinnosť zákon zaručí definovaním zodpovedností jednotlivých entít v rámci PKI, vytvorením kontrolného orgánu a určením sankcií v prípade nedodržania týchto pravidiel. Medzi tieto subjekty patria najmä: certifikačná a registračná autorita ako poskytovatelia certifikačných služieb, používatelia a kontrolný orgán. Ich povinnosti sú opísané v kapitole 4 venujúcej sa PKI.

Zákon by mal určiť v akých prípadoch a za akých podmienok je elektronický podpis ekvivalentný s vlastnoručným, prípadne akú má právnu účinnosť. Zákon môže zaviesť viacero druhov podpisov. Ak tak urobí mal by stanoviť rozdiely medzi nimi a určiť, ktorý typ má akú právnu váhu. Zároveň by mal stanoviť kedy a za akých podmienok sa môže, prípadne za akých podmienok sa nemôže použiť daný typ podpisu.

V rámci záujmu rozšírenia využitia elektronického podpisu je potrebné, aby zákon upravoval podmienky pre cezhraničné uznávanie certifikátov ako aj rozsah ich platnosti.

Nakoniec musí samozrejme zákon zohľadniť aj netechnické požiadavky (zaručiť konformnosť s existujúcou legislatívou).

5.5 Slovenský zákon o elektronickom podpise

V roku 2002 Národná rada Slovenskej republiky schválila zákon o elektronickom podpise. Zákon v prvom rade zavádza pojem elektronického podpisu do slovenskej legislatívy, určuje podmienky jeho používania a stanovuje za akých okolností je elektronický podpis právne ekvivalentný s vlastnoručným podpisom. Týmto spôsobom zákon umožňuje zrovnoprávniť elektronické dokumenty s papierovými. Pri tvorbe zákona sa vychádzalo z nasledujúcich požiadaviek a predpokladov:

1. Bolo by vhodné aby zákon bol čo najviac flexibilný a konformný s už existujúcimi technologickými štandardmi a inými zákonmi o elektronickom podpise. Vzhľadom na rôznorodé štandardy aj zákony toto bolo prakticky nerealizovateľné. Preto sa tvorcovia zákona (aj z dôvodu vstupu SR do EU) rozhodli použiť ako východisko pre poslanecký návrh **Direktívu EU o elektronickom podpise**.
2. Zákon má za úlohu, z dôvodu jeho technologického ladenia, vnieť do slovenskej legislatívy nové pojmy. Tieto pojmy sa týkajú oblasti kryptológie a informačnej bezpečnosti. Mnohé z nich sú prevzaté zo Vzorového zákona a Direktívy a za účelom predídienia ich zlej interpretácie sú konkretizované.
3. Podobne ako Vzorový zákon a Direktíva sa aj slovenský zákon venuje úprave používania elektronického podpisu len v **otvorených systémoch**. Medzi tieto nepatria napr. informačné systémy finančných inštitúcií, škôl, súkromných firiem, ... ktoré nie sú prístupné verejnosti. V prípade, že by sa zákon aplikoval aj na tieto systémy vzniknuté bezpečnostné požiadavky by nemuseli zodpovedať realite. Mohlo by sa stať, že by takéto požiadavky znemožnili prevádzku systému či už z dôvodu finančného alebo organizačného. Napriek tomu v prípade ak sa zúčastnené strany nedohodnú inak, môžu sa riadiť zákonom o elektronickom podpise aj v uzavretých systémoch. Zákon sa takisto nevzťahuje na používanie elektronického podpisu v systémoch zaoberajúcich sa utajovanými skutočnosťami. Dôvod je opačný ako v predošlom prípade. Takéto systémy majú vyššie nároky z hľadiska bezpečnosti.
4. Direktíva aj Vzorový zákon definujú elektronický podpis v technologicky neutrálnom zmysle. Tento spôsob umožňuje pokryť aj budúce potencionálne realizácie elektronického podpisu, ktoré nie sú založené na digitálnom podpise. Problém spojený s týmto riešením je v jeho zložitej implementácii. V prípade príliš všeobecne stanoveného zákona, tento by sa stal neúčinným a nerealizovateľným v praxi. Preto

sa tvorcovia zákona rozhodli realizovať (podobne ako väčšina krajín so zákonom o elektronickom podpise) elektronický podpis na základe **digitálneho podpisu**.

5. Na záver tvorcovia zákona museli zohľadniť už existujúce zákony tak, aby novovytvorený zákon nebol s nimi v rozpore. Bolo treba niektoré zákony upraviť najmä z dôvodu zrovnoprávnenia elektronického podpisu s vlastnoručným.

V tejto časti sa budeme venovať jednoduchému výkladu slovenského zákona o elektronickom podpise. Jeho plné znenie možno nájsť v [27], preto sa skôr zameráme na objasnenie základných pojmov, procedúr a zodpovedností vyplývajúcich zo zákona. Na záver spomenieme za akých podmienok je elektronický podpis právne ekvivalentný s vlastnoručným a priblížime pripravovanú novelu zákona. Pre lepšiu zrozumiteľnosť a ľahšiu orientáciu nebudeme uvádzať presné definície uvedené v zákone, ale vyberieme len najpodstatnejšie podmienky ku ktorým uvedieme aj ich stručné zdôvodnenie.

5.5.1 Definície

Digitálny a elektronický dokument

Zákon pre svoje neskoršie potreby definuje pojem *digitálneho dokumentu*. Digitálnym dokumentom sa rozumie číselne kódovaný dokument (pričom dokument je neprázdna konečná postupnosť znakov). Vzhľadom na to, že znaky nemusia byť len písmená, takáto definícia pokrýva bežné texty, počítačové programy, zvukové záznamy, obrazové záznamy a akékoľvek iné údaje, ktoré sme schopní reprezentovať digitálne. Ako bolo spomenuté zákon implementuje elektronický podpis za pomoci digitálneho podpisu. Digitálny podpis je matematická konštrukcia, ktorá číslu reprezentujúcemu dokument priradí číslo reprezentujúce podpis. Preto je potrebné, aby bol dokument konečný a neprázdny. K takto určenému dokumentu sme potom schopní jednoznačne priradiť číslo reprezentujúce dokument – zakódovať ho.

Na základe digitálneho dokumentu je definovaný *elektronický dokument*. Elektronický dokument je digitálny dokument uchovávaný na fyzickom nosiči, prenášaný alebo spracovávaný pomocou technických prostriedkov elektrickej, magnetickej, optickej alebo inej forme. Táto definícia zahŕňa už aj fyzickú realizáciu dokumentu (môže to byť dokument uložený v počítači, prechádzajúci počítačovou sieťou, ...).

Prostriedky na vyhotovenie elektronického podpisu

Zákon ďalej definuje pojmy *súkromného kľúča*, *verejného kľúča*. Tieto pojmy sme opísali v časti 3.2.3. V tej istej kapitole sme opísali aj *prostriedky na vyhotovenie elektronického podpisu*. Zákon ich definuje ako technické zariadenie alebo programové vybavenie alebo algoritmy ktoré slúžia na vytvorenie elektronického podpisu. Príkladom technického vybavenia môže byť osobný počítač, čipová karta spolu s čítačkou kariet, USB token. Príkladom programového vybavenia sú aplikácie slúžiace pre vytvorenie digitálneho podpisu – napr. Microsoft Outlook, Mozilla Thunderbird, prípadne špeciálny softvér na vytváranie elektronického podpisu, ktorý môže byť certifikovaný kontrolným úradom. Príkladom algoritmov sú podpisové schémy (RSA, DSA, El Gamal, ...) a hašovacie funkcie (MD5, SHA-1, SHA-2, ...).

Elektronický podpis a bezpečné zariadenie na vyhotovenie elektronického podpisu

Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

- a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
- b) je možné efektívne overiť na základe znalosti dokumentu a verejného kľúča prislúchajúceho k súkromnému kľúču¹², že elektronický dokument ku ktorému je táto informácia pripojená je totožný s dokumentom na základe ktorého bola táto informácia vytvorená.

Na rozdiel od vlastnoručného podpisu kde je podpis priamo účastný na dokumente, elektronický podpis nie je súčasťou elektronického dokumentu. Preto je elektronický podpis definovaný ako informácia spojená či logicky prepojená s podpísaným dokumentom. Keďže podpísaný elektronický dokument nie je nijako modifikovaný procedúrou podpisovania, tzn. nevieme určiť či bol dokument podpísaný len na základe samotného dokumentu, je za podpísaný dokument považovaný len elektronický dokument ku ktorému je dostupný aj jeho elektronický podpis.

Ako je známe zo sekcie 3.2.3 digitálne podpisy nie sú absolútne bezpečnou kryptografickou konštrukciou. Znamená to, že k verejnému kľúču sme schopní v konečnom čase zistiť súkromný kľúč. Podstatné je, že to nevieme spraviť efektívne, t.j. takéto odvodenie súkromného kľúča by vyžiadalo

¹²Použitého k vyhotoveniu podpisu.

enormné¹³ množstvo prostriedkov a času. Táto podmienka je pre správnu definíciu elektronického podpisu kritická. Existuje totiž len málo šifrových systémov, ktoré zaručujú absolútnu bezpečnosť a tieto systémy sú v praxi pre implementáciu elektronického podpisu nepoužiteľné. Medzi tieto systémy môžeme zaradiť, napríklad Vernamovu šifru¹⁴. Ako sme už spomenuli¹⁵, Vernamova šifra sa v praxi používa len veľmi málo a je pre implementáciu elektronického podpisu absolútne nevhodná. Keby sme však znížili svoje nároky a požadovali len absolútne bezpečný prenos kľúča, "stačil" by nám prenos kľúča pomocou kvantovej kryptografie. Čo sa týka kvantovej kryptografie, tá je zatiaľ viac-menej len vo výskumnom štádiu. Dosiahli sa síce isté výsledky týkajúce sa kvantového prenosu kryptografických kľúčov, ale v komerčnej sfére sa kvantová kryptografia zatiaľ nepoužíva a pravdepodobne sa nebude používať ani v blízkej budúcnosti.

Druhá podmienka zaručuje schopnosť elektronického podpisu zachovať integritu dokumentu. Takto definovaný elektronický podpis teda spĺňa základné atribúty podpisu – zviazanosť s dokumentom a integritu dokumentu. Zviazanosť s podpisovateľom je zabezpečená na základe certifikátov.

Elektronický podpis možno vytvoriť viacerými spôsobmi v závislosti od použitého technického vybavenia. Rôzne spôsoby vytvorenia podpisu spôsobia rôznu úroveň možnej ochrany podpisu pred jeho falšovaním. Zákon z toho dôvodu definuje pojem *bezpečného zariadenia na vyhotovenie elektronického podpisu*. Pod týmto pojmom sa rozumie prostriedok na vyhotovenie elektronického podpisu. Podrobné požiadavky kladené na takýto prostriedok sú definované vyhláškou č. 539 Národného bezpečnostného úradu. Na základe tohto vyhlásenia bezpečné zariadenie musí najmä:

- a) ochrániť súkromný kľúč používaný na podpisovanie. Takéto zariadenie nesmie umožniť neautorizovaný export súkromného kľúča. Bolo by taktiež vhodné aby zariadenie neumožnilo odvodenie kľúča za pomoci tzv. postranných kanálov. Táto metóda spočíva v odvodení súkromného kľúča na základe nepriamej informácie o procese podpisovania. Medzi takéto informácie môže patriť napr. dĺžka trvania podpisovacej procedúry alebo množstvo spotrebovanej energie pri podpisovaní,
- b) pracovať so schválenými podpisovými schémami, algoritmami a paramet-

¹³Na základe [7] by za použitia 114 počítačov s procesorom Pentium III taktovaným na 500 MHz a 170Gb pamäte trvalo rozbitie kľúča RSA dĺžky 1024 približne 3 milióny rokov. V prípade, že má čitateľ záujem, môže sa o tematike dozvedieť viac v [8], [6] a na internetovej stránke [The New RSA Factoring Challenge](#).

¹⁴Bohužiaľ bolo dokázané, že pre realizáciu absolútne bezpečného kryptosystému potrebujeme náhodný kľúč rovnakej dĺžky ako je správa (Pozri [4, str. 21]).

¹⁵Pozri 3.2.1

rami týchto algoritmov,

- c) zabezpečiť ochranu pred neautorizovanou a nedetekovateľnou modifikáciou zariadenia,
- d) zabezpečiť overenie identity operátora,
- e) pri zapnutí vykonať samočinné testovanie

Body a), c), d) a e) zaručia neschopnosť útočníka neoprávnene manipulovať so zariadením.

Bod b) má dve príčiny. Prvou je zabezpečenie kompatibility vytvorených podpisov s medzinárodnými štandardmi. Tou druhou je kontrola dozorujúceho úradu nad možnými prostriedkami potrebnými pre vytvorenie podpisu. Takto sa dá predísť použitiu neoverených proprietárnych schém a algoritmov, ktoré sa síce môžu zdať na prvý pohľad bezpečné ale v konečnom dôsledku môžu byť ľahko prelomiteľné.

Podobne ako Direktíva EÚ o elektronickom podpise aj slovenský zákon definuje dva druhy elektronického podpisu. *Zaručený elektronický podpis* je elektronický podpis ktorý spĺňa nasledovné požiadavky:

- a) je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného elektronického podpisu,
- b) možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie elektronického podpisu,
- c) spôsob jeho vyhotovovania umožňuje spoľahlivo určiť, ktorá fyzická osoba zaručený elektronický podpis vyhotovila,
- d) na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného elektronického podpisu je vydaný kvalifikovaný certifikát.

Tieto požiadavky kladené na zaručený elektronický podpis sú z veľkej miery prebrané z Direktívy Zaručený elektronický podpis prakticky zodpovedá "kvalifikovanému" elektronickému podpisu. Stručné zdôvodnenie požiadaviek som uviedol v tabuľke 5.1.

Certifikát verejného kľúča

Pre úplné splnenie požiadaviek kladených na podpis musí existovať procedúra, ktorá zviaže identitu podpisovateľa s jeho elektronickým podpisom. Toto zákon rieši zavedením pojmu známeho z PKI. *Certifikát verejného kľúča* je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v

certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný. Certifikát sa skladá z tela certifikátu a z elektronického podpisu tela certifikátu. Tento podpis je podpisom vydavateľa certifikátu a zaručuje overovateľovi že certifikát nebol neoprávnene modifikovaný. Telo certifikátu obsahuje najmä:

- a) identifikačné údaje vydavateľa certifikátu,
- b) identifikačné číslo certifikátu,
- c) identifikačné údaje držiteľa certifikátu,
- d) dátum a čas začiatku a konca platnosti certifikátu,
- e) verejný kľúč držiteľa certifikátu,
- f) identifikáciu algoritmov, pre ktoré je uvedený verejný kľúč určený,
- g) identifikáciu algoritmov použitých pri vyhotovení elektronického podpisu tela certifikátu.

Identifikačné údaje vydavateľa certifikátu sú potrebné pre overenie pravosti certifikátu. Vydavateľ certifikátu môže totiž certifikát medzičasom zneplatniť. Bez znalosti vydavateľa overovateľ nie je schopný overiť platnosť certifikátu ani jeho integritu (nemá verejný kľúč vydavateľa určený na overenie podpisu certifikátu).

Ako identifikačné údaje držiteľa certifikátu¹⁶ môže slúžiť aj pseudonym, ale v tomto prípade vydavateľ certifikátu musí tieto údaje ako pseudonym aj jasne označiť. Zároveň vydavateľ certifikátu musí poznať pravé identifikačné údaje držiteľa.

Z dôvodu existencie viacerých možných algoritmov implementujúcich digitálny podpis je potrebné, aby certifikát obsahoval údaje o algoritme, ktorý bol použitý pri jeho podpisovaní. Takisto musí jasne určovať pre aký algoritmus je verejný kľúč uvedený v certifikáte určený. Overovateľ nemá iný zdroj odkiaľ by zistil aký algoritmus zvolil podpisovateľ pri tvorbe elektronického podpisu. Ak overovateľ nepoužije správny overovací algoritmus, nebude schopný korektne overiť elektronický podpis patriaci k danému dokumentu.

Platnosť certifikátu je obmedzená kvôli podmienenej bezpečnosti asymetrickej kryptografie. Dĺžka platnosti certifikátu závisí od kryptografickej sily súkromného kľúča. Táto môže závisieť od dĺžky kľúča a od použitých algoritmov. Bližšie som sa tejto tematike venoval v 3.2.4.

¹⁶Identifikačné údaje môžu byť: meno, priezvisko, e-mailová adresa, url, dátum narodenia, zamestnanie, ...

Zákon takisto definuje pojem *krížového certifikátu*, ktorý sme opísali v sekcii 4.2.3.

Nato aby sme boli schopní rozlíšiť zaručený elektronický podpis od obyčajného definuje zákon *kvalifikovaný certifikát*. Kvalifikovaný certifikát môže byť vydaný buď akreditovanou certifikačnou autoritou fyzickej osobe alebo inej certifikačnej autorite (ako kvalifikovaný krížový certifikát). Druhým možným vydavateľom je Národný bezpečnostný úrad. Ten vydáva kvalifikované certifikáty certifikačným autoritám, ktoré splnili podmienky potrebné pre akreditáciu. Podstatné je, že kvalifikovaný certifikát musí obsahovať informáciu o tom, že je kvalifikovaný. V prípade absencie tohto údaje nie sme schopní jednoznačne rozlíšiť kvalifikovaný certifikát od obyčajného, keďže sa po fyzickej stránke tieto elektronické dokumenty nijako neodlišujú. Kvalifikovaný certifikát musí byť podpísaný zaručeným elektronickým podpisom vydavateľa. Táto požiadavka sa javí úplne prirodzená, pretože nemá zmysel používať slabší podpis na ochranu silnejšieho. Kvalifikovaný certifikát musí mať v sebe uvedené obmedzenia na použitie (v prípade že naň vydavateľ takéto obmedzenia kladie). Formát a obsah kvalifikovaného certifikátu upravuje vyhláška č. 538 Národného bezpečnostného úradu.

Zoznam zrušených certifikátov

Platnosť certifikátu môže byť ukončená ešte pred vypršaním doby uvedenej v certifikáte. Dôvodov môže byť viacero a sú opísané v kapitole 4 venujúcej sa PKI. Zrušenie platnosti certifikátu neznamena jeho fyzické zrušenie. Certifikát ako elektronický dokument stále existuje, preto je potrebné, aby jeho vydavateľ zaručil mechanizmus na základe ktorého sú schopní jednotliví používatelia zrušené certifikáty identifikovať. Zákon prevezmúc riešenie známe z PKI zavádza pojem *zoznamu zrušených certifikátov*. Zoznam zrušených certifikátov je elektronický dokument skladajúci sa z tela zoznamu zrušených certifikátov a elektronického podpisu tela zoznamu. Vydavateľ zoznamu podpisuje špeciálne na to určeným súkromným kľúčom telo zoznamu za účelom ochrany jeho integrity a autenticity.

Telo zoznamu obsahuje:

- a) identifikačné údaje vydavateľa certifikátov, ktorý spravuje tieto certifikáty,
- b) dátum a čas vydania zoznamu zrušených certifikátov,
- c) dátum a čas najneskoršieho vydania ďalšieho zoznamu zrušených certifikátov,

- d) zoznam identifikačných čísiel certifikátov, ktoré boli zrušené spolu s dátumom a časom ich zrušenia.

Prvé dve podmienky sú zrejmé. Identifikačné údaje vydavateľa sú potrebné pre používateľa z dvoch dôvodov. Za prvé používateľ potrebuje získať príslušný certifikát vydavateľa aby bol schopný overiť elektronický podpis tela dokumentu a tým aj integritu zrušených certifikátov. Za druhé používateľ potrebuje istotu, že ním hľadaný zoznam zrušených certifikátov bol vydaný vydavateľom od ktorého zoznam naozaj žiadal.

Dátum a čas vydania zoznamu slúži na overenie jeho aktuálnosti. V prípade, že používateľ overuje podpis, ktorý vznikol po vydaní tohto zoznamu nemôže si byť istý tým, že certifikát potrebný na overenie podpisu nebol zrušený, napriek tomu že nie je súčasťou zoznamu zrušených certifikátov. V takom prípade, ak bol certifikát následne zrušený, sa objaví v ďalšom zozname zrušených certifikátov. Používateľ sa dozvie termín vydania ďalšieho zoznamu z aktuálneho zoznamu, ktorý má k dispozícii.

Najpodstatnejšia časť zoznamu zrušených certifikátov je zoznam identifikačných čísiel revokovaných certifikátov. K týmto číslam musia prislúchať aj presné časy zrušenia, pretože obvykle na základe certifikačného poriadku držiteľ zodpovedá za škody spôsobené zneužitím certifikátu do doby kým nepredloží certifikačnej autorite autentickú žiadosť o jeho zrušenie.

Časová pečiatka

Časová pečiatka dokladuje existenciu elektronického dokumentu v istom časovom okamihu. Táto skutočnosť je dôležitá v prípade snahy poprieť elektronický podpis zo strany podpisovateľa. Podpisovateľ môže tvrdiť že jeho súkromný kľúč bol kompromitovaný, zneplatniť príslušný certifikát a tým aj podpis určitého dokumentu. Avšak ak vieme jednoznačne určiť, že dokument bol podpísaný ešte pred zneplatnením certifikátu, vieme aj to že podpis s ním spojený je platný a teda podpisovateľ nie je schopný svoj podpis poprieť.

Zákon definuje časovú pečiatku ako informáciu pripojenú alebo inak logic-ky spojenú s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

- a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča určeného na tento účel a bez elektronického dokumentu,
- b) na základe znalosti verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, s ktorým je spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie,

- c) vyhotovila ju akreditovaná certifikačná autorita použitím súkromného kľúča určeného na tento účel,
- d) možno ju vyhotoviť len použitím bezpečného zariadenia na vyhotovovanie časovej pečiatky,
- e) umožňuje jednoznačne identifikovať dátum a čas, kedy bola vyhotovená.

Prvé tri podmienky sú kritické pre bezpečnosť časových pečiatok. Keďže poskytovateľ služieb časovej pečiatky musí byť dôveryhodná tretia strana, je vhodné aby tieto služby vykonávala akreditovaná certifikačná autorita, na ktorej činnosť dozerá príslušný kontrolný orgán. Tento fakt je podstatný aj preto, že časová pečiatka zastáva podstatnú úlohu pri vytváraní niekoľkých typov zaručeného elektronického podpisu.

Certifikačná autorita, registračná autorita a Úrad

Vydavateľom certifikátov a inštitúciou ktorá sa stará o ich správu je dôveryhodná tretia strana. Zákon preberá opäť pojem známy z PKI – *certifikačná autorita*. Orgán zabezpečujúci komunikáciu klienta s certifikačnou autoritou sa nazýva *registračná autorita*. Ústredným kontrolným orgánom štátnej správy pre elektronický podpis je Národný bezpečnostný úrad (ďalej len *Úrad*). Povinnosti a úlohám týchto inštitúcií sa venujem v časti **5.5.2**.

Certifikačné služby a certifikačné činnosti

Zákon definuje *certifikačnou službou* najmä vydávanie certifikátov, zrušovanie platnosti certifikátov, poskytovanie zoznamu zrušených certifikátov, potvrdzovanie existencie a platnosti certifikátov, vyhľadávanie a poskytovanie vydaných certifikátov.

Certifikačnou činnosťou rozumie zákon poskytovanie certifikačných služieb, prijímanie žiadostí o vydanie certifikátu, vedenie evidencie, prevádzku potrebných technických zariadení a inú činnosť potrebnú na zabezpečenie poskytovania certifikačných služieb.

5.5.2 Úlohy a povinnosti plynúce zo zákona

Povinnosti certifikačnej autority

Prvoradou povinnosťou certifikačnej autority je vydávanie certifikátov verejných kľúčov a ich správa. Okrem týchto povinností zákon umožňuje certifikačnej autorite v súlade s Direktívou vykonávať aj iné činnosti, ktoré sú

chápané ako podnikanie¹⁷. Medzi tieto môžu patriť napríklad rôzne školenia alebo výpomoc pri budovaní súkromných PKI.

Povinnosti kladené zákonom na certifikačnú autoritu by sa dali rozdeliť do nasledovných kategórií. Povinnosti týkajúce sa:

- a) zverejnenia údajov o certifikačnej autorite,
- b) vydávania a správy certifikátov,
- c) organizačnej štruktúry a zabezpečenia procesov,
- d) vedenia archívu.

Certifikačná autorita musí ešte pred začatím svojej činnosti zverejniť relevantné údaje. Tieto údaje pomôžu používateľovi pri výbere medzi jednotlivými certifikačnými autoritami. Medzi tieto zo zákona patria predovšetkým¹⁸:

- a) certifikačný poriadok, ktorý obsahuje najmä informácie pre koho a za akých podmienok poskytuje služby, typy vydávaných certifikátov, práva a povinnosti používateľov svojich služieb, vzor žiadostí o poskytnutie služby, pravidlá používania a zrušovania certifikátov,
- b) technické špecifikácie, formáty, normy a štandardy používané pri vykonávaní činností,
- c) cenník svojich platených služieb a zoznam bezplatne poskytovaných služieb,
- d) obmedzenia pri poskytovaní svojich služieb, ak také existujú,
- e) spôsob overenia totožnosti žiadateľa o poskytnutie svojich služieb,
- f) informácie o svojej akreditácii.

Asi najpodstatnejšími kritériami pre používateľa sú obmedzenia, cenník a informácia o akreditácii. Na základe týchto kritérií je schopný rozhodnúť či daný typ certifikátu vyhovuje jeho požiadavkám.

Činnosti týkajúce vydávania a správy certifikátov sme opísali v sekcii 4.2.2. Zákon tieto aktivity upravuje, pričom kladie dôraz nato, aby počas výkonu certifikačných činností nebolo možné zo strany certifikačnej autority vyhotovovať kópie súkromných kľúčov, alebo uchovávať údaje o súkromných

¹⁷§12 odsek 2 z215/2002

¹⁸§12 odsek 5 z215/2002

kľúčoch používateľov jej služieb¹⁹. Ďalšou podstatnou požiadavkou zo strany zákona je existencia zmluvy medzi žiadateľom a certifikačnou autoritou. Táto zmluva môže byť vo forme písaného dokumentu podpísaného vlastnoručným podpisom, alebo vo forme elektronického dokumentu podpísaného zaručeným elektronickým podpisom²⁰.

Certifikačná autorita je zodpovedná za pravdivosť a úplnosť údajov uvedených v certifikátoch ktoré vydala. Ak certifikačná autorita zistí, že tieto údaje nie sú pravdivé alebo kompletne je povinná zaradiť certifikát do zoznamu zrušených certifikátov (CRL). Okrem tejto situácie sa certifikát môže dostať do CRL aj ak o zrušenie požiada vlastník certifikátu, alebo o tento akt požiada súd, alebo sa zistí že súkromný kľúč prislúchajúci k verejnému kľúču uvedenému na certifikáte pozná iná osoba ako držiteľ certifikátu. Certifikačná autorita je zo zákona povinná pravidelne vydávať CRL²¹. Certifikačná autorita môže dobrovoľne poskytovať službu on-line overovania certifikátov.

Z hľadiska organizačnej štruktúry a zabezpečenia procesov je certifikačná autorita povinná mať vypracované bezpečnostné pravidlá a pravidlá na výkon certifikačných činností. Tieto pravidlá musí samozrejme dodržiavať. O týchto pravidlách je povinná informovať tak používateľa certifikačných služieb ako aj iné právnické alebo fyzické osoby, ktoré o ne preukážu oprávnený záujem. Certifikačná autorita je ďalej povinná informovať používateľa o základných procedúrach spojených s vytváraním a overovaním elektronického podpisu.

V prípade, že certifikačná autorita chce zvýšiť svoju konkurencieschopnosť, môže poskytovať tzv. *akreditované* certifikačné služby. Takáto certifikačná autorita musí najprv prejsť procesom akreditácie, ktorý vykonáva Úrad. Súčasťou tohto procesu je aj externý audit, ktorý vykonáva nezávislá auditorská spoločnosť. Táto spoločnosť musí spĺňať kritériá, ktoré vydal Úrad vo vyhláške č. 540. V prípade úspešného ukončenia procesu akreditácie, môže akreditovaná certifikačná autorita vydávať kvalifikované certifikáty, ktoré sú nutnou podmienkou pre využívanie zaručeného elektronického podpisu. Úrad špecifikuje aké podmienky musí spĺňať akreditovaná certifikačná autorita. Tieto sú presne opísané vo vyhláške č. 540 NBÚ a preto spomeniem len najdôležitejšie. Certifikačná autorita musí zabezpečiť:

- a) obmedzený vstup do jej chránených priestorov. Štandardný postup môže mať výnimky obmedzené na nevyhnutné a okamžité riešenie havarijných stavov,
- b) existenciu fyzicky oddelených priestorov slúžiacich pre archiváciu a zálohu dôležitých údajov. Tieto priestory musia byť adekvátne chránené,

¹⁹§14 odsek 1 z215/2002

²⁰tamtiež

²¹§14 odsek 1 bod i z215/2002

- c) nepretržitú prevádzku na úrovni poskytovania služby registrácie požiadaviek na funkciu časovej pečiatky,
- d) vedenie archívu,
- e) vedenie dokumentácie a prevádzku svojej internetovej stránky,
- f) existenciu a dodržiavanie bezpečnostných pravidiel týkajúcich sa vykonávania certifikačných činností,

Akreditovaná certifikačná autorita musí okrem týchto podmienok spĺňať aj podmienky ktoré sú kladené na obyčajné certifikačné authority. Navyše niektoré z týchto podmienok sa musia riadiť podľa prísnejších pravidiel. Medzi tieto napríklad patrí presne stanovený formát poriadku akreditovanej certifikačnej authority ako aj presný formát dokumentu zaoberajúceho sa štruktúrou pravidiel na výkon certifikačných činností. Akreditovaná certifikačná autorita musí navyše oboznámiť používateľa s informáciami o technických produktoch, procedúrach a zariadeniach, ktoré označil Úrad za vhodné pre použitie s zaručeným elektronickým podpisom.

Ak žiadateľ o akreditáciu splnil podmienky na udelenie akreditácie podľa tohto zákona, Úrad do 90 dní od prijatia žiadosti rozhodne o akreditácii a certifikačnej autorite vystaví certifikát.²² Rád by som poukázal na vážnu formuláciu zodpovednosti Úradu. Zákon ponecháva rozhodnutie o akreditovaní na Úrad v prípade, že certifikačná autorita splnila podmienky na akreditáciu. Úrad musí rozhodnúť do 90 dní a to kladne alebo záporne. V prípade, že Úrad rozhodne záporne certifikačná autorita nezíska akreditáciu napriek tomu že spĺňa podmienky na jej udelenie. Myslím si, že vzhľadom na to že zákon hovorí o tom, že certifikačná autorita podmienky na akreditáciu už splnila, úrad by ju mal bezpodmienečne akreditovať. Tvorcovia zákona pravdepodobne touto formuláciou mali na mysli to, že úrad rozhodne do 90 dní o tom či certifikačná autorita splnila podmienky akreditácie určené zákonom a na základe tohto rozhodnutia akreditáciu pridelí alebo nepridelí.

Úloha registračnej authority

Funkciou registračnej authority je sprostredkovanie komunikácie medzi klientom a certifikačnou autoritou. Registračná autorita je zodpovedná najmä za²³:

- a) prijímanie žiadostí o vydanie certifikátu,

²²§13 odsek 4 z215/2002

²³§21 odsek 4 z215/2002

- b) kontrolu súladu údajov uvedených v žiadosti s údajmi v predloženom preukaze totožnosti.

Registračná autorita môže ďalej prijímať žiadosti o zrušenie certifikátov ako aj poskytovať iné certifikačné služby.

Registračná autorita podlieha certifikačnému poriadku príslušnej certifikačnej autority. Táto má za povinnosť kontrolovať dodržiavanie jednotlivých pravidiel. Ich vzájomný vzťah je upravený zmluvou medzi certifikačnou autoritou a danou registračnou autoritou.

Povinnosti používateľov

Držiteľ certifikátu je zodpovedný za:

- a) uvedenie správnych a úplných informácií pri vyplňaní žiadosti o certifikát,
- b) ochranu svojho súkromného kľúča, a v prípade jeho kompromitácie musí bezodkladne požiadať príslušnú certifikačnú alebo registračnú autoritu o jeho zrušenie.

Strata alebo vyzradenie súkromného kľúča môže mať za dôsledok schopnosť protivníka vytvárať falošné podpisy. Tento akt by spôsobil finančné škody a naštobil by dôveru v elektronický podpis.

Podpisovateľ je povinný riadiť sa zákonom a certifikačným poriadkom, najmä časťou popisujúcou proces vytvorenia podpisu. Je povinný brať na zreteľ obmedzenia ktoré vydala certifikačná autorita na certifikát verejného kľúča, ako aj obmedzenia stanovené certifikačným poriadkom a zákonom týkajúce sa produktov a technologických pomôcok, ktoré môže používať pri procese vytvorenia podpisu.

Overovateľ podobne ako podpisovateľ sa musí riadiť zákonom a certifikačným poriadkom, pričom musí najmä správne overiť platnosť certifikátu, ktorý používa na overenie elektronického podpisu. Na tento účel môže použiť prostriedky určené zákonom vyhovujúce certifikačnému poriadku príslušnej certifikačnej autority.

Požiadavky na produkty pre elektronický podpis

Produkty pre elektronický podpis by sa dali zhrnúť do troch kategórii: produkty na vyhotovovanie (zaručených) elektronických podpisov, produkty na vyhotovovanie a uchovávanie (kvalifikovaných) certifikátov a produkty pre overovanie (zaručených) elektronických podpisov.

Produkty na vyhotovovanie zaručených elektronických podpisov musia najmä spoľahlivo chrániť v nich uložený súkromný kľúč pred zneužitím nepovolanou osobou. Medzi tieto produkty patria napr. bezpečné zariadenia na vytvorenie elektronického podpisu.

Na vyhotovovanie a uchovávanie kvalifikovaných certifikátov sa musia používať také zariadenia a postupy, ktoré zabráňujú ich falšovaniu. Ak by sa podarilo získať súkromný kľúč certifikačnej autority umožnilo by to vydávať falošné certifikáty alebo zoznamy zneplatnených certifikátov, v závislosti od typu kľúča ktorý by sa získal. Takýto útok na certifikačnú autoritu by mohol viesť ku katastrofickým následkom až k skolabovaniu PKI.

Na overovanie zaručených elektronických podpisov sa musia používať technické zariadenia a postupy, ktoré zabezpečia, že:

- a) podpísaný elektronický dokument sa pri overovaní zaručeného elektronického podpisu nezmení,
- b) zaručený elektronický podpis sa spoľahlivo overí a výsledok overovania sa správne zobrazí,
- c) možno určiť, či podpísaný elektronický dokument je zhodný s elektronickým dokumentom, ku ktorému bol zaručený elektronický podpis vyhotovený,
- d) overovateľ môže určiť osobu, ktorej zaručený elektronický podpis patrí a použitie pseudonymu je jasne vyznačené.

Úrad vydá zoznam ním certifikovaných produktov ktoré spĺňajú horeuvedené požiadavky. Tento zoznam slúži akreditovaným certifikačným autoritám, aby si zvolili konkrétne produkty, ktoré budú používané na podpisovanie a overovanie zaručených elektronických podpisov a na vyhotovovanie a uchovávanie kvalifikovaných certifikátov. Úrad nemusí nutne posudzovať všetky produkty uvedené v zozname ale môže sa spoliehať aj na medzinárodné certifikačné a šandardizačné orgány.

Úrad

Úrad je najvyšším orgánom štátnej správy pre elektronický podpis. Jeho úlohou je vykonávať dohľad nad dodržiavaním zákona o elektronickom podpise a je zároveň najvyššou (koreňovou) certifikačnou autoritou v Slovenskej republike.

Úrad vykonáva kontrolu a akreditáciu certifikačných autorít. Tieto mu z toho dôvodu musia umožniť prístup k svojim systémom a poskytnúť potrebnú dokumentáciu. Úrad takisto rozhoduje o akreditácii zahraničných certifikačných autorít.

Úrad vedie zoznam všetkých (akreditovaných) certifikačných autorít pôsobiacich na Slovensku. Akreditovaným certifikačným autoritám vydáva kvalifikované certifikáty verejných kľúčov. Týmto im umožňuje vydávať kvalifikované certifikáty pre svojich klientov.

V prípade že akreditovaná certifikačná autorita ukončí svoju činnosť úrad zruší jej certifikát verejného kľúča. Certifikáty ňou vydané prejdú pod správu inej akreditovanej certifikačnej autority, alebo ak žiadna akreditovaná certifikačná autorita tieto certifikáty neprevezme, prevezme ich úrad.

Ďalšou významnou úlohou úradu je sledovanie medzinárodných štandardov a posudzovanie súladu medzinárodne certifikovaných produktov s domácimi kritériami. Dôvodom je zaručenie interoperability slovenských elektronických podpisov s medzinárodnými štandardmi. Ďalej sa týmto zaručí dostatočná miera bezpečnosti produktov použitých slovenskými certifikačnými autoritami.

5.5.3 Typy elektronického podpisu plynúce zo zákona a procedúry s nimi spojené

Vo všeobecnosti by sa typy elektronických podpisov uvedených v Slovenskom zákone o elektronickom podpise dali rozdeliť na dve hlavné skupiny. Sú nimi obyčajný elektronický podpis a zaručený elektronický podpis. Úrad ďalej špecifikuje zaručený elektronický podpis vo všeobecne záväznej vyhláške. V nej uvádza jednotlivé formáty zaručeného elektronického podpisu ako aj spôsob jeho vyhotovenia a overenia. V tejto časti popíšem spôsob vytvorenia a overenia elektronického podpisu v závislosti od jeho typu.

Podpisovanie elektronických dokumentov

Vyhotovenie "obyčajného" elektronického podpisu nie je zo zákona v podstate nijako obmedzené. Táto procedúra je v zákone opísaná nasledovne: Podpisovateľ vyhotoví elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a elektronického dokumentu vyhotoví nový údaj, ktorý spĺňa podmienky uvedené v §3 odsek 1 zákona 215/2002. Tieto podmienky sa vzťahujú na definíciu elektronického podpisu a špecifikoval som ich v sekcii [5.5.1](#) venovanej definíciám.

Naopak vyhotovenie zabezpečeného elektronického podpisu je z dôvodu jeho vyššej právnej sily v zákone podchytené. Zákon hovorí, že podpisovateľ vyhotoví zaručený elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a daného elektronického dokumentu vyhotoví pomocou bezpečného zariadenia na vyhotovenie elektronického

podpisu nový údaj, ktorý spĺňa podmienky podľa odseku 1 §4 z215/2002. Tieto podmienky sú opísané v sekcii 5.5.1.

Zákon ponecháva úpravu spôsobu vyhotovovania zaručeného elektronického podpisu a jeho formát na Úrad. Tento ich uvádza vo vyhláške č. 537. Vyhláška špecifikuje postup vytvorenia jednotlivých formátov zaručeného elektronického podpisu tak, že:

- 1) podpisovateľ vyhotoví zaručený elektronický podpis dokumentu, ktorý chce podpísať.
- 2) Tento sa v závislosti od vybraného formátu logicky prepojí s doplnkovou informáciou ako sú napr. časové pečiatky alebo informácie potrebné pre overenie platnosti.

Ako vidieť spôsob vytvorenia zaručeného elektronického podpisu závisí od jeho formátu. Preto v nasledujúcej časti popíšem a vysvetlím typy zaručeného elektronického podpisu.

Formáty zaručeného elektronického podpisu

Uvedená vyhláška rozpoznáva nasledovné formáty zaručeného elektronického podpisu²⁴:

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

Zaručený elektronický podpis bez časovej pečiatky obsahuje²⁵:

- a) identifikátor podpisovej politiky použitej pri vyhotovení a overení daného zaručeného elektronického podpisu,
- b) podpisové údaje, ktoré podpisujúci zahrnul do zaručeného elektronického podpisu (napríklad miesto a čas vyhotovenia daného elektronického podpisu, meno fyzickej osoby podpisujúcej za právnickú osobu a pod.),
- c) digitálny podpis, ktorý bol vyhotovený na základe

²⁴Vyhláška č. 537 NBÚ §3 odsek 1

²⁵Vyhláška č. 537 NBÚ §3 odsek 2

- 1) digitálneho odtlačku podpisovaného dokumentu,
- 2) identifikátora podpisovej politiky,
- 3) údajov, ktoré podpisujúci zahrnul do elektronického podpisu.

Vyhláška okrem jadra podpisu – digitálneho podpisu, špecifikuje aj dodatočné informácie, ktoré môžu byť pripojené k digitálnemu podpisu za účelom správneho overenia a predídenia jeho falšovania. Podpisová politika slúži na identifikovanie obmedzení asociovaných s vydaním a následným používaním kvalifikovaného certifikátu prislúchajúceho k verejnému kľúču spojeného so súkromným kľúčom použitým na vytvorenie zaručeného elektronického podpisu²⁶. Niektoré z týchto obmedzení môžu byť označené ako kritické. V prípade nesplnenia takéhoto obmedzenia nesmie byť daný kvalifikovaný certifikát považovaný za platný.

Ďalšou extenziou použitou v zaručenom elektronickom podpise je dodatočná informácia, ktorá môže byť užitočná pre používateľa, ale nijak priamo neobmedzuje platnosť zaručeného elektronického podpisu. Takouto informáciou môže byť napr. miesto a čas podpisovania dokumentu, alebo meno fyzickej osoby podpisujúcej za právnickú osobu, zoznam potrebných certifikátov pre overenie príslušného kvalifikovaného certifikátu, zoznam potrebných CRL na overenie príslušného kvalifikovaného certifikátu apod.

Zaručený elektronický podpis s časovou pečiatkou má formu zaručeného elektronického podpisu, ku ktorému je pripojená časová pečiatka vyhotovená na základe daného zaručeného elektronického podpisu. Proces vytvárania časovej pečiatky prebieha nasledovne:

1. Žiadateľ vyhotoví digitálny odtlačok²⁷ dokumentu, ktorý chce podpísať a pošle ho poskytovateľovi služby časových pečiatok.
2. Poskytovateľ služby pomocou bezpečného zariadenia na vyhotovenie časových pečiatok vyhotoví časovú pečiatku do času daného jeho politikou vydávania časových pečiatok a odošle ju žiadateľovi. V prípade že žiadosť nespĺňala všetky požiadavky špecifikované zákonom poskytovateľ služby časovú pečiatku nesmie vytvoriť.

Vzhľadom na náročnosť invertovania hašovacej funkcie je pre útočníka ťažké zistiť aký dokument je podpisovaný. Ak je požadovaná vyššia úroveň bezpečnosti je možné aby táto komunikácia prebiehala šifrovane.

²⁶Ináč povedané: slúži napr. na určenie použitých algoritmov a obmedzení kladených na daný certifikát.

²⁷Ten musí byť vytvorený pomocou schválenej hašovacej funkcie, ktoré sú špecifikované v prílohe vyhlášky. Sú to SHA1 a RIPEMD160

Vydavateľ časových pečiatok uchováva zoznam ním vydaných časových pečiatok a záznamy o mimoriadnych udalostiach v systéme slúžiacom na výdaj časových pečiatok. Tieto údaje musí uchovávať tak dlho ako má stanovené v politike časových pečiatok.

Zaručený elektronický podpis s úplnou informáciou na overenie platnosti má formu zaručeného elektronického podpisu s časovou pečaťou, ku ktorému sú pripojené úplné informácie o všetkých kvalifikovaných certifikátoch verejných kľúčov potrebných na overenie platnosti daného zaručeného elektronického podpisu, ako aj úplné informácie o zoznamoch zrušených kvalifikovaných certifikátov alebo informácie o stave kvalifikovaných certifikátov, ktoré sú rozhodujúce na overenie platnosti daného zaručeného elektronického podpisu²⁸.

Tento formát podpisu je vhodný pre podpisovanie dôležitých dokumentov. Tým že podpis obsahuje všetky potrebné informácie na jeho overenie, je zaručená korektná procedúra overovania podpisu. Táto procedúra môže zlyhať len v prípade, že sa niekto pokúsil dokument falšovať. Nevýhodou takéhoto podpisu je jeho veľkosť a zložitejšia procedúra vyhotovenia.

Na ochranu podpisu pred starnutím podpisových algoritmov a hašovacích funkcií sa používa tzv. **archívny formát elektronického podpisu**. Ten obsahuje všetky údaje potrebné pre jeho overenie a navyše je k nemu pripojená doplnková časová pečať. Táto je vytvorená pomocou silnejších algoritmov a musí pokrývať všetky podstatné zložky podpisu. Proces priradenia doplnkovej časovej pečiatky sa môže časom opakovať – staršie pečiatky môžu byť pokryté novšími, vytvorenými na základe silnejších algoritmov alebo s použitím dlhších kľúčov. Časové pečiatky tak zaručujú aj napriek starnutiu algoritmov integritu archívneho podpisu. V prípade prelomenia podpisového algoritmu, ešte stále nie je možné falšovať archívny podpis. Pre jeho úspešné falšovanie musíme byť schopní prelomiť aj algoritmus použitý na podpis časovej pečiatky. Ten však v čase jej platnosti musí byť dostatočne kryptograficky silný. Na predĺžovanie platnosti archívneho elektronického podpisu slúži práve možnosť použiť viacero časových pečiatok.

Overovanie elektronického podpisu

Podobne ako pri vytváraní "obyčajného" elektronického podpisu ani pri jeho overovaní zákon neukladá striktné podmienky. Určuje len dva základné body, podľa ktorých by mal overovateľ postupovať.

1. Overenie prebieha za pomoci špeciálnych prostriedkov²⁹, elektronického

²⁸Vyhláška č. 537 NBÚ §3 odsek 4

²⁹prostriedky na overovanie elektronického podpisu – §2 bod i) z215/2002

dokumentu a verejného kľúča patriaceho podpisovateľovi.

2. Overovateľ môže požiadať o preukázanie pravosti verejného kľúča. Na tento účel slúži príslušný certifikát verejného kľúča.

Pri overovaní zaručeného elektronického podpisu zákon opäť zavádza vyššie požiadavky. V §5 z215/2002 uvádza, že overovateľ na základe kvalifikovaného certifikátu skontroluje či verejný kľúč slúžiaci na overenie zaručeného elektronického podpisu naozaj patrí podpisovateľovi. Na rozdiel od "obyčajného" podpisu tentokrát zákon udáva overovateľovi povinnosť vykonať túto kontrolu. Výsledok tejto kontroly je pozitívny ak je kvalifikovaný certifikát verejného kľúča platný a verejný kľúč uvedený v certifikáte zodpovedá verejnému kľúču potrebnému na overenie zaručeného elektronického podpisu.

Kvalifikovaný certifikát je platný v dobe, pre ktorú sa overuje jeho platnosť ak³⁰:

- a) takáto doba je medzi začiatkom a koncom platnosti certifikátu,
- b) zaručený elektronický podpis tela certifikátu je platný,
- c) v tejto dobe nebol certifikát zrušený.

Overenie platnosti certifikátu si môže vyžiadať overenie platnosti viacerých certifikátov. V tom prípade daný certifikát je platný v dobe, pre ktorú sa overuje jeho platnosť, len vtedy ak je platný v dobe pre ktorú sa overuje platnosť certifikátu každý z overovaných certifikátov.

Zákon nekladie ďalšie požiadavky na proces overovania zaručeného elektronického podpisu, ale udeľuje povinnosť Úradu vypracovať všeobecne záväzný predpis, ktorý ho určí. Úrad tento proces upravuje v §11 vyhlášky č. 537. Na základe tejto vyhlášky overenie zaručeného elektronického podpisu prebieha nasledovne.

Overovateľ potrebuje pre overenie zaručeného elektronického podpisu: elektronický dokument s ktorým je podpis logicky spojený, platný verejný kľúč prislúchajúci k súkromnému kľúču pomocou ktorého bol dokument podpísaný, podpisovú politiku, ktorej identifikátor je určený v zaručenom elektronickom podpise.

Overenie zaručeného elektronického podpisu závisí od jeho typu. V prvom rade je potrebné overiť či je platný digitálny podpis obsiahnutý v zaručenom elektronickom podpise. Túto procedúru vykoná aplikácia nato určená³¹. Nasledne nato overovateľ overí, že elektronický podpis bol vyhotovený a použitý

³⁰§7 odsek 7 z215/2002

³¹Procedúra je opísaná v kapitole 3 venujúcej sa základom kryptológie.

v súlade s podpisovou politikou. Je preto úlohou aplikácie zobrazit' všetky kritické obmedzenia týkajúce sa podpisu používateľovi, aby bol schopný posúdiť jeho platnosť. V prípade, že má aplikácia možnosť posúdiť splnenie týchto obmedzení môže tak urobiť aby zjednodušila proces overovania.

Overenie zaručeného elektronického podpisu s časovou pečiatkou pozostáva z overenia elektronického podpisu a overenia platnosti časovej pečiatky. Časová pečiatka je platná ak bola vydaná v súlade s politikou časových pečiatok a zaručený podpis vydavateľa časovej pečiatky je platný. Takto podpisovateľ overí, že časová pečiatka nemá porušenú integritu a teda čas v nej uvedený je platný pre digitálny odtlačok zodpovedajúci podpísanému dokumentu.

Overenie zaručeného elektronického podpisu s úplnou informáciou na overenie pozostáva z overenia dostupnosti a úplnosti informácií na overenie zaručeného podpisu a platnosti zaručeného elektronického podpisu s pečiatkou podľa predchádzajúceho odseku.

Overenie platnosti archívneho zaručeného elektronického podpisu spočíva v overení platnosti doplnkovej časovej pečiatky, úplnosti informácií na overenie zaručeného elektronického podpisu a samozrejme overenia podpisu samotného.

5.5.4 Právna váha elektronického podpisu a jeho spôsob využitia

V zásade by sa využitie elektronického podpisu dalo rozdeliť na základe rôznych používateľov a dokumentov ktoré podpisujú do troch základných kategórií. Do prvej spadá Úrad. Úrad podpisuje zaručeným elektronickým podpisom najmä úradom vydané kvalifikované certifikáty akreditovaných certifikačných autorít, úradom vydaný zoznam zrušených kvalifikovaných certifikátov a vyhotovuje aj zaručený elektronický podpis svojho kvalifikovaného certifikátu verejného kľúča. Dôvod je zřejmý. Úrad je najvyššou autoritou v rámci slovenskej PKI, a preto si musí vydávať kvalifikovaný certifikát sám. Zároveň musí zabezpečiť dostupnosť a integritu tohto certifikátu. Certifikát môže zverejniť napríklad v dennej tlači, na svojej internetovej stránke resp. hocikde inde kde je verejnosti dobre dostupný.

Druhou kategóriou používateľov elektronického podpisu sú poskytovatelia certifikačných služieb. Títo využívajú (zaručený) elektronický podpis na zaručenie integrity vydaných (kvalifikovaných) certifikátov, zoznamu zrušených (kvalifikovaných) certifikátov a zaručenie služby časovej pečiatky. Je vhodné spomenúť, že zo zákona vyplýva povinnosť certifikačnej autority používať pre rôzne účely podpisovania, špeciálne na tieto účely určené súkromné kľúče.

Do tretice sú tu "obyčajní" používatelia využívajúci elektronický podpis na podpisovanie ľubovoľných elektronických dokumentov.

Hoci sa tieto spôsoby na prvý pohľad líšia v princípe ostávajú rovnaké. Zákon preto nijak špeciálne neupravuje spôsoby podpisovania jednotlivých typov dokumentov. Pre zaručenie dostatočnej bezpečnosti však kladie procedurálne, organizačné a technologické požiadavky na jednotlivých podpisovateľov, tak aby zaručil dostatočné zabezpečenie ich súkromných kľúčov.

Druhým možným delením spôsobu použitia elektronického podpisu je rozdelenie na základe typu informačného systému v ktorom sa používa. Zákon rozlišuje tri typy informačných systémov: otvorené, uzavreté a systémy ktoré prichádzajú do styku s utajovanými skutočnosťami. Ako som už spomínal zákon sa systémami, ktoré prichádzajú do styku s utajovanými skutočnosťami nezaobrá. V prípade systémov, ktoré sú uzavreté sa zákon aplikuje pokiaľ sa účastníci nedohodnú inak³².

Osobitnou kapitolou sú otvorené systémy. Zákon obmedzuje použitie elektronického podpisu v styku s verejnou správou len na zaručený elektronický podpis³³ a udáva povinnosť upraviť spôsob použitia elektronického podpisu Úradom.

Úrad vo vyhláške č. 542 upravuje spôsob a postup používania v obchodnom a administratívnom styku. Na účely tejto vyhlášky by sa tieto pojmy dali zjednodušene opísať nasledovne. Obchodný styk by sa dal charakterizovať ako komunikácia medzi poskytovateľom služieb v elektronickom obchode a ich príjemcom resp. spotrebiteľom. Administratívny styk je komunikácia medzi orgánom verejnej moci resp. správou a fyzickou alebo právnickou osobou³⁴.

Obchodný styk

Na základe vyhlášky možno používať v obchodnom styku tak zaručený ako aj obyčajný elektronický podpis. Ich právna váha sa môže líšiť. Kým vyhláška zrovnoprávňuje zaručený elektronický podpis použitý v obchodnom styku s vlastnoručným podpisom, váhu obyčajného elektronického podpisu ponecháva na dohodu medzi komunikujúcimi subjektmi.

Formát podpisovaného dokumentu v obchodnom styku závisí od dohody zúčastnených strán, avšak ak formát elektronického dokumentu pripúšťa použitie aktívnych prvkov a sú v elektronickom dokumente prítomné, tak tento dokument nie je možné elektronicky podpísať. V prípade takto podpísaného dokumentu nie je zaručená jeho "stabilita". Dokument obsahujúci aktívne

³²§1 odsek 3 z215/2002

³³§5 odsek 1 z215/2002

³⁴Pre presné definície pozri vyhlášku č. 542 úradu §2 odseky a) a b).

prvky (makrá, vírusy, ...) je schopný zmeny obsahu a preto nie je možné zaručiť, že podpisovateľ si je vedomý a plne súhlasí s tým čo podpísal resp. overovateľ si je vedomý a plne súhlasí s tým čo akceptoval za podpísaný dokument.

Administratívny styk

Tak na základe vyhlášky ako aj na základe zákona možno v administratívnom styku využívať len zaručený elektronický podpis.

Vyhláška určuje aj formáty elektronických dokumentov, ktoré sú akceptovateľné v administratívnom styku. Ide o najpoužívanejšie formáty, ktoré neumožňujú existenciu aktívnych prvkov. Medzi tieto patria najmä: *ASCII* v niektorom z kódovaní znakov podľa ISO, *RTF*, *PDF*, *HTML* a *XHTML*, *XML* a protokoly používané pri elektronickej pošte. Za zmienku stojí, že napriek odstráneniu aktívnych prvkov ani pri použití týchto formátov nemusí byť zobrazenie dokumentu jednoznačne určené. Napríklad HTML 4.01 umožňuje za použitia kaskádových štýlov špecifikovať iný výzor dokumentu pri prehliadaní v počítači a iný pri tlači dokumentu. Podobne umožňuje RTF aj HTML existenciu "bieleho textu na bielom podklade" ako aj iné nepríjemné zradnosti.

Orgán verejnej moci alebo verejnej správy sprostredkováva komunikáciu s fyzickou alebo právnickou osobou pomocou elektronickej podateľne. Táto prijíma, odosiela, overuje a potvrdzuje elektronické dokumenty v styku s fyzickými alebo právnickými osobami. Vyhláška ďalej špecifikuje v §6 povinnosti kladené na prevádzku elektronickej podateľne. Vzhľadom na rozsiahlosť tejto tematiky sa jej nebudem bližšie venovať.

V prípade že elektronický dokument je podpísaný zaručeným elektronickým podpisom a je podaný pomocou elektronickej podateľne, má rovnakú právnu účinnosť ako dokument podpísaný vlastnoručným podpisom. Súčasne s podávaným elektronickým dokumentom musí byť podaný aj kvalifikovaný certifikát potrebný pri overení zaručeného elektronického podpisu daného dokumentu.

5.5.5 Novela Slovenského zákona o elektronickom podpise

V súčasnosti sa pripravuje novela zákona o elektronickom podpise. Vzhľadom na to, že v čase písania tejto diplomovej práce nie je k dispozícii finálna verzia pripravovanej novely, nie sme schopní presne určiť jej formuláciu. Na základe pracovnej verzie novely a pripomienok uverejnených na internetovej stránke

úradu sme však schopní približne určiť, ktorých častí zákona by sa mohla novela týkať.

Problémy implementácie zákona v praxi

Podobne ako je to v iných oblastiach legislatívy, aj v otázke zákona o elektronickom podpise existuje viacero rôznorodých názorov. Faktom ostáva, že tri roky po prijatí zákona o elektronickom podpise nie je veľmi rozvinuté portfólio služieb spojených s elektronickým podpisom a elektronický podpis sa využíva najmä v uzavretých systémoch.

Zákonu je v súčasnej podobe vyčítaná najmä čiastočná nekompatibilita s Direktívou a jeho príliš vysoké požiadavky na bezpečnosť.

Pred tým než sa pozrieme na problematické okruhy v zákone, je treba si uvedomiť, že problém implementácie zákona nespočíva len v zákone samotnom, ale aj v nie práve najvyššej informatizácii spoločnosti.

Treba si uvedomiť nízku nasýtenosť trhu poskytovania Internetových služieb. Našťastie za posledné dva roky sa začal Internet pomerne slušne rozširovať nielen na školách a pracoviskách ale už aj v rámci domácností.

Chýba osвета zo strany štátu, tretieho sektora, prípadne poskytovateľov certifikačných služieb³⁵. Z toho dôvodu panuje v laickej verejnosti nedôvera v elektronický podpis. V rámci osvety by bolo vhodné aspoň rámcovo objasniť používateľom, kedy je potrebné použiť zaručený a kedy "obyčajný" elektronický podpis.

Chýba elektronická podateľňa pomocou ktorej by mohli komunikovať fyzické či právnické osoby so štátnou správou. Momentálne používateľ nemá prakticky možnosť využiť zaručený elektronický podpis v komunikácii so štátnou správou.

Zaručený vs. "obyčajný" elektronický podpis

Podľa súčasnej platnej legislatívy je "obyčajný" elektronický podpis diskriminovaný. V styku so štátnou správou je totiž možné používať len zaručený elektronický podpis³⁶. Toto legislatívne opatrenie je v rozpore s Direktívou, v ktorej sa vyslovene uvádza, že právna účinnosť elektronického podpisu nesmie byť upretá len z dôvodu, že nie je založený na kvalifikovanom certifikáte resp. nebol vytvorený pomocou bezpečného zariadenia na vytváranie elektronických podpisov³⁷.

³⁵Hoci používateľ osvetu zo strany certifikačnej autority mnohokrát chápe ako reklamu.

³⁶§5 odsek 1 z215/2002

³⁷Článok 5 odsek 2 Direktívy

Dôvodom použitia zaručeného elektronického podpisu sú jeho vyššie bezpečnostné záruky a z nich vyplývajúca vyššia teoretická možnosť ochrany pred jeho úspešným falšovaním. Treba si však uvedomiť nasledovné fakty.

V komunikácii s verejnou mocou nemusí byť vždy potrebné použiť vlastnoručný podpis a v takomto prípade by mohol "obyčajný" elektronický podpis vylepšiť komunikáciu medzi zúčastnenými stranami.

Problematická sa môže zdať argumentácia, že vlastnoručné podpisy sa dajú falšovať a napriek tomu sa používajú. Problém spočíva v efektívnosti falšovania elektronického podpisu (za predpokladu prístupu k súkromnému kľúču). Útočník je schopný oveľa jednoduchšie a rýchlejšie podpis falšovať.

Napriek týmto faktom existujú aplikácie v ktorom by postačoval aj "obyčajný" elektronický podpis založený na certifikáte vydanom dôveryhodnou certifikačnou autoritou. Netreba preto obmedzovať komunikáciu medzi verejnou mocou a inými subjektmi len na zaručený elektronický podpis. Treba však jasne stanoviť pôsobnosť obyčajného elektronického podpisu a podmienky za akých ho je možné použiť³⁸.

Certifikačná autorita a akreditácia

Slovenský zákon o elektronickom podpise zavádza ako jednu z podmienok pre vydávanie kvalifikovaných certifikátov akreditáciu certifikačnej autority, ktorá ich vydáva. Toto sa môže javiť ako rozpor s Direktívou, ktorá zavádza pojem akreditácie len ako dobrovoľné osvedčenie. Toto osvedčenie slúži ako pomôcka pre zorientovanie sa na trhu poskytovateľov certifikačných služieb. Direktíva nepodmieňuje vydávanie kvalifikovaných certifikátov akreditáciou príslušného poskytovateľa certifikačných služieb.

Všimnime si však, že Direktíva zavádza pojem "dobrovoľnej akreditácie", ale zákon zavádza len pojem "akreditácie". Hoci bol tento výber zo strany tvorcov zákona pomerne nešťastný (vzhľadom na podobnú formuláciu s iným významom vyskytujúcu sa v Direktíve), nemožno povedať že zákon je v rozpore s Direktívou. Sama Direktíva v prílohe 2 určuje povinnosť poskytovateľa certifikačných služieb vydávajúceho kvalifikované certifikáty preukázať spôsobilosť a spoľahlivosť potrebnú pre vykonávanie certifikačných služieb. Slovenský zákon navyše špecifikuje akým spôsobom certifikačná autorita svoju spôsobilosť preukáže.

Elektronický podpis v automatizovaných systémoch

Na základe súčasného zákona nemožno automatizovane vydávať elektronický podpis v mene právnickej osoby. Sú však situácie, kedy by automatizova-

³⁸Realizovať sa to dá napríklad pomocou podpisovej politiky.

né vydávanie elektronického podpisu značne urýchlilo a zjednodušilo proces komunikácie medzi zúčastnenými subjektmi. Napr. podpisovanie výkazov z banky, faktúr, ...

Novela zákona plánuje riešiť túto situáciu zavedením tzv. elektronickej značky. Tá bude spojená s osobou ktorá bude za ňu zodpovedná na základe tzv. kvalifikovaného systémového certifikátu. V rámci novely treba definovať právnu váhu elektronickej značky ako aj procesy s ňou spojené.

Ostatné problémy

Okrem spomenutých problémov sa zákonu vytýka príliš reštriktívna politika v oblasti používania certifikovaného softvéru v rámci vytvárania zaručeného elektronického podpisu ako aj prísne požiadavky kladené na tento softvér. Hoci je tento postup správny je potrebné si uvedomiť, že ani certifikovaný softvér bez potrebnej podpory zo strany operačného systému³⁹ nemôže úplne zaručiť bezpečnostné požiadavky na úrovni aplikácie.

Podmienky na vývoj certifikovaného softvéru bránia vytvoreniu tzv. open-source riešenia⁴⁰, ktorý by mohol prispieť rozšíreniu elektronického podpisu. Všetky doteraz certifikované aplikácie pre tvorbu zaručeného elektronického podpisu vyžadujú použitie operačného systému od firmy Microsoft (MS Windows) a preto sú používatelia iných operačných systémov diskriminovaní.

Na záver je treba uviesť, že na základe stanoviska úradu k §17 zákona o elektronickom podpise je možné uznať zahraničné kvalifikované certifikáty len na základe medzinárodnej dohody medzi SR a príslušným štátom⁴¹. Úrad vo svojom stanovisku popisuje prečo sa nemôže zaručiť za zahraničné certifikačné authority. Pre uznanie kvalifikovaného certifikátu nestačí teda na základe stanoviska úradu fakt, že bol vydaný ako kvalifikovaný certifikát v niektorej z krajín Európskej únie, čo je v rozpore s §17 odsek 2 zákona.

5.5.6 Zhrnutie a zákona a prehľad identifikovaných požiadaviek

Pre používateľa sú najpodstatnejšími pojmami v zákone, pojmy týkajúce sa (zaručeného) elektronického podpisu, (kvalifikovaného) certifikátu verejného kľúča a (akreditovanej) certifikačnej authority. Preto si v nasledujúcej tabuľke (5.2) zhrnieme aké sú bezpečnostné požiadavky a záruky stanovené zákonom spojené s uvedenými pojmami. Takisto uvedieme aké by mohli technologické požiadavky na možné riešenie v praxi.

³⁹Pozri [30]

⁴⁰Pozri [31]

⁴¹Prípadne na základe §17 odsek 1

Tabuľka 5.2: Prehľad identifikovaných bezpečnostných požiadaviek plynúcich zo z215/2002

Citácia zákona	Bezpečnostné požiadavky	Komentár	Možné technologické riešenie
<p>§3 odsek 1: Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:</p> <p>a) nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,</p> <p>b) na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.</p>	<p>EP musí:</p> <ol style="list-style-type: none"> 1) zaručiť integritu dokumentu, 2) zabrániť popretiu vyhotovenia podpisu, 3) zabrániť efektívne falšovať dokument⁴², tak aby k nemu vytvorený elektronický podpis bol platný. <p>Na vyhotovenie EP nie je nutné mať k dispozícii špeciálny HW ani SW.</p>	<p>Zákon nijak neobmedzuje spôsob vytvorenia EP, pokiaľ spĺňa jeho definíciu.</p> <p>Požiadavky sú podmienené bezpečným uložením súkromného kľúča a z toho plynúcou neschopnosťou tento kľúč zneužiť.</p> <p>Elektronický podpis sám osebe nezaručuje identifikáciu osoby, ktorá dokument podpísala.</p>	<ul style="list-style-type: none"> • digitálny podpis – súkromný a verejný kľúč + certifikát vydaný na tento kľúč (na vytvorenie možno využiť napr. SW OpenSSL), • štandardný HW (PC), • štandardný SW na vytvorenie digitálneho podpisu napr. poštový klient MS Outlook, Eudora, Mozilla Thunderbird, ...
<p>§5 odsek 2: Overovateľ overuje elektronický podpis prostriedkami na overovanie elektronického podpisu využitím podpísaného elektronického dokumentu a verejného kľúča patriaceho udávanejmu podpisovateľovi.</p> <p>§5 odsek 3: Pri overovaní elektronického podpisu overovateľ môže požadovať overenie pravosti verejného kľúča, to znamená toho, že verejný kľúč patrí podpisovateľovi. Na tento účel môže použiť certifikát verejného kľúča podpisovateľa.</p>	<p>Na overenie EP je nutné mať k dispozícii:</p> <ul style="list-style-type: none"> • elektronický dokument a EP príslušného dokumentu, • potrebný verejný kľúč. <p>Na overenie EP nie je nutné mať k dispozícii certifikát verejného kľúča, špeciálny HW ani SW.</p>	<p>Zákon umožňuje overenie EP bez nutnosti overenia pôvodu verejného kľúča, ktorý pri tom používame, ale ponecháva možnosť overovateľovi tak urobiť ak to uzná za vhodné.</p>	<ul style="list-style-type: none"> • štandardný HW a SW ako v predošlom prípade, • verejný kľúč získaný na základe dôveryhodnej tretej strany (certifikát vydaný CA), alebo verejný kľúč dodaný osobne, PGP, alebo verejný kľúč získaný z iného dôveryhodného zdroja (web podpisovateľa, ...)

⁴²bez znalosti súkromného kľúča

Citácia zákona	Bezpečnostné požiadavky	Komentár	Možné technologické riešenie
<p>§4 odsek 1: Zaručený elektronický podpis je elektronický podpis, ktorý musí spĺňať podmienky podľa §3:</p> <p>a) je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného elektronického podpisu,</p> <p>b) možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie elektronického podpisu podľa § 2 písm. h),</p> <p>c) spôsob jeho vyhotovovania umožňuje spoľahlivo určiť, ktorá fyzická osoba zaručený elektronický podpis vyhotovila,</p> <p>d) na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného elektronického podpisu je vydaný kvalifikovaný certifikát.</p>	<p>ZEP musí spĺňať požiadavky kladené na EP, navyše ZEP musí:</p> <ol style="list-style-type: none"> 1) zabezpečiť identifikáciu podpisovateľa (spojenie pomocou kvalifikovaného certifikátu) 2) znemožniť vytvorenie ZEP bez vôle jeho vlastníka tzn.: <ul style="list-style-type: none"> • bezpečne generovať, uložiť a používať súkromný kľúč, • zaistiť autentifikáciu pred použitím SSCD, • zaistiť bezpečnú komunikáciu medzi HW a SW, • korektne zobrazíť podpisovaný text, • overiť formát podpisovaného dokumentu, • vyžiadať potvrdenie podpísania. <p>Na vytvorenie ZEP je potrebné disponovať špeciálnym HW a SW(SSCD⁴³ napr. čipové karty). HW aj SW musí byť certifikovaný úradom.</p>	<p>Vzhľadom na vyššiu právnu účinnosť ZEP je potrebné zaistiť vyššiu bezpečnosť ZEP. Zákon to zabezpečuje zavedením povinnosti použitia SSCD a existencie kvalifikovaného certifikátu. SSCD zaručí, že podpis nebude vytvorený bez vôle vlastníka súkromného kľúča⁴⁴.</p> <p>Ak by sa tvorcovia rozhodli certifikáciu vynechať mohlo by to síce zvýšiť konkurencieschopnosť a zjednodušiť prístup k aplikáciám, ale na druhej strane by sa musel používateľ sám rozhodovať vo veľmi dôležitej otázke týkajúcej sa tvorby ZEP. Vzhľadom na zložitosť tejto tematiky, by to bol pre bežného človeka ťažký problém a mohli by vzniknúť situácie, ktoré by narušili dôveru ľudí v elektronický podpis.</p> <p>Kvalifikovaný certifikát umožní dôveryhodne zviazať súkromný kľúč s identitou jeho držiteľa⁴⁵.</p> <p>K ZEP možno pripojiť časovú pečiatku, pre dôveryhodné určenie času podpisania dokumentu⁴⁶.</p>	<ul style="list-style-type: none"> • digitálny podpis – bezpečne generovaný súkromný a verejný kľúč + kvalifikovaný certifikát vydaný ACA (napr. DTCA, CAEVPÚ), • štandardný HW + čipová karta/USB token., • štandardný SW + SW certifikovaný úradom, • podpisovateľ musí byť oboznámený s certifikačným poriadkom a certifikačnou politikou príslušnej ACA. Nadštandardný SW/HW môže poskytnúť ACA.

⁴³Secure Signature Creation Device – bezpečné zariadenie na vyhotovenie elektronického podpisu

⁴⁴Pozri str. 68

⁴⁵Pozri str. 69.

⁴⁶Pozri str. 72 a 73

Citácia zákona	Bezpečnostné požiadavky	Komentár	Možné technologické riešenie
<p>§5 odsek 4: Pri overovaní zaručeného elektronického podpisu overovateľ na základe kvalifikovaného certifikátu verejného kľúča overí, či verejný kľúč na overenie zaručeného elektronického podpisu patrí podpisovateľovi.</p> <p>§5 odsek 5: Podrobnosti o podmienkach platnosti pre zaručený elektronický podpis, postup pri overovaní a podmienky overenia zaručeného elektronického podpisu ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad⁴⁷.</p>	<p>Na overenie ZEP je nutné mať k dispozícii:</p> <ul style="list-style-type: none"> • elektronický dokument a ZEP príslušného dokumentu, • platný príslušný kvalifikovaný certifikát. <p>Procedúra overovania ZEP musí zaručiť že:</p> <ul style="list-style-type: none"> • podpísaný dokument sa pri overovaní ZEP nezmení, • overovateľ môže určiť osobu, ktorej ZEP patrí a použitie pseudonymu je jasne vyznačené, • výsledok overovania sa korektne zobrazí. 	<p>Overenie ZEP závisí od jeho formátu⁴⁸, pričom overovateľ je zodpovedný za kontrolu vlastníctva verejného kľúča potrebného na overenie ZEP. Na tento účel overovateľ musí skontrolovať platnosť príslušného kvalifikovaného certifikátu (prípadne viacerých certifikátov).</p> <p>Overovateľ samozrejme môže použiť technologické prostriedky, ktoré mu tento proces zjednodušia za podmienky, že proces overovania spĺňa podmienky uložené v §24 odsek 5 a vyhláškou č. 539 úradu.</p>	<ul style="list-style-type: none"> • Štandardný HW a SW, • príslušné kvalifikované certifikáty potrebné na overenie platnosti verejného kľúča, • príslušné vydané CRL, • verejný kľúč získaný na základe kvalifikovaného certifikátu vydaného ACA. <p>Navyše overovateľ potrebuje poznať certifikačný poriadok prípadne podpisovú politiku príslušnej ACA a riadiť podľa nej proces overovania ZEP.</p>
<p>§6 odsek 3: Certifikát verejného kľúča (ďalej len „certifikát“) je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný (ďalej len „držiteľ certifikátu“).</p> <p>§6 odsek 4: Certifikát sa skladá z tela certifikátu a z elektronického podpisu tela certifikátu.</p> <p>§6 odsek 5: určuje obsah tela certifikátu pozri str. 69</p>	<p>Certifikát musí najmä:</p> <ul style="list-style-type: none"> • zviazať identitu držiteľa a jeho súkromného kľúča, • umožniť identifikovať použité algoritmy pri overovaní (Z)EP, • umožniť identifikovať vydavateľa, • zaručiť integritu údajov, ktoré sú v ňom uvedené. <p>Certifikát je vydaný svojim vydavateľom t.j. buď CA alebo úrad⁴⁹.</p>	<p>Pre dôveryhodné zviazanie identity podpisovateľa a jeho súkromného kľúča je potrebné využiť službu dôveryhodnej tretej strany⁵⁰.</p> <p>Zvyšné požiadavky zaručia korektné využívanie certifikátu a jeho integritu a autenticitu.</p> <p>Zákon neupravuje otázku platnosti certifikátu.</p>	<p>Certifikát vydaný certifikačnou autoritou vo formáte X509v3.</p>

⁴⁷Vyhláška č. 537 NBÚ

⁴⁸Pozri str. 82

⁴⁹§2 bod u) z215/2002

⁵⁰Pozri kapitolu 4

Citácia zákona	Bezpečnostné požiadavky	Komentár	Možné technologické riešenie
<p>§7 odseky 2,3,4 pojednávajú o kvalifikovaných certifikátoch. Kvalifikovaný certifikát môže byť vydaný fyzickej osobe, ACA a úradu. Z tejto skutočnosti vychádzajú aj presné požiadavky (Pozri z215/2002 §7). Uvedieme len ich zovšeobecnenie.</p> <p>Kvalifikovaný (krížový) certifikát je certifikát, ktorý:</p> <ul style="list-style-type: none"> • vydala ACA fyzickej osobe (alebo inej ACA) resp. úrad ACA, • je v ňom uvedené, že je kvalifikovaný (krížový) certifikát, • má v sebe uvedené obmedzenia na jeho použitie, ak tretia strana také obmedzenia rozlišuje, resp. je v ňom uvedený účel, na ktorý je určený, • má telo podpísané ZEP vydavateľa. 	<p>Kvalifikovaný certifikát musí spĺňať všetky podmienky ako certifikát, navyše musí byť:</p> <ul style="list-style-type: none"> • odlišiteľný od obyčajného certifikátu, • vydávaný úradom resp. ACA, ktorá zaručí splnenie dodatočných bezpečnostných a organizačných podmienok stanovených vo vyhláske č. 540 úradu. 	<p>Vzhľadom na to, že sa kvalifikovaný certifikát používa na overenie ZEP musí umožniť splniť vyššie bezpečnostné požiadavky kladené na ZEP.</p> <p>Preto je potrebné aby bol kvalifikovaný certifikát vydaný ACA, ktorú kontroluje úrad.</p> <p>Vo vyhláske č. 538 stanovuje úrad formát kvalifikovaného certifikátu. Presnejšie stanovuje pojmy identifikačných údajov držiteľa a vydavateľa, ako aj proces spojený s vydaním kvalifikovaného certifikátu. Popisuje taktiež spôsob vydávania zoznamu zrušených kvalifikovaných certifikátov, jeho formát a periodicitu jeho vydania.</p> <p>Zákon upravuje podmienky platnosti kvalifikovaného certifikátu v §7 odsek 7 z215/2002.</p>	<p>Kvalifikovaný certifikát vydaný ACA (resp. úradom) vo formáte X509v3.</p>

Citácia zákona	Bezpečnostné požiadavky	Komentár	Možné technologické riešenie
<p>§12 odsek 1: <i>Certifikačná autorita je poskytovateľ certifikačných služieb, ktorý spravuje certifikáty a vykonáva certifikačnú činnosť.</i></p> <p>§12 odseky 5,6 a §14 odsek 1 je opísaný v povinnostiach CA na str. 73.</p>	<p>Certifikačná autorita musí zaručiť spoľahlivosť svojich služieb na základe:</p> <ol style="list-style-type: none"> 1) vypracovania a dodržiavania bezpečnostných pravidiel: <ul style="list-style-type: none"> • pre fyzickú bezpečnosť, • pre organizačnú bezpečnosť. 2) určenia vhodných kryptografických algoritmov, 3) zabezpečenia príslušného SW a HW, 4) vypracovania dokumentácie pozostávajúcej z: <ul style="list-style-type: none"> • certifikačného poriadku, • vzorov zmlúv o vydaní a používaní certifikátu, • cenníku poskytovaných certifikačných služieb, • prevádzkových záznamov. 5) zmluvného prepojenia medzi certifikátom a jeho držiteľom. 	<p>Bezpečnostné pravidlá slúžia najmä pre interné účely CA. Umožňujú riadiť a kontrolovať procesy v rámci CA. CA nie je viazaná úradom na vyhlášky, môže sa teda rozhodnúť sama aké kryptografické algoritmy bude používať a na aké kryptografické algoritmy obmedzí použitie verejných kľúčov ňou vydaných certifikátov.</p> <p>HW a SW musí zodpovedať bezpečnostným pravidlám CA a musí byť dostatočný aby umožnil zaručiť splnenie záväzkov CA uvedených v dokumentácii.</p> <p>Dokumentácia, najmä prevádzková slúži na jasné definovanie procesov a zodpovedností v rámci poskytovania certifikačných služieb. Na základe tejto dokumentácie, zákona a príp. zmluvy sa môže tak používateľ ako aj CA odvolávať na svoje práva.</p> <p>Za všetky dokumenty zodpovedá samotná CA, úrad nešpecifikuje ich obsah ani formu. Obsah dokumentov čiastočne upravuje z215/2002.</p>	<p>Komplexné riešenie v sebe okrem iného zahŕňa:</p> <ul style="list-style-type: none"> • zaobstaranie (špeciálneho) HW potrebného na správu certifikátov (napr. kryptografické moduly), • zaobstaranie (špeciálneho) SW potrebného na správu certifikátov a poskytovanie informačných služieb, • zaobstaranie servrov slúžiacich ako adresárové, web servre, backup servre, • zaručenie informačnej bezpečnosti napr. zaobstaranie IDS, firewall-u, antivírus, bezpečnostné záplaty, • zaručenie fyzickej bezpečnosti t.j. vhodných priestorov a ich ochrany.

Citácia zákona	Bezpečnostné požiadavky	Komentár	Možné technologické riešenie
<p>§13 odsek 1: Certifikačná autorita môže požiadať úrad o akreditáciu.</p> <p>§13 odsek 2: Akreditovanou certifikačnou autoritou môže byť právnická osoba alebo fyzická osoba, ktorá má vytvorené materiálne, priestorové, technické, personálne, organizačné a právne podmienky na poskytovanie akreditovaných certifikačných služieb. Podrobnosti o podmienkach na poskytovanie akreditovaných certifikačných služieb ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.</p> <p>§14 odsek 2: Akreditovaná certifikačná autorita je povinná mať vypracované bezpečnostné pravidlá a pravidlá na výkon certifikačných činností podľa pravidiel ustanovených všeobecne záväzným právnym predpisom, ktorý vydá úrad.</p>	<p>ACA musí zabezpečiť všetky požiadavky kladené na CA, pričom sa ale požaduje vyššia miera zabezpečenia a poskytovaných záruk.</p> <p>Pre splnenie týchto podmienok ACA musí navyše najmä:</p> <ul style="list-style-type: none"> • používať úradom stanovené kryptografické algoritmy, • používať úradom stanovené formáty ZEP, kvalifikovaného certifikátu a CRL, • vytvoriť bezpečnostné pravidlá konformné s vyhláškou č. 541 NBÚ. Tieto dokumenty slúžia na kontrolu a riadenie certifikačných procesov a procesov spojených s organizačným riadením ACA. Môžu napr. určovať požiadavky na spracovanie informácií, organizačnú štruktúru ACA, analýzu rizík, havarijné plánovanie, ... • zabezpečiť vhodné priestory s kontrolovaným vstupom, • zabezpečiť oddelené priestory určené na bezpečné skladovanie archívu, • zabezpečiť vlastný systém priebežnej kontroly funkčnosti, • zabezpečiť službu časovej pečiatky a revokácie certifikátov aj v prípade zlyhania základnej infraštruktúry. 	<p>Vyššie stanovené bezpečnostné nároky na ACA sú podmienené vysokou zodpovednosťou, ktorú ACA nesie. Pri nedbalom plnení svojich povinností ACA môže spôsobiť neschopnosť používateľov overiť elektronické podpisy.</p> <p>Ak by ACA <u>hrubo</u> porušila svoje povinnosti, môže prísť aj k falšovaniu ZEP, z čoho vyplýva falšovanie vlastnoručného podpisu.</p> <p>Preto je bezpodmienečne potrebné aby plnenie týchto podmienok kontroloval kontrolný orgán.</p> <p>Zákon určuje, že týmto kontrolným orgánom má byť úrad. Ak zistí porušenie niektorých z týchto podmienok, môže v závislosti od závažnosti priestupku, stanoviť pokutu alebo až pozastaviť činnosť certifikačnej autority. Navyše sa ACA musí pravidelne podrobovať nezávislému auditu.</p>	<p>Pre komplexné riešenie treba splniť technologické, procedurálne a organizačné požiadavky kladené na CA a navyše treba zabezpečiť:</p> <ul style="list-style-type: none"> • zaobstaranie úradom certifikovaného SW a HW, • zabezpečiť 24 hodinovú dostupnosť služby zrušovania certifikátov, • kvalifikovaný personál. V rámci personálu je potrebné aby boli zastávané prinajmenšom nasledovné pozície: • administrátor – osoba zodpovedná za chod systému po technickej stránke, za jeho zálohovanie, inštalácie SW, ... • operátor – osoba zodpovedná za chod systému po obchodnej stránke, vydávanie certifikátov, registráciu používateľov, ... • bezpečnostný referent – osoba zodpovedná za dodržiavanie bezpečnostných opatrení. <p>Ako pomôcka pri budovaní ACA môžu poslúžiť štandardy ITSEC a Common Criteria zaoberajúce sa bezpečnosťou informačných systémov.</p>

Kapitola 6

Záver

V práci sme sa snažili predostrieť komplexný pohľad na problematiku elektronického podpisu, digitálneho podpisu a PKI z technologického, bezpečnostného a právneho hľadiska.

Vzhľadom na rozsiahlosť vybranej problematiky zostalo viacero problémov, ktorým sme sa nevenovali vôbec alebo nie sme sa im nevenovali v plnej miere. Medzi tieto patria najmä nasledovné problémy:

Štandardy – Presný popis štandardov a ich implementácia v praxi je dôležitá z hľadiska bezpečnosti aj z hľadiska interoperability jednotlivých vybudovaných (národných) PKI. V práci sme sa venovali popisu štandardov len okrajovo, tak aby mal čitateľ predstavu o ich obsahu a podstate problémov ktoré riešia.

Detailná analýza zákona – Bolo by potrebné do detailov formálne rozpracovať bezpečnostné požiadavky vyplývajúce zo zákona, ktoré boli načrtnuté v poslednej kapitole.

Zahraničné zákony o elektronickom podpise – Z hľadiska implementácie zákona v praxi¹ by bolo zaujímavé porovnať bezpečnostné požiadavky identifikované v slovenskom zákone s požiadavkami zákonov členských krajín Európskej únie o elektronickom podpise.

Novela slovenského zákona o elektronickom podpise – Na záver by bolo dobré bližšie analyzovať novelu o slovenského zákona o elektronickom podpise, porovnať ju so súčasným zákonom a identifikovať aké bude mať účinky na systémy v ktorých sa už elektronický podpis používa, ako aj aký bude mať vplyv na rozvoj elektronického podpisu.

¹Cezhraničné poskytovanie certifikačných služieb, uznávanie zahraničných kvalifikovaných certifikátov, ...

Literatúra

- [1] Pavel Vondruška, Příručka: Standardy a normy (ALG082, MFF UK, 2004).
- [2] Crypto-World, Informační sešit GCUCMP, <http://crypto-world.info>.
- [3] Stinson, D. R.: Cryptography Theory and Practice, CRC Press, 1995.
- [4] Menezes, A. J. – van Oorschot, P. C. – Vanstone S. A.: Handbook of Applied Cryptography, CRC Press, 1997. <http://www.cacr.math.uwaterloo.ca/hac/>.
- [5] Martin Stanek: Základy kryptologie, verzia 0.15b, materiál k prednáške z kryptologie na FMFI UK. <http://www.dcs.fmph.uniba.sk/stanek/crypto/main2.pdf>.
- [6] Robert D. Silverman: An Analysis of Shamir's Factoring Device, RSA Laboratories' Bulletin 12, 1999. <http://www.comms.scitech.susx.ac.uk/fft/crypto/RSAbulletin/bulletn12.pdf>.
- [7] Robert D. Silverman: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, RSA Laboratories' Bulletin 13, 2000. <http://www.nullify.org/docs/bulletin13/bulletin13.html>.
- [8] Lenstra A. K. – Lenstra H. W. – Manasse M. S. – Pollard J. M.: The number field sieve. <http://www.std.org/msm/common/nfspaper.pdf>.
- [9] Jaroslav Janáček – Richard Ostertág: Problems in Practical Use of Electronic Signatures, Security & Control of IT in Society – II, Proceedings of the IFIP WG 9.6/11.7 Working Conference, (63–75), Bratislava, 2001.
- [10] Jozef Mistrík: Grafológia, Obzor. 1985.
- [11] Jozef Vyskoč: Bezpečnosť informačných systémov, Bratislava, 1999. <http://www.vaf.sk/download/scripta.zip>.

- [12] Bruce Schneier: Secrets and Lies, Wiley, 2000.
- [13] Peter Gutmann, X.509 Style Guide, 2000.
<http://www.cs.auckland.ac.nz/pgut001/pubs/x509guide.txt>.
- [14] Shimshon Berkovits, Santosh Chokhani – Judith A. Furlong – Jisoo A. Geiter – Jonathan C. Guild: Public Key Infrastructure Study, Mitre, 1994.
- [15] Jaroslav Janáček: Certifikačná autorita, Diplomová práca, FMFI UK, Bratislava, 2000. <http://www.dcs.fmfi.uniba.sk/janacek/home/CA.ps>.
- [16] D. Richard Kuhn – Vincent C. Hu – W. Timothy Polk – Shu-Jen Chang: Introduction to Public Key Technology and the Federal PKI Infrastructure, National Institute of Standards and Technology, 2001.
- [17] Carlisle Adams – Steve Lloyd: Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition, Addison Wesley, 2002.
- [18] RFC2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
- [19] RFC3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- [20] RFC3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- [21] Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats, ETSI TS 101 733.
- [22] Time stamping profile, ETSI TS 101 861.
- [23] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, UNITED NATIONS New York, 2002.
- [24] EESSI: Directive of the European Parliament and of the Council on digital signatures, 1999.
- [25] BSI: BSI Manual for Digital Signatures, Version 1.
- [26] Poslanecký návrh zákona o elektronickom podpise, Dôvodová správa.
- [27] Slovenský zákon o elektronickom podpise a o zmene a doplnení niektorých zákonov, 2002.

- [28] Vyhlášky č. 537 – 542 Národného bezpečnostného úradu, 2002.
- [29] Internetová stránka Národného bezpečnostného úradu,
<http://www.nbusr.sk>.
- [30] Jaroslav Janáček: Postrehy k elektronickému podpisu v SR, 2004.
http://www.nbusr.sk/NBU_SEP/leg_rozne/prip_janacek.doc.
- [31] Ivan Kopáčik: O elektronickom podpise, 2004.
http://www.nbusr.sk/NBU_SEP/leg_rozne/prip_kopacik.doc.
- [32] <http://www.zbierka.sk>.
- [33] Ronny Bjones – David Race – Stefan Santesson – Mirek Lang – Jiri Sklepnik – Jeremy Hilton – Suzana Vukcevic – Claudio Vacalebre – Patrick Van Eecke – Georgia Skouma – Susan Koeppen: Qualified Electronic Signatures Tutorial, Microsoft Corporation, 2004.
<http://www.microsoft.com/downloads/details.aspx?FamilyID=0b3c55f6-11d4-4f46-8a37-0ba004e14dcf&DisplayLang=en>.