KATEDRA INFORMATIKY
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
UNIVERZITA KOMENSKÉHO, BRATISLAVA

# Vytváranie a overovanie archívnych elektronických podpisov

diplomová práca

Tomáš Záhorec

**Vedúci diplomovej práce :**
doc. RNDr. Daniel Olejár PhD.

Bratislava
2008

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

.....

## Poďakovanie :

Ďakujem svojmu vedúcemu diplomovej práce za všetky konzultácie a cenné rady pri písaní diplomovej práce. Okrem toho ďakujem svojej rodine, všetkým priateľom a blízkym za pomoc a podporu.

# Abstrakt

Rozvoj informačných technológií prispel k tomu, že stále viac dokumentov existuje len v elektronickej podobe. Keďže elektronické dokumenty by mali mať rovnakú právnu váhu ako papierové, musia okrem iného poskytovať rovnaké záruky na integritu a autentickosť ako papierové verzie dokumentov. Na zaistenie bezpečnosti elektronických dokumentov sa používajú rozličné metódy. Jedným z najdôležitejších bezpečnostných mechanizmov používaných na zaistenie integrity a autentickosti elektronických dokumentov je elektronický podpis. Diplomová práca sa venuje konceptu archívneho elektronického podpisu, ktorého úlohou je zaistenie integrity a autentickosti elektronických dokumentov v dlhodobom horizonte. Diplomová práca skúma možnosti jeho použitia v praxi, obsahuje analýzu údajov potrebných na overenie archívneho elektronického podpisu a analýzu bezpečnostných požiadaviek na proces jeho vytvárania a overovania. V závere diplomovej práce sú popísané pripravované legislatívne zmeny zákona o elektronickom podpise.

**Kľúčové slová :** archívny zaručený elektronický podpis, digitálny podpis, informačná bezpečnosť, kryptológia, kvalifikovaný certifikát, certifikačná autorita, public key infrastructure, potrebná informácia/údaje

# Obsah

# 1 Úvod

Vďaka rozvoju informačných technológií sa používanie elektronických dokumentov stalo každodennou súčasťou života väčšiny obyvateľov vyspelých krajín. Dokumenty v elektronickej forme postupne nahrádzajú papierové dokumenty. Inak tomu nie je ani na Slovensku a je pravdepodobné, že tento trend bude i naďalej stále silnieť. Skutočnosť, že používanie elektronických dokumentov sa rozšírilo do všetkých oblastí súkromného a verejného života, so sebou priniesla aj nové požiadavky na bezpečnosť informácií uložených v digitálnej forme.

V mnohých prípadoch totiž nestačí dokument len vytvoriť, je potrebné ho aj podpísať. Týmto autor dokumentu adresátovi okrem iného zaručuje, že dokument skutočne vytvoril on, a že s obsahom dokumentu súhlasí. Dokumenty v papierovej forme podpisujeme vlastnoručným podpisom. Aby sme mohli spoľahlivo používať elektronické dokumenty, bolo potrebné nájsť spôsob, akým by sa dali elektronické dokumenty podpisovať a vytvoriť mechanizmus, ktorý by bol analógiou k vlastnoručnému podpisu, t.j. poskytoval rovnaké bezpečnostné záruky ako vlastnoručný podpis. Túto funkciu vo svete digitálnych (elektronických) dokumentov plní elektronický podpis založený na digitálnom podpise.

Životnosť vlastnoručného podpisu dokumentu nie je neobmedzená, závisí hlavne od životnosti materiálu - nosiča, na ktorom je dokument vytvorený. Avšak pri vhodnom zaobchádzaní s papierovými dokumentami (dokumentami, ktoré ako nosič používajú papier) môže vlastnoručný podpis zaručiť ich dlhodobú ochranu. Pri elektronických dokumentoch podpísaných pomocou elektronického podpisu môžu byť po istom čase prekonané algoritmy, na ktorých sa tento podpis zakladá, resp. nemusí byť dostupná informácia potrebná na overenie elektronického podpisu. Preto obyčajný elektronický podpis na zaistenie autentickosti a integrity dlhodobo uchovávaných digitálnych/elektronických dokumentov nepostačuje, ale je potrebné použiť špeciálny typ elektronického podpisu, nazývaný archívny elektronický podpis.

## 1.1 Ciele diplomovej práce

Cieľom mojej diplomovej práce je v prvom rade ponúknuť čitateľovi základný prehľad v oblasti informačnej bezpečnosti a kryptológie, oboznámiť

ho s infraštruktúrou verejného kľúča (PKI), ozrejmiť funkciu certifikátov verejných kľúčov a úlohu certifikačných autorít.

Najdôležitejším cieľom je ale analyzovať koncept archívneho elektronického podpisu hlavne z technologického hľadiska, teda zistiť, akú všetku informáciu je potrebné mať na overenie archívneho elektronického podpisu, aké je množstvo tejto informácie, či je toto množstvo konečné. Analýza dá odpoveď na otázku, či je koncept archívneho elektronického podpisu v takej forme, v akej je v súčasnej slovenskej legislatíve definovaný (Zákon č. 215/2002 Zbierky zákonov o elektronickom podpise a o zmene a doplnení niektorých zákonov [15], Vyhláška Národného bezpečnostného úradu č. 537/2002 Zb. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky [16]), skutočne realizovateľný. Popritom je cieľom mojej diplomovej práce aj navrhnúť spôsob, akým by sa archívny elektronický podpis mal vytvárať a overovať, pričom sa pozriem aj na bezpečnostné požiadavky týchto procesov.

Nakoniec informujem čitateľa o pripravovaných legislatívnych zmenách v oblasti elektronických podpisov a smerovaní do budúcnosti.

## 1.2 Výsledky

Pred začatím analýz som sa na koncept archívneho elektronického podpisu pozeral skôr skepticky. Predpokladal som, že množstvo informácie potrebnej na overenie archívneho elektronického podpisu bude veľmi veľké, či dokonca, že bude narastať donekonečna. Nevedel som, či sa pri overovaní digitálnych podpisov a časových pečiatok v procese overovania archívneho elektronického podpisu nemôžem dostať do cyklu alebo ku kruhovým referenciám.

Dospel som ale k prekvapujúcim výsledkom. Podľa výsledkov analýz je koncept archívneho elektronického podpisu v podmienkach Slovenskej republiky bez väčších problémov realizovateľný. Množstvo potrebnej informácie je porovnateľné s veľkosťou podpisovaných dokumentov a pri dodržaní všetkých bezpečnostných zásad je proces vytvárania a overovania archívneho elektronického podpisu ľahko realizovateľný.

## 1.3 Štruktúra diplomovej práce

Diplomová práca je určená predovšetkým pre pracovníkov certifikačných autorít, pracovníkov v oblasti infraštruktúry verejného kľúča, programátorov

aplikácií na prácu s elektronickými podpismi, ale aj užívateľov týchto aplikácií. Delí sa na kapitoly. V úvodnej kapitole sa čitateľ dostáva do problému, a dozvedá, o čom diplomová práca je.

Vzhľadom na široké spektrum potenciálnych čitateľov, diplomová práca ďalej obsahuje kapitolu o informačnej bezpečnosti a kryptológii, v ktorej sú spomenuté aspoň základné informácie a definície pojmov z oblasti týchto vedných disciplín. Táto kapitola je určená predovšetkým pre užívateľov, ktorí nemajú potrebné informatické vzdelanie, pre pochopenie základných pojmov.

Potom nasleduje kapitola o infraštruktúre verejného kľúča, v ktorej sú informácie o certifikátoch, cetifikačných autoritách, ich úlohách, vzájomných vzťahoch a štruktúre. Je určená najmä pre užívateľov a programátorov, aby sa oboznámili s realizáciou PKI.

Najdôležitejšia je kapitola o archívnom elektronickom podpise, v ktorej sa nachádzajú analýzy konceptu archívneho elektronického podpisu. Je určená pre všetkých, ktorí majú záujem dozvedieť sa o archívnom elektronickom podpise a možnosti jeho použitia v praxi, od odborníkov po laikov.

Každá kapitola sa podľa významového obsahu jednotlivých častí môže deliť na podkapitoly. Podľa úrovne vedomostí môže čitateľ kapitoly, ktorých obsah je pre neho známy preskočiť. V prípade potreby v nich nájde presné definície pojmov, pre prípad, že by mu bol niektorý pojem neznámy, alebo by sa len potreboval uistiť, v akom význame sa pojem v práci používa.

V závere diplomovej práce sú zhrnuté výsledky, nájdeme tu zoznam použitých skratiek, zoznam použitej literatúry a obsah CD s prílohami.

# 2 Základné pojmy

Diplomová práca pojednáva o jednom z prostriedkov na zaistenie bezpečnosti elektronických dokumentov, o elektronickom podpise. Elektronický podpis je informácia pripojená k elektronickému dokumentu, ktorá má niekoľko dôležitých funkcií. Slúži predovšetkým na zabezpečenie integrity a autentickosti ním podpísaných elektronických dokumentov. Overovanie elektronického podpisu vytvoreného neznámym podpisovateľom si vyžaduje

- poznanie verejného kľúča, ktorý tvorí pár so súkromným kľúčom použitým pri vytváraní elektronického podpisu,
- identifikáciu držiteľa súkromného kľúča.

Obe funkcie plní certifikát verejného kľúča, ktorý držiteľovi súkromného kľúča vydala dôveryhodná tretia strana, tzv. certifikačná autorita (CA). Certifikačná autorita overila identitu držiteľa súkromného kľúča, overila, či predložený verejný kľúč, na ktorý má vydať certifikát tvorí pár so súkromným kľúčom podpisovateľa, ktorý žiada o vydanie certifikátu. Verejný kľúč a meno držiteľa certifikátu (držiteľa súkromného kľúča) je zapísané v certifikáte, ktorý certifikačná autorita vydala a podpísala svojím elektronickým podpisom. Overovateľ elektronického podpisu overí elektronický podpis vydavateľa certifikátu, zistí, či je certifikát platný a ak áno, pomocou verejného kľúča z certifikátu overí elektronický podpis. Meno uvedené v certifikáte je potom meno človeka, ktorý elektronický podpis vytvoril.

Celá táto procedúra má niekoľko nedostatkov. Skôr, ako overovateľ môže použiť verejný kľúč z certifikátu na overenie elektronického podpisu, potrebuje overiť elektronický podpis na certifikáte. A na to potrebuje poznať verejný kľúč certifikačnej autority, ktorá certifikát vydala. Ak to nie je certifikačná autorita, ktorej verejný kľúč overovateľ pozná (napríklad certifikačná autorita, ktorá mu vydala certifikát), podpis na certifikáte overuje na základe certifikátu verejného kľúča, ktorý certifikačnej autorite vydala iná certifikačná autorita. Táto rekurzia nie je nekonečná a pravidlá upravujúce používanie elektronických podpisov vylučujú cykly. V hierarchickej infraštruktúre verejného kľúča (PKI - public key infrastructure) sa overovateľ po niekoľkých krokoch dostane k najvyššej CA, tzv. koreňovej CA, ktorej verejný kľúč poznajú (teda mali by poznať) všetci používatelia elektronických podpisov z domény danej koreňovej CA.

Existuje však ešte iný problém. Z bezpečnostných dôvodov je životnosť certifikátu obmedzená a certifikát možno kedykoľvek v priebehu jeho životnosti zrušiť. Certifikát, ktorý bol zrušený, nemožno použiť na overenie elektronického podpisu. Certifikačná autorita je povinná pravidelne vydávať zoznamy zrušených certifikátov (každých 24 hodín). Každý takýto zoznam zrušených certifikátov je podpísaný elektronickým podpisom, pre overenie ktorého platia tie isté pravidlá, ako pre obyčajné elektronické podpisy. Naviac, aby si boli používatelia elektronických podpisov istí, kedy došlo k nejakej udalosti (doručenie elektronického dokumentu, vytvorenie elektronického podpisu, stiahnutie zoznamu zrušených certifikátov a pod.) môžu si na ktorýkoľvek dokument nechať vydať časovú pečiatku, čo je v podstate elektronický podpis na haš (digitálny odtlačok) dokumentu a časový údaj. Z uvedeného vyplýva, že elektronicky podpísaný dokument môže obsahovať niekoľko vnorených elektronických podpisov a overovanie každého z nich si vyžaduje poznať certifikát verejného kľúča a príslušný zoznam zrušených certifikátov, na ktorom by sa potenciálne mohol daný certifikát nachádzať. Je zrejmé, že rozsah informácií potrebných na prevádzku CA a PKI prudko narastá (okrem iného aj denne pribúdajúce zoznamy zrušených certifikátov), a preto sú informácie, ktoré sa aktuálne nepoužívajú, v zákonom stanovenej dobe archivované. To však znamená, že môže nastať situácia, keď overovateľ potrebuje overiť elektronický podpis na dokumente, ktorý bol podpísaný tak dávno, že informácie potrebné na jeho overenie už nie sú voľne dostupné.

Aby bolo možné riešiť tento problém, bol v Zákone č. 215/2002 Zbierky zákonov o elektronickom podpise a o zmene a doplnení niektorých zákonov definovaný formát archívneho elektronického podpisu (definovaný v technickej špecifikácii ETSI TS 101 733 v1.7.3 [37]), ktorý obsahuje všetky informácie potrebné na overenie elektronického podpisu.

Zákon o elektronickom podpise platí 5 rokov a archívne elektronické podpisy sa zatiaľ nepoužívajú, a preto nie je jasné, či je koncepcia archívneho elektronického podpisu správna a či legislatíva upravuje dostatočne jeho používanie. Čas používania archívnych elektronických podpisov sa blíži a preto by bolo užitočné analyzovať tak kryptologickú stránku (zastarávanie a slabnutie použitých kryptografických primitívov), technologickú stránku (je možné zozbierať všetku informáciu potrebnú na overenie archívneho elektronického podpisu) ako aj legislatívnu stránku (postačuje zákon a vykonávacie predpisy na úpravu používania archívnych elektronických podpisov), prípadne iné aspekty.

# 3 Základy informačnej bezpečnosti a kryptológie

Informačná bezpečnosť je vedná disciplína, ktorej hlavnou úlohou je najmä ochrana informácií a informačných systémov pred hrozbami počas celého ich životného cyklu. Pre dosiahnutie svojich cieľov využíva informačná bezpečnosť aj poznatky iných technických, ale aj humanitných vedných odborov, pričom najužšie prepojená je práve s kryptológiou.

Kryptológia je vedná oblasť, ktorá sa zaoberá konštrukciou a analýzou kryptosystémov. Spočiatku sa kryptológia upriamovala na zabezpečenie dôvernosti údajov, teda na šifrovanie. Neskôr sa začala zaoberať aj ostatnými požiadavkami na integritu údajov, autentickosť, nepopierateľnosť konania, či časovú súslednosť.

V nasledujúcich častiach sa budú nachádzať základné informácie, techniky a celkový náhľad na informačnú bezpečnosť a kryptológiu. Podrobnejšie informácie o týchto dvoch vedných disciplínach možno nájsť v literatúre, ktorá sa podrobne venuje informačnej bezpečnosti [2] a kryptológii [3], ako aj v niektorých diplomových prácach študentov Fakulty matematiky, fyziky a informatiky Univerzity Komenského v Bratislave, ktoré sa danej problematike venujú [39,40,41]. Nasledujúce časti sa opierajú o spomenuté zdroje a čerpajú z nich poznatky.

## 3.1 Informačná bezpečnosť

Moderná spoločnosť postupne prechádza pri spracovávaní údajov k automatizácii. Výhodou automatizovaného spracovania informácií je predovšetkým možnosť spracovať veľké množstvá informácií. K tomu je potrebné využívať informačné systémy založené na informačných a komunikačných technológiách (IKT). Takýto systém sa skladá z hardvéru, kam patria nielen počítače, ale aj ostatné zariadenia, či káble, zo softvéru - operačných systémov a aplikácií, a z dát - informácií, ktoré systém spravuje. Jeho prevádzka je závislá od ďalších faktorov, akými sú hlavne fyzická organizácia systému, rozmiestnenie hardvéru, spôsob softvérového riešenia systému a v neposlednom rade aj technické a legislatívne normy, pravidlá, zvyklosti a skúsenosti. Súhrn takýchto faktorov, ktoré nejakým spôsobom ovplyvňujú chod

a funkčnosť systému, nazývame bezpečnostné okolie systému. Patria sem všetky entity nachádzajúce sa mimo systému. Väčšinou sa zaujímame iba o také okolie, s ktorým systém vzájomne interaguje. Pomyselnú deliacu čiaru medzi systémom a jeho okolím budeme nazývať hranica IKT systému. IKT systémy je potrebné podrobne popísať, aby bolo možné zabezpečiť ich spoľahlivosť, ochranu a bezpečnosť. IKT systém popisujeme na rôznych úrovniach abstrakcie, aby sme sa vyhli zbytočne zložitým popisom, ktoré sú nie vždy žiadané. IKT systémy sa popisujú na základe medzinárodných štandardov. Každý štandard musí byť podložený certifikátom. V súčasnosti sa používa štandard ISO/IEC 15408, ktorý je podrobne popísaný v prílohe Common Criteria [4,5,6,7]. Rovnako sa v prílohe nachádza aj metodika založená na tomto štandarde [8,9] a metodické materiály amerického Národného inštitútu pre štandardy a technológie (NIST - National Institute of Standards and Technology) [10,11,12].

### 3.1.1 Informačný a komunikačný systém

Informačný a komunikačný systém definujeme ako systém technických a programových prostriedkov, ktorých úlohou je zber, prenos, spracovanie, ukladanie a uchovanie informácií. Je zriadený pre dosahovanie určených cieľov a plnenie definovaných úloh. IKT systém tvorí logický celok, ktorý obsahuje samostatné časti, nazývané položky - assets. Položkami môžu byť aj nemateriálne entity, údaje, znalosti, dobré meno organizácie, či schopnosť poskytovať služby.

Hrozba je akákoľvek udalosť, ktorej následkom je odchýlka od pravidiel, upravujúcich činnosť IKT systémov. Ak takáto udalosť nastane, hovoríme, že hrozba bola naplnená, prišlo k bezpečnostnému incidentu. O naplnenie hrozby, prípadne jej využitie, sa možu pokúšať aj konkrétne osoby, v takomto prípade ide o útok, osoby označujeme za útočníkov. Okrem incidentov zapríčinených vedomým konaním ľudí, môže nastať situácia, kedy dôjde k naplneniu hrozby v dôsledku neúmyselného konania, prípadne v dôsledku technickej poruchy. Osoba, zariadenie alebo skutočnosť, ktorá zapríčinila naplnenie hrozby sa označuje pojmom nositeľ hrozby. Výsledky uskutočnenia hrozby nazývame dopady alebo dôsledky.

Aby mohli nastať bezpečnostné incidenty, je potrebné, aby mal systém tzv. slabé miesta - zraniteľnosti. Sú to vlastnosti, nedostatky alebo riešenia systému, ktoré umožňujú hrozbu realizovať. Každý bezpečnostný incident nastáva s určitou pravdepodobnosťou a má pre systém nejaké dôsledky. Oba

tieto faktory sa súhrnne označujú ako bezpečnostné riziko. Riziko je strednou hodnotou dôsledkov naplnenia hrozby, narastá s rastúcou pravdepodobnosťou naplnenia hrozby ako aj s rastúcim rozsahom dôsledkov pri naplnení hrozby.

Pri popise každého IKT systému je dôležitá analýza rizík - odhad pravdepodobnosti výskytu bezpečnostných incidentov a analýza dopadu a dôsledkov týchto incidentov na systém. Rovnako dôležité je aj definovať bezpečnostné opatrenia, teda pravidlá a prostriedky na elimináciu rizík a zníženie pravdepodobnosti naplnenia hrozieb. Podľa rizika možno hrozby rozdeliť do troch základných skupín - kritické, stredne závažné a nepodstatné. Podľa charakteru hrozby sa potom navrhujú, realizujú a kontrolujú konkrétne bezpečnostné opatrenia.

### 3.1.2 Ciele informačnej bezpečnosti

Úlohou informačnej bezpečnosti je však nielen ochrana systému, ale aj ochrana informácií, ktoré systém spracováva a uchováva. Základné ciele informačnej bezpečnosti sú integrita údajov, dôvernosť údajov, dostupnosť, autentickosť, nepopierateľnosť konania a časová súslednosť.

Integrita údajov zaručuje, že údaje sa počas ich prenosu nezmenia, či už úmyselným konaním tretej osoby, alebo v dôsledku zníženej kvality prenosového kanála, či iných faktorov. Rovnako u uložených či zálohovaných údajoch treba zamedziť neautorizovaným zmenám obsahu. Aby bolo možné zaručiť integritu údajov, je potrebné, v čo najväčšej miere zabrániť zmenám prenášaných údajov. Vo všeobecnosti nie je možné na 100% zamedziť poškodeniu, či zmene údajov dôsledkom technických chýb alebo nepriaznivých vplyvov prostredia. Do istej miery možno chyby vzniknuté vplyvom prostredia eliminovať použitím samoopravných kódov, ktoré sú schopné detekovať a opraviť chyby malého rozsahu. Pre zaistenie integrity údajov je rovnako potrebná schopnosť všetkých komunikujúcich strán identifikovať prípadné zmeny v prenášaných údajoch. Takúto schopnosť dosahujeme pomocou hašovacích funkcií, hašovacích funkcií s tajným kľúčom a elektronických podpisov.

IKT systémy veľakrát pracujú s údajmi, ktoré sú určené len pre istú skupinu ľudí. Je dôležité, aby prístup k takýmto informáciám mali len oprávnené osoby. Hovoríme, že tieto informácie sú dôverné. Zamedziť prístupu neoprávnených osôb k údajom a tým ich kompromitácii, teda zabezpečiť dôvernosť údajov, možno metódou riadenia prístupu. Prístup k údajom je povolený len

oprávneným osobám. Spoľahlivejšia metóda je šifrovanie. Zamedzuje útočníkom prístup k údajom aj v prípade neoprávneného odpočúvania komunikačného kanála, čo prvá metóda zabezpečiť nedokáže.

Dostupnosť informácií znamená, že informácie sú oprávneným osobam k dispozícii vtedy, keď ich potrebujú, v požadovanom rozsahu a na určenom mieste. Dostupnosť údajov nie je možné zabezpečiť za každých okolností. Dôsledkom úmyselných útokov, vplyvov prostredia, či technických porúch môžu nastať situácie, kedy sa údaje stanú dočasne nedostupnými. V niektorých prípadoch, ako sú napríklad trvalé poškodenia pevných diskov, sa informácie môžu stať nedostupnými natrvalo. Keď sa hovorí o dostupnosti, vždy je potrebné určiť maximálny čas, počas ktorého sa vzniknuté príčiny nedostupnosti údajov odstránia a obnoví sa oprávneným osobám prístup k informáciám. Dostupnosť je väčšinou zabezpečovaná použitím záložných zdrojov, zálohovaním, archivovaním alebo zrkadlením údajov na diskových poliach.

Pod autentickosťou rozumieme schopnosť spoľahlivo určiť pôvod informácií, overiť identitu osoby, ktorá dokument vytvorila, a pritom zaručiť, že dokument nebol pozmenený, a to dokonca ani samotným autorom dokumentu. Prostriedkom na zabezpečenie autentickosti údajov je elektronický podpis. Závisí totiž od obsahu dokumentu, čím je zabezpečené, že informácia sa nezmení, a na jeho vytvorenie je potrebná znalosť súkromného kľúča autora, čím je zabezpečená identifikácia autora dokumentu.

Nepopierateľnosť konania zaručuje, že osoba zúčastnená na komunikácii, prípadne modifikácii údajov, nie je schopná poprieť vykonanie daných akcií. Inými slovami, v prípade potreby je možné dokázať, že konkrétnu akciu vykonala konkrétna osoba. Napríklad takto nie je možné odmietnuť vykonanú objednávku tovaru, alebo chybu pri editácii a zmene údajov, či už úmyselnú alebo neúmyslenú.

Časová súslednosť umožňuje odhaliť existenciu údajov v čase a zistiť postupnosť vykonávania akcií, určiť ich vzájomnú súslednosť. Najjednoduchším riešením je pridať k informácii údaj o aktuálnom čase. Treba však ošetriť prípadnú nezosynchronizovanosť jednotlivých subjektov pracujúcich s informáciami.

### 3.1.3 Bezpečnostné funkcie a požiadavky

Spomenuté ciele dosahujeme pomocou bezpečnostných funkcií. Samozrejme, nie vždy vyžadujeme všetky ciele naraz. Funkcionálne bezpečnostné požiadavky určujú, ktoré bezpečnostné funkcie má IKT systém poskytovať. Re-

alizácia funkcií poskytovaných systémom nemusí byť dostatočná, prípadne môže byť chybná. Dôveryhodné systémy musia spĺňať popri funkcionálnych bezpečnostných požiadavkách aj požiadavky na bezpečnostné záruky. Ich úlohou je poskytnúť dôveru, že bezpečnostné funkcie sú dostatočné a správne implementované. Oba typy bezpečnostných požiadaviek, definovanie ich tried a rozdelenie na jednotlivé úrovne, ako aj závislosti a vzťahy medzi nimi sú podrobne popísané v Common Criteria [4,5,6,7].

### 3.1.4 Bezpečnostný zámer

Profil ochrany - Protection profile je bezpečnostný model abstraktného systému. Jeho cieľom je zistiť bezpečnostné problémy danej množiny systémov a produktov označovaných za cieľ ohodnotenia - Target of Evaluation (TOE) a špecifikovať bezpečnostné požiadavky na systém bez toho, aby diktoval, ako presne budú tieto požiadavky implementované. Definuje štandardnú množinu požiadaviek, ktoré by mali systémy TOE spĺňať. Môže byť navrhnutý pre konkrétne typy TOE systémov, ale aj pre rôzne množiny systémov, ktoré sa potom spájajú do kombinovaných TOE systémov alebo produktov. Protection profile je základom pre vypracovanie bezpečnostného zámeru.

Množina bezpečnostných požiadaviek a špecifikácií IKT systému sa nazýva bezpečnostný zámer - security target. Vychádza z Protection profile, ale na rozdiel od neho, obsahuje ďalsie informácie o presnej implementácii bezpečnostných požiadaviek, popisuje ako sú realizované v rámci konkrétneho produktu alebo systému. Pre systém, ktorý spĺňa požiadavky definované v Protection profile, je na základe tohto profilu vytvorený bezpečnostný zámer, ktorý demonštruje ako je systém implementovaný, ako pracuje, aby vyhovoval bezpečnostným požiadavkám.

## 3.2 Kryptológia

Pri komunikácii dvoch subjektov, si tieto medzi sebou posielajú informácie väčšinou zapísané v podobe textu. Takto posielaný text, ktorého obsahom je daná informácia, nazývame správa alebo údaj. Matematicky je správa postupnosť slov nad abecedou $\Sigma$. Takáto správa sa posiela od jedného účastníka komunikácie k druhému pomocou prenosového kanála. Takto prenášanú správu môže zachytiť protivník odpočúvajúci komunikáciu. Aby sa predišlo

zneužitiu alebo modifikácii informácie uloženej v správe týmto útočníkom, je potrebné, aby sa správa neposielala po prenosovom kanáli v otvorenom tvare, ale aby bola šifrovaná.

### 3.2.1 Šifrovanie

Šifrovanie je metóda transformácie otvoreného textu na šifrový text pomocou vhodne zvoleného šifrovacieho algoritmu tak, aby bol zachovaný obsah (informácia), ale zmenená formu zápisu (text správy). Takto útočník nie je schopný získať zo zachytenej správy informáciu. Avšak toto musí byť umožnené adresátovi správy, ktorý dokáže bezchybne dešifrovať prichádzajúci šifrový text späť na odosielateľom odoslaný otvorený text. Aby sme želaný efekt dosiahli, požívame pri šifrovaní kľúče. Kľúč je popri správe jedným zo vstupov šifrovacieho algoritmu a pomocou neho algoritmus spracuje správu. Rovnako je znalosť kľúča potrebná aj pri dešifrovaní zašifrovanej správy.

"Kryptológia sa delí na dve časti - kryptografiu a kryptoanalýzu."[2] Obidve časti môžeme prezentovať ako samostatné vedné disciplíny. Zatiaľčo kryptografia sa zaoberá hlavne tvorbou šifier, návrhom šifrovacích algoritmov a bezpečnostných protokolov, kryptoanalýza skúma možné hrozby a možnosti útokov na tieto štruktúry, ale aj spôsoby, ako dešifrovať zašifrovaný text.

Šifrovacie algoritmy môžeme zaradiť do dvoch základných skupín. Jednou sú algoritmy symetrického kryptosystému, na druhej strane ide o algoritmy asymetrického kryptosystému. Rozdiel medzi týmito dvoma typmi je v použití kľúča.

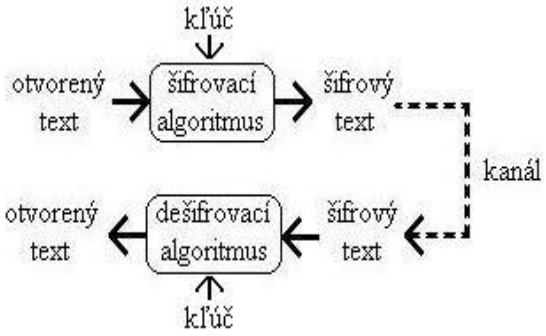
### 3.2.2 Symetrické šifrovanie

Pri symetrickom šifrovaní sa na šifrovanie a rovnako aj na dešifrovanie použije ten istý kľúč. Z tohto dôvodu je nevyhnutnosťou, aby bol kľúč tajný, a aby ho poznali len oprávnené osoby, teda osoby, ktoré medzi sebou komunikujú. Predstavme si ale, že chceme zabezpečiť komunikáciu viac ako dvoch účastníkov, pričom vyžadujeme, aby každá jedna dvojica bola schopná súkromnej komunikácie. V takom prípade by sme museli mať samostatný kľúč pre každú z dvojíc. Pre komunikáciu n účastníkov by sme teda potrebovali $\binom{n}{2}$ rôznych kľúčov, pričom každý účastník by musel disponovať (n-1) rôznymi kľúčmi - pre každú osobu, s ktorou by chcel komunikovať, by musel

použiť iný kľúč. Takéto riešenie je neprehľadné, zložité na realizáciu a vedie k chybám.

### 3.2.3 Asymetrické šifrovanie

Pri použití symetrického šifrovania musia adresát aj odosielateľ poznať tajný kľúč. Ak ale chceme, aby mohol správu adresátovi poslať ktokoľvek, teda aj osoba, ktorú adresát nepozná, bolo by pri takomto spôsobe šifrovania potrebné zverejniť adresátov šifrovací kľúč. Tým by sa narušila dôvernosť všetkých šifrových správ, zašifrovaných pomocou toho istého kľúča. Pri asymetrickom šifrovaní je situácia odlišná. Používajú sa dva kľúče, jeden na šifrovanie, druhý na dešifrovanie. Tieto dva kľúče musia navzájom tvoriť pár, pričom ale jeden z druhého sa nedá odvodiť, a preto jeden môžeme zverejniť. Šifrovací kľúč nazývaný aj verejný, je známy a nie je potrebné jeho utajenie. Ktokoľvek je schopný zašifrovať ľubovoľnú správu, ktorú potom odošle príjemcovi. Avšak dešifrovací kľúč, nazývaný aj súkromný, je tajný a pozná ho len adresát správy. Samozrejme, tento tajný kľúč nesmie byť známy útočníkovi, aby nebolo možné prípadné dešifrovanie zachytených správ. Celá komunikácia je zjednodušene zobrazená na obrázku:




Obr.1 Takýmto spôsobom sa zabezpečuje dôvernosť prenášanej informácie.

### 3.2.4 Symetrický šifrovací systém

Popíšeme si šifrovacie algoritmy formálnejšie. Uvažujme tri konečné množiny - $P$ (množina otvorených textov), $C$ (množina šifrových textov) a $K$ (množina kľúčov). Symetrický šifrovací systém je potom dvojica $\langle E, D\rangle$, kde $E : P \times K \rightarrow C$ je šifrovacia funkcia a $D : C \times K \rightarrow P$ je jej dešifrovacia funkcia spĺňajúca podmienku $\forall k \in K\ \forall p \in P : D(E(p,k),k) = p$.

Medzi základné symetrické šifry patria Jednoduchá substitučná šifra, Permutačná šifra, či Vernamova šifra, ktoré však boli používané skôr v minulosti. V súčasnosti sa zo symetrických šifrovacích systémov používajú hlavne blokové a prúdové šifry. Ako príklad spomenieme Feistelovské šifry, konkrétne algoritmus DES (Data Encryption Standard) z roku 1977, ktorý bol neskôr nahradený algoritmom Rijndael, ktorý je od roku 2000 štandardom AES (Advanced Encryption Standard).

### 3.2.5 Asymetrický šifrovací systém

Označme $P$ množinu otvorených textov, $C$ množinu šifrových textov a $R$ množinu $\{0,1\}^*$. Asymetrický šifrovací systém je potom dvojica $\langle E, D\rangle$, kde $E : P \times R \to C$ je šifrovacia funkcia a $D : C \to P$ je jej dešifrovacia funkcia. Množina $R$ umožňuje náhodnú voľbu pri šifrovaní. Všimnime si ale, že funkcie $E$ a $D$ nie sú parametrizované prvkom z množiny kľúčov. Súkromný kľúč a k nemu prislúchajúci verejný kľúč totiž generujeme ešte pred definovaním šifrovacej a dešifrovacej funkcie. Tieto funkcie sú potom generované na základe konkrétnych kľúčov. Inými slovami, použitie funkcií je ekvivalentné použitiu kľúčov, keďže funkcie sú priamo závislé na vopred zvolených kľúčoch. Šifrovacia funkcia je verejná, dešifrovacia funkcia je naopak súkromná. Asymetrický šifrovací systém musí byť korektný (dešifrovaním šifrového textu dostaneme pôvodný otvorený text), realizovateľný (šifrovacia aj dešifrovacia funkcia musia byť efektívne realizovateľné) a bezpečný (zo znalosti len šifrovacej funkcie je prakticky nemožné túto funkciu invertovať, teda zistiť dešifrovaciu funkciu v reálnom čase).

K zástupcom asymetrických šifrovacích systémov patria RSA, Rabinov systém a ElGamalov systém. Ich bezpečnosť je založená na neschopnosti riešiť ťažké problémy akými sú problém faktorizácie (RSA, Rabin) a problém diskrétneho logaritmu (ElGamal). Podrobnejšie informácie o týchto úlohách, ako aj konkrétnejší popis spomínaných symetrických i asymetrických algoritmov možno nájsť v prílohe [3].

### 3.2.6 Manažment kryptografických kľúčov

Kľúče sú dôležitou zložkou pre zachovanie bezpečnosti šifrovacích systémov a ostatných kryptografických prostriedkov, ktoré kľúče využívajú. Bezpečnosť celého systému je priamo závislá od bezpečnosti kľúčov. Kľúče musia byť chránené pred modifikáciou a prezradením. Je dôležité zabezpečiť ich vhodné

spravovanie, utajenie a riadenie prístupu počas celého životného cyklu od ich vygenerovania, pri ich distribúcii, počas ich využívania a samozrejme aj po tom, ako sa prestanú používať, je potrebné zabezpečiť ich ochranu, archiváciu, alebo prípadnú likvidáciu. Manažment kľúčov definuje protokoly a procedúry na realizáciu všetkých spomínaných akcií.

### 3.2.7 Hašovacie funkcie

Pri práci s elektronickými dokumentami dochádza často k situácii, kedy je možné pre urýchlenie a zjednodušenie ich spracovania použiť namiesto pôvodného dokumentu len jeho kratšiu reprezentáciu. Takejto reprezentácii dokumentu, ktorá je obvykle podstatne kratšia ako originál, hovoríme haš alebo digitálny odtlačok. Funkciu $h : X \to Y$, použitú na vytvorenie odtlačku, nazývame kryptografická hašovacia funkcia. Množina odtlačkov $Y$ je konečná, od množiny vzorov $X$ to nepožadujeme. Hodnota $x \in X$ je potom pôvodný dokument a hodnota $h(x)$ je jeho digitálny odtlačok.

Hašovacie funkcie musia mať niektoré základné vlastnosti, aby mohli byť bezpečne použité v schémach digitálnych podpisov, pri kontrole integrity, alebo v kryptografických protokoloch. Najdôležitejšiou vlastnosťou hašovacích funkcií je jednosmernosť. Hovoríme, že hašovacia funkcia je jednosmerná, ak pre daný odtlačok $y = h(x)$ nie je možné efektívne nájsť vzor $x$. Druhou dôležitou vlastnosťou je odolnosť voči kolíziám. Kolízia nastáva vtedy, ak majú dva rôzne dokumenty rovnaký odtlačok. Vtedy by mohlo dôjsť k zneužitiu tohto faktu nahradením jedného dokumentu druhým, pričom odtlačok by ostal rovnaký. Rozlišujeme dva stupne odolnosti voči kolíziám. Slabá odolnosť znamená, že pre dané $x \in X$ nevieme efektívne nájsť $x' \in X \setminus \{x\}$ také, že $h(x) = h(x')$. Silná odolnosť znamená, že nevieme efektívne nájsť také dve rôzne $x, x' \in X$, že $h(x) = h(x')$. Aby mala hašovacia funkcia požadované vlastnosti, musí byť počet prvkov množiny $Y$ dostatočne veľký. Inak by sa ľahko hľadali kolízie, keby sme mali k dispozícii len obmedzene malý počet odtlačkov. Avšak ani príliš veľká hodnota $|Y|$ nie je dobrá, pretože pridlhé odtlačky môžu z hľadiska časovej zložitosti komplikovať ich použitie napríklad v schémach digitálnych podpisov.

V súčasnosti sa používajú nové hašovacie funkcie SHA-256, SHA-384 a SHA-512 (SHA - Secure Hash Algorithm), ktoré sú súčasťou štandardu SHS (Secure Hash Standard). Čísla 256, 384 a 512 určujú dĺžku vypočítaného digitálneho odtlačku v bitoch. Súčasťou štandardu aj staršia hašovacia funkcia SHA-1. Medzi často používané hašovacie funkcie patrí aj funkcia MD5.

# 4 Základy PKI

V nasledujúcej kapitole sa dozvieme viac o elektronickom podpise, jeho využití, o certifikátoch a infraštruktúre verejného kľúča.

## 4.1 Elektronický podpis

Podľa zákona č. 215/2002 Zbierky zákonov o elektronickom podpise a o zmene a doplnení niektorých zákonov zo dňa 15. marca 2002 :

"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) 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 použitím na jej vyhotovenie" [15].

Z takto formulovanej definície vyplýva, že nie je možné elektronický podpis jedného dokumentu pripojiť k inému dokumentu a získať tak korektne podpísaný dokument, a že nie je možné pozmeniť obsah podpísaného dokumentu a zachovať korektnosť elektronického podpisu. Ak chceme, aby nebolo možné poprieť autorstvo vlastného elektronického podpisu, musíme použiť zaručený elektronický podpis.

"Zaručený elektronický podpis je elektronický podpis, ktorý musí spĺňať podmienky podľa § 3:
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 podľa § 2 písm. h),
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" [15].

Elektronický podpis teda nie je len digitálny obrázok vlastnoručného podpisu, ako si mnoho ľudí myslí. Elektronický podpis je zväčša založený digitálnom podpise, teda na kryptografickom mechanizme, ktorý je prostriedkom na realizáciu niektorých bezpečnostných funkcií, hlavne integrity a autentickosti. Príjemca správy dokáže prostredníctvom zaručeného elektronického podpisu overiť, kto správu podpísal, a že informácia nebola po podpísaní modifikovaná. Na druhej strane odosielateľ nemôže poprieť podpísanie správy.

Elektronický podpis je informácia v elektronickej podobe. Aby nebolo možné elektronický podpis jednoducho pripojiť k ľubovoľnému dokumentu, aj k takému, ktorý podpisovateľ nepodpísal, je potrebné, aby elektronický podpis nebol závislý len na identite podpisujúceho, ale aj na dokumente, ktorý podpisuje.

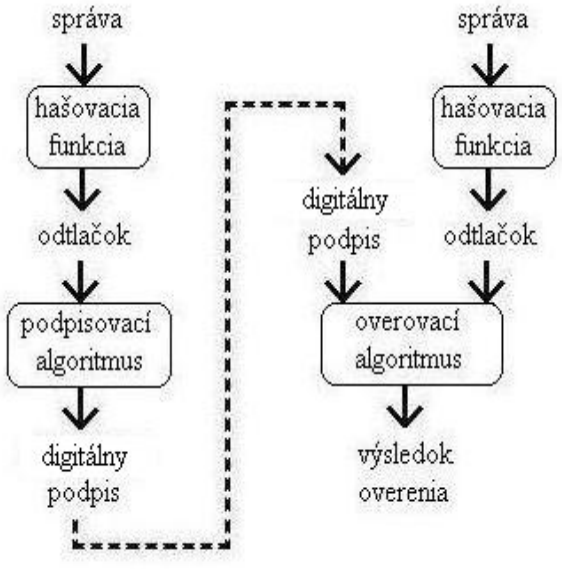
Elektronický podpis má za úlohu v prípade potreby nahradiť vlastnoručný podpis. Medzi týmito dvoma typmi podpisov ale existujú dva dôležité rozdiely, a to, že elektronický podpis nie je súčasťou podpisovaného dokumentu, ako je to pri vlastnoručnom podpise, ale je jeho prídavnou informáciou, a že elektronický podpis je možné kopírovať bez toho, aby sa akokoľvek zmenil, čo samozrejme pri vlastnoručnom podpise možné nie je. Aby nemohla byť táto skutočnosť zneužitá pripojením kópie elektronického podpisu k inému dokumentu, je potrebné, aby bol elektronický podpis viazaný na konkrétny dokument. Rovnako dôležité je zabezpečiť, aby nemohol byť elektronický podpis s dokumentom skopírovaný a použitý viackrát, napríklad príkaz na prevod peňazí v banke musí obsahovať aj dodatočnú informáciu, aby bola operácia vykonaná len raz.

### 4.1.1 Schémy digitálnych podpisov

Základom elektronických podpisov sú digitálne podpisy, teda výstupy podpisovacieho algoritmu. Digitálny podpis je dokument alebo haš dokumentu zašifrovaný pomocou súkromného kľúča podpisovateľa. Spôsoby vytvárania a overovania digitálnych podpisov sú definované v schémach digitálnych podpisov. Obsahujú popis algoritmu na podpisovanie a popis overovacieho algoritmu. Schémy digitálnych podpisov sú realizované v praxi pomocou systémov s verejnými kľúčmi a s použitím hašovacích funkcií. Namiesto celého dokumentu sa podpisuje len jeho digitálny odtlačok. Hašovacie funkcie používame hlavne z dôvodu zníženia časovej zložitosti asymetrických systémov,

vyhotovenie a podpísanie digitálneho odtlačku je podstatne rýchlejšie ako podpisovanie celého dokumentu. Druhým pozitívom pri použití hašovacích funkcií je ochrana informácií pred niektorými typmi útokov vďaka vlastnostiam, ktoré hašovacie funkcie majú - jednosmernosť a odolnosť voči kolíziám.

Na obrázku je znázornené, akým spôsobom sú vytvárané a overované digitálne podpisy :




Obr.2 Schéma vytvárania a overovania digitálneho podpisu.

### 4.1.2 RSA a ElGamalova schéma

Pri použití RSA schémy je digitálny podpis realizovaný rovnako ako asymetrický šifrovací systém RSA. Šifrovacia transformácia plní úlohu overovacieho algoritmu, zatiaľčo dešifrovacia transformácia slúži ako podpisovací algoritmus.

Použitie ElGamalovej schémy vyžaduje určité úpravy oproti ElGamalovmu asymetrickému systému, pretože šifrovacia a dešifrovacia transformácia nie sú navzájom inverzné. Pri vytváraní podpisov v ElGamalovej schéme treba dbať aj nato, aby nebola pri podpisovaní dvoch rôznych správ použitá rovnaká hodnota generátora náhodných čísel, pretože táto skutočnosť vedie k prezradeniu súkromného kľúča. Voľbe generátora náhodných čísel preto musíme venovať náležitú pozornosť.

Podrobný popis RSA a ElGamalovej schémy digitálnych podpisov sa nachádza v použitej literatúre [3].

### 4.1.3 DSA schéma

Súčasťou štandardu DSS (Digital Signature Standard)[13] je aj schéma DSA (Digital Signature Algorithm). DSA je schéma ElGamalovho typu, jej bezpečnosť je založená na probléme diskrétneho logaritmu. Štandard DSS používa pre DSA schému hašovaciu funkciu SHA-1, vytvárajúcu 160 bitov dlhý odtlačok. Pre ilustráciu uvediem aj formálny popis DSA. Inicializácia prebieha nasledovne :

1. Zvolíme náhodne 160 bitov dlhé prvočíslo $q$.
2. Zvolíme náhodne 1024 bitov dlhé prvočíslo $p$ také, že $q \mid (p-1)$.
3. Vypočítame $g = h^{(p-1)/q}$, kde $h \in_R \{2, 3, ..., p-2\}$ je náhodne zvolené číslo také, že platí $h^{(p-1)/q} > 1$.
4. Zvolíme $x \in_R Z_q^*$ a vypočítame $y = g^x \ mod \ p$.

Čísla $p$, $q$ a $g$ môžu byť spoločné aj pre väčšiu skupinu užívateľov. Štvorica $\langle y, p, q, g\rangle$ tvorí verejný kľúč, hodnota $x$ je súkromný kľúč. Spôsob, akým vypočítame $g$ zaručuje, že rád prvku $g$ v grupe $(Z_p^*, \cdot)$ je $q$.

Označme $m$ podpisovaný dokument, $H$ hašovaciu funkciu a $s$ digitálny podpis dokumentu. Digitálny podpis vytvoríme nasledovne :

1. Zvolíme náhodné $k \in_R \{1, ..., q-1\}$
2. Vypočítame $r = (g^k \ mod \ p) \ mod \ q$.
3. Vypočítame $s$ :

$$s = (H(m) + xr)k^{-1} \ mod \ q.$$

Ak pri výpočte nastane situácia, že dostaneme $r = 0$ alebo $s = 0$, je potrebné vygenerovať nové $k$ a výpočet opakovať. Táto možnosť je ale vysoko nepravdepodobná.
4. Digitálny podpis správy $m$ je dvojica $\langle r, s\rangle$.

Overovanie digitálneho podpisu k správe $m$ možno na základe znalosti verejného kľúča a digitálneho podpisu. Overovanie prebieha nasledovne :

1. Overíme, že $s, r \in Z_q^*$.

2. Vypočítame $u_1 = H(m) \cdot s^{-1} \; mod \; q$.
3. Vypočítame $u_2 = r \cdot s^{-1} \; mod \; q$.
4. Podpis je korektný práve vtedy, keď :

$$(g^{u_1} \cdot y^{u_2} \; mod \; p) \; mod \; q = r.$$

Digitálny podpis v DSA schéme je kratší ako v ElGamalovej a RSA schéme. Tento fakt zabezpečuje modulárne delenie parametrom $q$. Pritom je ale bezpečnosť týchto schém na rovnakej úrovni. Dôležité pri vytváraní digitálneho podpisu v DSA schéme je po použití parametra $k$ tento zabudnúť, pretože jeho znalosť vedie k odhaleniu súkromného kľúča $x$.

## 4.2 Právna úprava elektronického podpisu

Vytvorenie elektronického podpisu bolo veľkým plusom pre elektronickú komunikáciu. Užívatelia verejných sietí, najmä internetu, sa viac nemuseli obávať, či správa, ktorú obdržali, nebola počas prenosu poškodená, zmenená alebo inak úmyselne ale aj neúmyselne znehodnotená. Z právneho hľadiska len definovanie formátu elektronického podpisu nestačilo. Myšlienku elektronického podpisu bolo treba doviesť do reálnej podoby, a tým aj právne podchytiť a zakomponovať elektronický podpis, spôsob jeho vytvárania a overovania, jeho funkcie a vlastnosti, ako aj jeho právnu silu do zákona. Právnu formu elektronického podpisu na Slovensku stanovuje Zákon o elektronickom podpise a o zmene a doplnení niektorých zákonov č. 215/2002 Zb. [15] schválený NR SR 15. marca 2002. Účinnosť nadobudol 1. mája 2002, s výnimkou niektorých paragrafov, nadobúdajúcich účinnosť 1. septembra 2002.

Zákon č. 215/2002 Zb. o elektronickom podpise rozoznáva dva druhy elektronických podpisov - obyčajný elektronický podpis a zaručený elektronický podpis. Úlohou obyčajného elektronického podpisu je preukázať, že dokument bol podpísaný osobou, ktorá vlastní súkromný kľúč, teda že ide skutočne o osobu, o ktorej predpokladáme, že tento dokument podpísala. Zároveň poskytuje možnosť overenia, či počas prenosu nedošlo k modifikácii tohto dokumentu. Zaručený elektronický podpis, ktorý musí spĺňať kritériá dané v § 4 zákona č. 215/2002 Zb. [15] zaručuje popri integrite a autentickosti údajov aj nepopierateľnosť konania podpisovateľa. V styku so štátnymi úradmi sa musí používať tento druh elektronického podpisu. Podstatou zaručeného

elektronický podpisu je skutočnosť, že je vytváraný pomocou bezpečného zariadenia na vyhotovenie elektronického podpisu a na verejný kľúč je vydaný kvalifikovaný certifikát. Ak však určitá právna norma vyžaduje na právne úkony notárske osvedčenie podpisu, musí byť takto osvedčený i zaručený elektronický podpis.

## 4.3 Certifikáty a infraštruktúra verejného kľúča

Vďaka asymetrickým kryptosystémom je možné bezpečne oddeliť súkromný a verejný kľúč a zabezpečiť publikovanie verejného kľúča. Problém je ale v tom, ako sa osoba, ktorá chce overiť nejaký podpis, dostane k verejnému kľúču pre tento podpis. Utajenie kľúča nie je potrebné, avšak musíme zabezpečiť, aby kľúč nemohol niekto modifikovať pred alebo počas prenosu k overovateľovi. Potenciálny útočník by mohol overovateľovi preposlať namiesto verejného kľúča podpisovateľa svoj verejný kľúč a týmto kľúčom podpísanú upravenú správu namiesto pôvodnej správy bez toho, aby túto skutočnosť overovateľ odhalil, keďže overenie podpisu v takomto prípade prebehne bez problémov. V súčasnosti sa na distribúciu a prenos kľúčov od podpisovateľa k overovateľovi využíva metóda dôveryhodnej tretej strany - Trusted Third Party (TTP). TTP poskytuje overovateľovi službu, ktorá mu potvrdí, že daný verejný kľúč skutočne patrí podpisovateľovi. Dôležité je, že dôveryhodnej tretej strane veria obaja účastníci, teda podpisovateľ aj overovateľ.

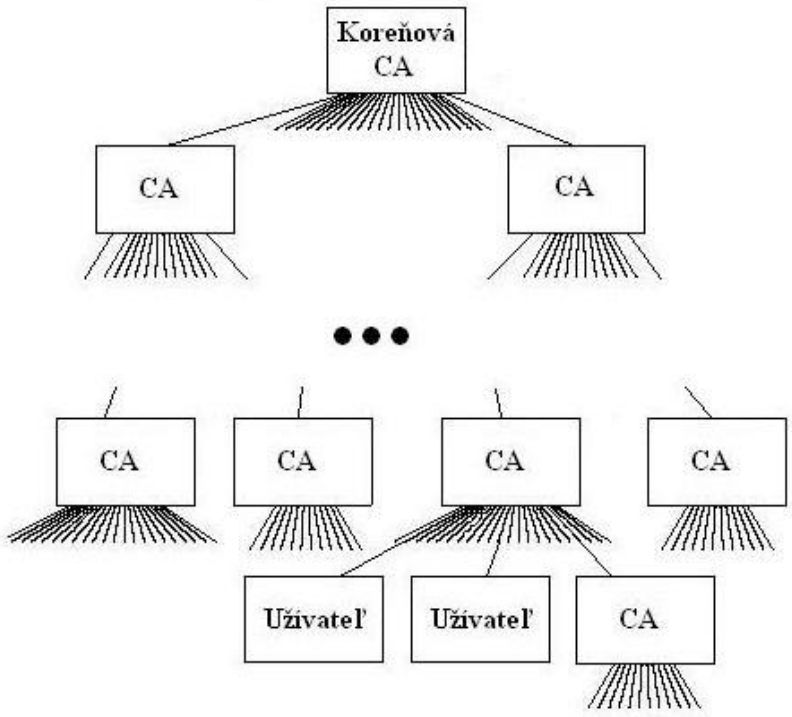
### 4.3.1 Certifikát verejného kľúča

Momentálne najrozšírenejšou schémou, ktorá implementuje metódu využitia TTP, je použitie certifikátov. Certifikát verejného kľúča je elektronický dokument, ktorý viaže verejný kľúč k identite jeho držiteľa. Podľa § 6 zákona č. 215/2002 Zb. [15], certifikát verejného kľúča je potvrdenie, že kľúč z certifikátu patrí danej osobe.

### 4.3.2 Certifikačná autorita

Certifikačná autorita je dôveryhodná tretia strana, ktorá je zodpovedná za vydávanie, správu a rušenie certifikátov verejného kľúča. Certifikačné autority sú zoradené do štruktúr. Niekedy sa môžu využívať aj štruktúry typu

všeobecných orientovaných grafov, väčšinou sú však využívané hierarchické štruktúry tak, ako je zobrazené na obrázku :




Obr.3 Hierarchická štruktúra certifikačných autorít.[19]

Certifikačná autorita, ktorá inej certifikačnej autorite, prípadne užívateľovi, vydala a podpísala certifikát, sa nachádza na vyššej úrovni ako táto certifikačná autorita či užívateľ. Na vrchole každej hierarchickej štruktúry stojí koreňová certifikačná autorita. Na Slovensku zastáva miesto koreňovej certifikačnej autority Národný bezpečnostný úrad (NBÚ).

Podľa § 10 zákona č. 215/2002 Zb. [15] vykonáva NBÚ na Slovensku okrem iného aj dohľad nad dodržiavaním zákona o elektronickom podpise, udeľuje a odníma certifikačným autoritám akreditáciu, vydáva osvedčenia o akreditácii a eviduje certifikačné autority pôsobiace v Slovenskej Republike.

Každá certifikačná autorita poskytuje certifikačné služby, spravuje certifikáty a vykonáva certifikačnú činnosť. Certifikačnou službou sa rozumie

najmä vydávanie certifikátov, zrušovanie platnosti certifikátov, poskytovanie zoznamu zrušených certifikátov, potvrdzovanie existencie a platnosti certifikátov, vyhľadávanie a poskytovanie vydaných certifikátov. Okrem poskytovania týchto služieb sa pod certifikačnou činnosťou rozumie aj prijímanie žiadostí o vydanie certifikátu, vedenie evidencie, či prevádzka potrebných technických zariadení.

Medzi služby poskytované certifikačnou autoritou patrí aj registrácia užívateľov. Užívatelia sa musia predtým, ako im bude vydaný certifikát, registrovať u certifikačnej autority. Po overení identity užívateľa, mu certifikačná autorita pridelí jednoznačné meno, pod ktorým bude môcť vytvárať elektronické podpisy. V prípade, že užívateľ z ľubovoľného dôvodu nechce podpisovať dokumenty svojím menom, môže požiadať o pridelenie pseudonymu, ktorý bude používať pri podpisovaní namiesto svojho mena.

Ešte predtým ako je možné vydať nejaký certifikát je potrebné vygenerovať kľúče, konkrétne je potrebné vygenerovať pár - súkromný kľúč a verejný kľúč. Žiadny konkrétny pár nesmie byť vygenerovaný viac ako jedenkrát. Samozrejme, je potrebné zamedziť neautorizovanému prístupu k páru kľúčov. Párové údaje sú generované na základe vybranej metódy generovania kľúčov, ktorá zodpovedá príslušnému štandardu pre elektronické podpisy. Pár kľúčov musí byť vytvorený vo vhodnom bezpečnom prostredí, teda na zariadení, ktoré spĺňa požiadavky na vyhotovovanie zaručených elektronických podpisov podľa zákona č. 215/2002 Zb. [15] a bolo pre tento účel certifikované NBÚ. Toto zariadenie je počas generovania kľúčov zásadne pod výhradnou kontrolou užívateľa. Vygenerovaný súkromný kľúč v ňom zostáva uložený i počas práce s ním, pričom je garantované, že súkromný kľúč nikdy zariadenie neopustí. Takýmto zariadením môže byť špeciálna čipová karta alebo USB token.

Ak už je pár kľúčov vygenerovaný, certifikačná autorita overí potrebné náležitosti žiadateľa o vydanie certifikátu (doklady, vlastníctvo súkromného kľúča patriaceho k predloženému verejnému kľúču) a následne vydá žiadateľovi certifikát verejného kľúča. Každý certifikát vydaný užívateľovi musí obsahovať jeho identifikáciu, jeho verejný kľúč a dobu platnosti certifikátu. Tieto informácie podpíše certifikačná autorita svojím elektronickým podpisom. Tým berie na seba zodpovednosť za obsah vydaného certifikátu.

Vydaný certifikát verejného kľúča je zvyčajne uložený na čipovej karte spolu so súkromným kľúčom užívateľa. Prístup k informáciám na čipovej karte je zabezpečený väčšinou pomocou hesla alebo PIN kódu, no môže byť zabezpečený aj biometrickou identifikačnou metódou, napríklad pomocou geometrie odtlačkov prstov, dúhovky, či sietnice.

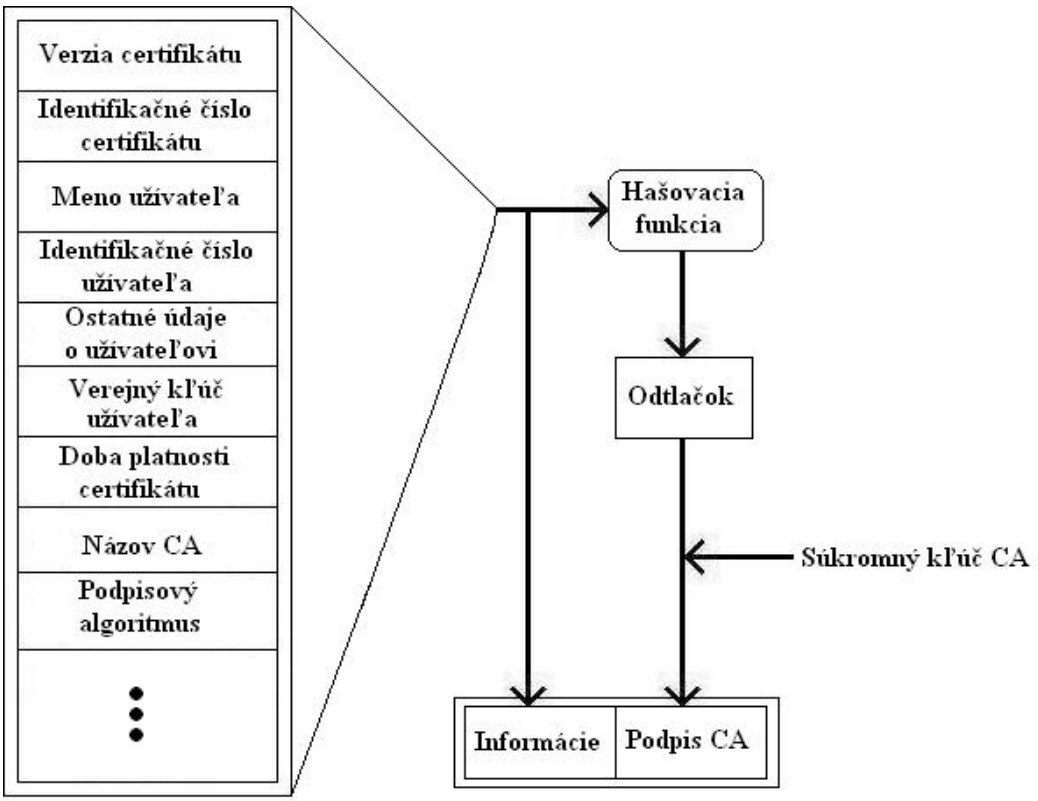
Povinnosťou každej certifikačnej autority je vytvoriť podmienky, ktoré umožnia overovateľovi overiť platnosť certifikátu, ktorý certifikačná autorita vydala. Zrušené certifikáty sú uvádzané na zozname zrušených certifikátov - Certificate revocation list (CRL), ktorý obsahuje aj informáciu o čase, kedy bol ten ktorý certifikát zrušený. Certifikačná autorita musí pravidelne vydávať zoznam ňou zrušených certifikátov. Certifikačná politika danej certifikačnej autority určuje, ako často bude CRL vydávaný. Tieto zoznamy zrušených certifikátov musia byť prístupné komukoľvek a kedykoľvek. Spôsob zverejňovania CRL je definovaný certifikačnou politikou danej certifikačnej autority.

V niektorých prípadoch je potrebné pripojiť k podpisovanému dokumentu aj časovú pečiatku - informáciu o aktuálnom čase, kedy bol dokument podpísaný. Túto informáciu je možné v prípade potreby overiť, teda určiť čas, kedy bol dokument podpísaný. Keďže nastavenie aktuálneho času môže mať každý užívateľ vo svojom systéme rôzne, je potrebné zabezpečiť synchronizáciu medzi jednotlivými užívateľmi. Z tohto dôvodu sa vydávanie časových pečiatok presunulo do kompetencie certifikačných autorít, ktoré zaručujú jednotnosť časových údajov pre všetkých užívateľov.

### 4.3.3 Infraštruktúra verejného kľúča

Systém usporiadania certifikačných autorít, normy a pravidlá pre vydávanie a používanie certifikátov verejného kľúča a systém publikácie kľúčov súborne nazývame infraštruktúra verejného kľúča - Public key infrastructure (PKI). Dve základné operácie spoločné pre všetky PKI sú správa certifikátov a overovanie platnosti certifikátov.

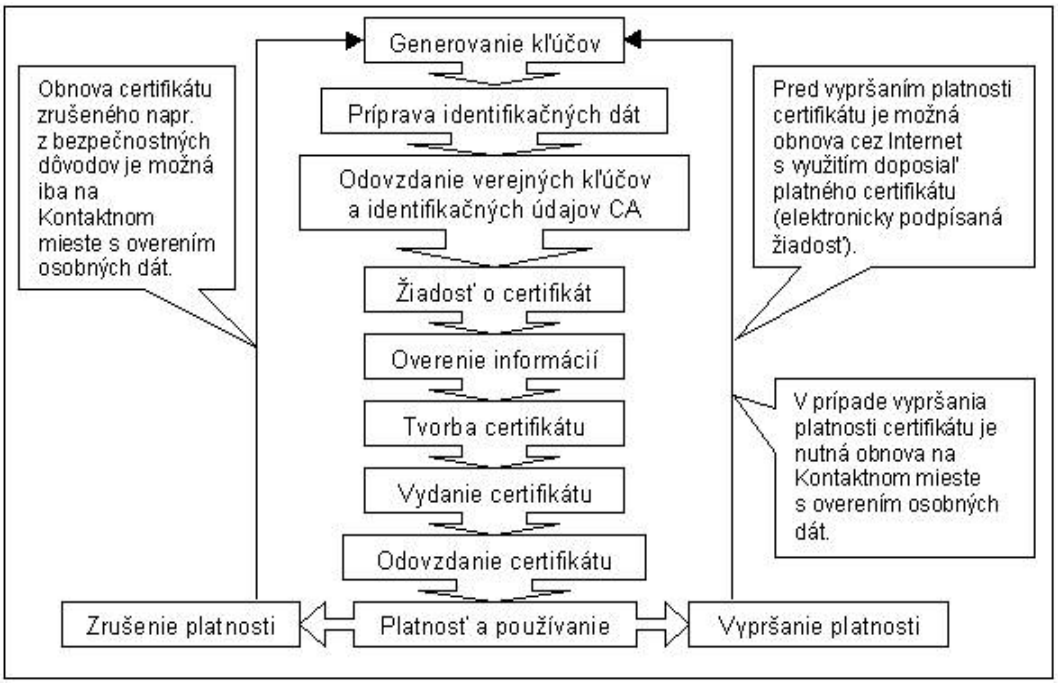
Podľa medzinárodného štandardu ISO X.509 pre PKI musí každý certifikát obsahovať verejný kľúč, jednoznačnú identifikáciu držiteľa certifikátu, jeho meno, dobu platnosti certifikátu, identifikáciu vydávateľa certifikátu a ním vytvorený elektronický podpis, ktorý zaručuje platnosť údajov uvedených v certifikáte. Štruktúra certifikátu je zobrazená na obrázku :




Obr.4 Certifikát verejného kľúča.[22]

Z toho, ako bol certifikát navrhnutý, vyplýva, že ak chce overovateľ zistiť, či sú údaje v certifikáte správne a platné, musí mať k dispozícii verejný kľúč certifikačnej autority - vydávateľa certifikátu a musí byť schopný overiť jej podpis. Ak overovateľ nepozná verejný kľúč vydávateľa certifikátu, má možnosť dozvedieť sa tento kľúč z certifikátu vydávateľa. Hierarchická štruktúra certifikačných autorít zaručuje konečnosť tejto rekurzie získavania verejných kľúčov jednotlivých vydávateľov certifikátov. Posledným krokom je získanie verejného kľúča koreňovej certifikačnej autority (ktorá je všeobecne dôveryhodná). Nie vždy musí cyklus končiť až pri koreňovej CA. Ak sa overovateľ v hierarchii dostane k certifikačnej autorite, ktorú pozná (napr. v minulosti overoval jej certifikát, alebo je to CA, ktorá mu vydala certifikát), nie je potrebné postupovať vyššie, cyklus sa v tomto bode zastaví. Hovoríme, že cyklus sa zastavil v bode dôvery. Takýchto bodov dôvery môže overovateľ poznať relatívne veľa.

Pri vytváraní certifikátu je potrebné dodržať určité štandardné postupy a zachovať následnosť jednotlivých akcií, ktoré s certifikátom vykonávame. Celý proces je zobrazený na obrázku :




Obr.5 Životný cyklus certifikátu verejného kľúča.[42]

V prvom kroku sa pomocou čipovej karty alebo USB tokenu vygeneruje pár kľúčov. Okrem toho musí užívateľ odovzdať certifikačnej autorite svoje identifikačné údaje. Ak si užívateľ splní všetky spomenuté povinnosti, môže požiadať o vydanie certifikátu.

V tejto chvíli vstupuje do hry certifikačná autorita. Overí identitu a ostatné informácie odovzdané užívateľom. Rovnako overí, že súkromný kľúč užívateľa tvorí pár k predloženému verejnému kľúču. Ak všetky kroky prebehnú bezproblémovo, certifikačná autorita vytvorí certifikát a vydá ho užívateľovi. Odovzdanie certifikátu prebieha pomocou čipovej karty či iného média. Od tejto chvíle môže užívateľ vytvárať elektronické podpisy.

Platnosť každého certifikátu nie je neobmedzená a dokonca je ju možné ukončiť aj predčasne, ak je na to dôvod. Kvôli prehľadnosti a možnosti overiť platnosť konkrétneho certifikátu, každá certifikačná autorita je povinná pravidelne vydávať zoznamy zrušených certifikátov. Platnosť jedného certifikátu

je v Slovenskej republike 12 mesiacov. Pred vypršaním platnosti je možné certifikát obnoviť elektronicky podanou žiadosťou podpísanou podpisom z ešte platného certifikátu. Po vypršaní platnosti alebo po zrušení certifikátu je pre jeho obnovenie nutné navštíviť kontaktné miesto certifikačnej autority a podať žiadosť o obnovu osobne. Všetky zrušené certifikáty aj so žiadosťami sa archivujú najmenej 10 rokov. Podrobnejší popis jednotlivých etáp životného cyklu certifikátu ako aj infraštruktúry verejného kľúča je popísaný v použitej literatúre [19,20,21,22].

## 4.4 Formáty elektronických podpisov

V praxi sa ukázalo, že jediný formát zaručeného elektronického podpisu je nedostačujúci na veľké množstvo rôznorodých právnych účelov. Zaručený elektronický podpis má preto viacero rôznych formátov, ktorých použitie závisí od toho, na aký účel elektronický podpis slúži. Jednotlivé formáty vymedzuje Vyhláška Národného bezpečnostného úradu č. 537/2002 Zb. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky [16] a presne špecifikuje dokument Formáty zaručených elektronických podpisov [23] vydaný NBÚ. Zaručený elektronický podpis musí byť kompatibilný v rámci celej SR a EÚ tak, aby uznával rovnaké právne požiadavky na podpis vo vzťahu k údajom v elektronickej forme rovnako ako vlastnoručný podpis vo vzťahu k papierovým dokumentom a aby bol prijateľný ako dôkaz pri súdnych sporoch. Formáty zaručených elektronických podpisov sú :

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

Zaručený elektronický podpis bez časovej pečiatky je najjednoduchším formátom zaručených elektronických podpisov. Obsahuje identifikátor podpisovej politiky použitej pri podpisovaní a overovaní podpisu, podpisové údaje, ktoré podpisujúci do podpisu zahrnul (napríklad miesto a čas vyhotovenia podpisu, meno podpisujúcej osoby) a samotný digitálny podpis vytvorený na základe digitálneho odtlačku dokumentu, identifikátora podpisovej politiky a údajov zahrnutých do podpisu.

Zaručený elektronický podpis s časovou pečiatkou má formu zaručeného elektronického podpisu, ku ktorému je pripojená časová pečiatka vyhotovená na základe daného zaručeného elektronického podpisu.

Zaručený elektronický podpis s úplnou informáciou pre overenie platnosti má formu zaručeného elektronického podpisu s časovou pečiatkou, ku ktorému sú pripojené úplné informácie o všetkých kvalifikovaných certifikátoch verejného kľúča potrebných na overenie platnosti podpisu, ako aj úplné informácie o zoznamoch zrušených kvalifikovaných certifikátov, alebo informácie o stave kvalifikovaných certifikátov potrebných na overenie platnosti podpisu.

Archívny zaručený elektronický podpis má formu zaručeného elektronického podpisu s časovou pečiatkou, ku ktorému sú pripojené všetky údaje potrebné na overenie archívneho zaručeného elektronického podpisu. Na tieto údaje je vyhotovená časová pečiatka, ktorá je k nim pripojená.

Vymedzenie technických požiadaviek na jednotlivé formáty zaručených elektronických podpisov a ich podrobná špecifikácia sú popísané v použitej literatúre [23].

## 4.5 Štandardy pre elektronické podpisy

Štandardy pokrývajúce šifrovací systém RSA, Diffieho-Hellmanov protokol na výmenu kľúčov, certifikáty verejných kľúčov, algoritmy na šifrovanie, dešifrovanie, podpisovanie a na tvorbu digitálnych odtlačkov, ktoré v roku 1993 vydali RSA Laboratories (dnes už súčasťou súkromnej firmy RSA Security) sa označujú za štandard PKCS - Public Key Cryptography Standards. Štandard PKCS sa delí na viac častí - noriem. Norma PKCS#1 napríklad popisuje postup šifrovania dát pomocou kryptosystému RSA, zatiaľčo norma PKCS#7 popisuje spôsob formátovania správ. V použitej literatúre [24-34] možno nájsť všetky dnes existujúce normy PKCS.

Stratégia riešenia problematiky elektronického podpisu z legislatívneho hľadiska v rámci Európskej únie je súčasťou štandardov EESSI - European Electronic Signature Standardisation Initiative. Záverečná správa EESSI [35] obsahuje identifikáciu požiadaviek, analýzu potrieb v oblasti štandardizácie a riešenia problémov súvisiacich s praktickou aplikáciou elektronických podpisov, certifikátov a poskytovateľov certifikačných služieb v krajinách EÚ.

Štandardy týkajúce sa elektronického podpisu a ostatné informácie o formátoch elektronických podpisov sú pravidelne vydávané ETSI (European Telecommunications Standards Institute) ako technické štandardy TS 101 733. Najnovšie verzie v1.5.1 a v1.7.3 možno nájsť v použitej literatúre [36,37].

# 5 Archívny elektronický podpis

Pre plnohodnotné využívanie elektronických podpisov bolo potrebné vytvoriť certifikáty, infraštruktúry verejných kľúčov a stanoviť úlohy pre jednotlivé subjekty komunikácie. S používaním elektronických podpisov nastali po niekoľkých rokoch ich používania problémy. Začali sa množiť certifikáty, vzniklo množstvo nových certifikačných autorít, zoznamy zrušených certifikátov sa rozrastali. Všetky tieto informácie však museli byť dostupné a archivované. Archivácia certifikátov, žiadostí o certifikáty, pravidelne vydávaných zoznamov zrušených certifikátov a ostatných informácií bola pre certifikačné autority stále náročnejšia úloha. Je potrebné, aby tieto informácie boli dostupné aj niekoľko desiatok až stoviek rokov. Napríklad zdravotná dokumentácia pacienta musí byť u všeobecného lekára podľa Zákona č. 576/2004 Zb. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov [38] archivovaná ešte 20 rokov po smrti pacienta. Samozrejme, nie každá certifikačná autorita má takú dlhú životnosť. A tak by sa mohlo stať, že elektronický podpis, ktorý bol vytvorený pred dlhšou dobou, už nie je možné overiť z dôvodu nedostupnosti potrebných informácií. V niektorých prípadoch môže dôjsť ku kompromitácii CA, prípadne algoritmy použité na vytvorenie podpisu sa po dlhšej dobe stanú menej bezpečnými alebo neodolnými voči novým typom útokov. Aby sa zabránilo takýmto patovým situáciám a súčasne nekonečnému rozrastaniu archívov, bol navrhnutý formát zaručeného elektronického podpisu s úplnou informáciou pre overenie platnosti a formát archívneho zaručeného elektronického podpisu, ktorý má okrem všetkých informácií potrebných na overenie platnosti navyše aj časovú pečiatku na tieto údaje.

Archívny elektronický podpis slúži najmä na ochranu podpísaného dokumentu z dlhodobého hľadiska. Zabezpečuje dôveryhodné uzavretie obsahu všetkých potrebných informácií na overenie podpisu na dlhú dobu. Archivovanie elektronického podpisu so všetkými certifikátmi a údajmi potrebnými na overenie platnosti a jeho podpísanie pomocou algoritmu s dlhším kľúčom má ochrániť podpis na dostatočne dlhý časový interval.

Pri overovaní elektronického podpisu a zaručeného elektronického podpisu je potrebné overiť aj údaje z pripojeného certifikátu. V prvom rade je dôležité overiť platnosť pripojeného certifikátu. Kontrolujeme vlastne, či v čase, keď bol dokument podpísaný, bol certifikát na použitý verejný (a teda

aj súkromný) kľúč platný. Túto informáciu sa dozvieme od certifikačnej autority, ktorá certifikát vydala, konkrétne zo zoznamov zrušených certifikátov tejto certifikačnej autority, ktoré sú dostupné v archíve na internete. Často musíme prejsť viacero archívov certifikačných autorít v PKI.

Pri overovaní archívneho zaručeného elektronického podpisu nám odpadá potreba prezerať archívy na internete. Všetky potrebné informácie máme k dispozícii priamo s podpisom.

## 5.1 Definícia

Archívny zaručený elektronický podpis je jedným z formátov zaručených elektronických podpisov. Podľa § 3 ods. 5 Vyhlášky Národného bezpečnostného úradu č. 537/2002 Zb. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky [16] je formát archívneho zaručeného elektronického podpisu definovaný nasledovne :

"Archívny zaručený elektronický podpis má formu zaručeného elektronického podpisu s časovou pečiatkou, ku ktorému sú pripojené všetky údaje potrebné na overenie daného archívneho zaručeného elektronického podpisu podľa § 11 ods. 1. Na údaje potrebné na overenie daného archívneho zaručeného elektronického podpisu je vyhotovená časová pečiatka, ktorá je k nim pripojená" [16].

Archívny zaručený elektronický podpis teda obsahuje :

a) identifikátor použitej podpisovej politiky

b) podpisové údaje, ktoré podpisujúci do podpisu zahrnul (napríklad miesto a čas vyhotovenia podpisu, meno fyzickej osoby podpisujúcej za právnickú osobu a pod.)

c) digitálny podpis vytvorený na základe digitálneho odtlačku podpisovaného dokumentu, identifikátora podpisovej politiky a údajov zahrnutých do podpisu

d) časovú pečiatku na zaručený elektronický podpis

e) údaje potrebné na overenie daného archívneho zaručeného elektronického podpisu

f) časovú pečiatku na údaje potrebné na overenie podpisu.

Pod údajmi potrebnými na overenie daného archívneho zaručeného elektronického podpisu podľa § 11 ods. 1 sa rozumejú :

a) elektronický dokument, pre ktorý bol podpis vytvorený
b) zaručený elektronický podpis dokumentu
c) platný verejný kľúč prislúchajúci k súkromnému kľúču použitému na vytvorenie zaručeného elektronického podpisu
d) podpisovú politiku, ktorej identifikátor je uvedený v zaručenom elektronickom podpise.

Na overenie archívneho zaručeného elektronického podpisu potrebujeme ešte všetky certifikáty potrebné na overenie všetkých digitálnych podpisov a časových pečiatok a informácie o platnosti certifikátov, teda všetky relevantné CRL. Z právneho hľadiska je týmto formát archívneho zaručeného elektronického podpisu ošetrený, avšak jeho technické parametre je potrebné podrobne špecifikovať.

### 5.1.1 Atribúty podpisu

Predtým, ako formálne špecifikujeme samotný formát archívneho zaručeného elektronického podpisu, popíšeme aké všetky atribúty elektronického podpisu existujú, aká je ich funkcia a akú informáciu obsahujú.

Atribút : `id-contentType`
Popis : identifikátor typu údajov

Atribút : `id-messageDigest`
Popis : digitálny odtlačok správy

Atribút : `id-signingTime`
Popis : podpisovateľom deklarovaný čas podpísania, jeho hodnota je medzi 1.1.1950 a 31.12.2049 vo formáte UTCTime (YYMMDDHHMMSSZ) alebo GeneralizedTime (YYYYMMDDHHMMSSZ)

Atribút : `id-aa-ets-otherSigCert`
Popis : postupnosť identifikátorov certifikátov od certifikátu podpisovateľa až po certifikát koreňovej certifikačnej autority (NBÚ), musí obsahovať minimálne identifikátor certifikátu podpisovateľa

Atribút : `id-aa-signingCertificate`
Popis : rovnako ako id-aa-ets-otherSigCert, ale môže sa používať len do 1.1.2009

Atribút : `id-aa-ets-sigPolicyId`
Popis : identifikátor podpisovej politiky použtej pri podpisovaní a rovnako pri overovaní elektronického podpisu

Atribút : `id-aa-signatureTimeStampToken`
Popis : časová pečiatka vyhotovená na digitálny podpis dokumentu

Atribút : `id-aa-ets-certificateRefs`
Popis : kompletný zoznam identifikátorov certifikátov celej certifikačnej cesty bez certifikátu podpisovateľa

Atribút : `id-aa-ets-revocationRefs`
Popis : úplný zoznam identifikátorov CRL alebo OCSP slúžiacich na overenie platnosti certifikátu podpisovateľa a celej certifikačnej cesty až po certifikát dôveryhodnej CA

Atribút : `id-aa-ets-escTimeStamp`
Popis : časová pečiatka, ktorej účelom je ochrániť platnosť elektronického podpisu v prípade, že dôjde k skompromitovaniu kľúča CA a zrušeniu certifikátu CA, je vyhotovená na digitálny odtlačok zo spojených hodnôt digitálneho podpisu a atribútov id-aa-ets-certificateRefs, id-aa-ets-revocationRefs a id-aa-signatureTimeStampToken

Atribút : `id-aa-ets-CertCRLTimestamp`
Popis : časová pečiatka, ktorej účelom je ochrániť platnosť elektronického podpisu v prípade, že dôjde k skompromitovaniu kľúča CA a zrušeniu certifikátu CA, je vyhotovená na digitálny odtlačok zo spojených hodnôt atribútov id-aa-ets-certificateRefs a id-aa-ets-revocationRefs, slúži na zefektívnenie vydávania časových pečiatok

Atribút : `id-aa-ets-certValues`
Popis : kompletné certifikáty celej certifikačnej cesty bez certifikátu podpisovateľa, môže obsahovať aj iné certifikáty, napr. krížové alebo certifikáty

potrebné na overenie časovej pečiatky

Atribút : `id-aa-ets-revocationValues`
Popis : úpné CRL alebo OCSP minimálne celej certifikačnej cesty, môže obsahovať aj iné CRL a OCSP, napr. slúžiace na overenie krížových certifikátov alebo časovej pečiatky

Atribút : `id-aa-ets-archiveTimestamp`
Popis : archívna časová pečiatka, ktorej účelom je dlhodobé archivovanie elektronického podpisu s kompletnými certifikátmi a údajmi na overenie platnosti, aby bolo možné elektronický podpis overiť aj keď dôjde k skompromitovaniu kľúča CA, zrušeniu platnosti certifikátu CA, nedostupnosti CA alebo zníženiu bezpečnosti podpisového algoritmu, ochrana na dlhšiu dobu je zabezpečená opečiatkovaním s algoritmom s väčším kľúčom

Atribút : `id-aa-ets-contentTimestamp`
Popis : časová pečiatka, ktorej účelom je potvrdiť, že forma podpisovaných údajov existovala už v čase vydania časovej pečiatky a teda pred samotným podpisom

Atribút : `id-aa-ets-signerLocation`
Popis : pomocná informácia o adrese miesta, kde podpisovateľ vykonal elektronické podpisovanie

Tieto atribúty môžu byť pre konkrétny formát zaručeného elektronického podpisu povinné alebo voliteľné, záleží to od úrovne bezpečnosti, ktorú od daného formátu vyžadujeme.

### 5.1.2 Formálna špecifikácia

Formát archívneho zaručeného elektronického podpisu je špecifikovaný v dokumente Formáty zaručených elektronických podpisov [23], ktorý vydal NBÚ. Archívny zaručený elektronický podpis obsahuje samotný digitálny podpis a navyše povinne obsahuje atribúty :

`id-contentType`,
`id-messageDigest`,

id-signingTime,
id-aa-ets-otherSigCert alebo id-aa-signingCertificate,
id-aa-ets-sigPolicyId,
id-aa-signatureTimeStampToken,
id-aa-ets-certificateRefs,
id-aa-ets-revocationRefs,
id-aa-ets-escTimeStamp alebo id-aa-ets-CertCRLTimestamp,
id-aa-ets-certValues,
id-aa-ets-revocationValues,
id-aa-ets-archiveTimestamp.

Môže obsahovať aj voliteľné atribúty :

id-aa-ets-contentTimestamp,
id-aa-ets-signerLocation.

Uvedená, v súčasnosti platná, špecifikácia vychádza z technickej špecifikácie ETSI pre formáty elektronických podpisov [36].

## 5.2 Vytváranie a overovanie archívneho elektronického podpisu

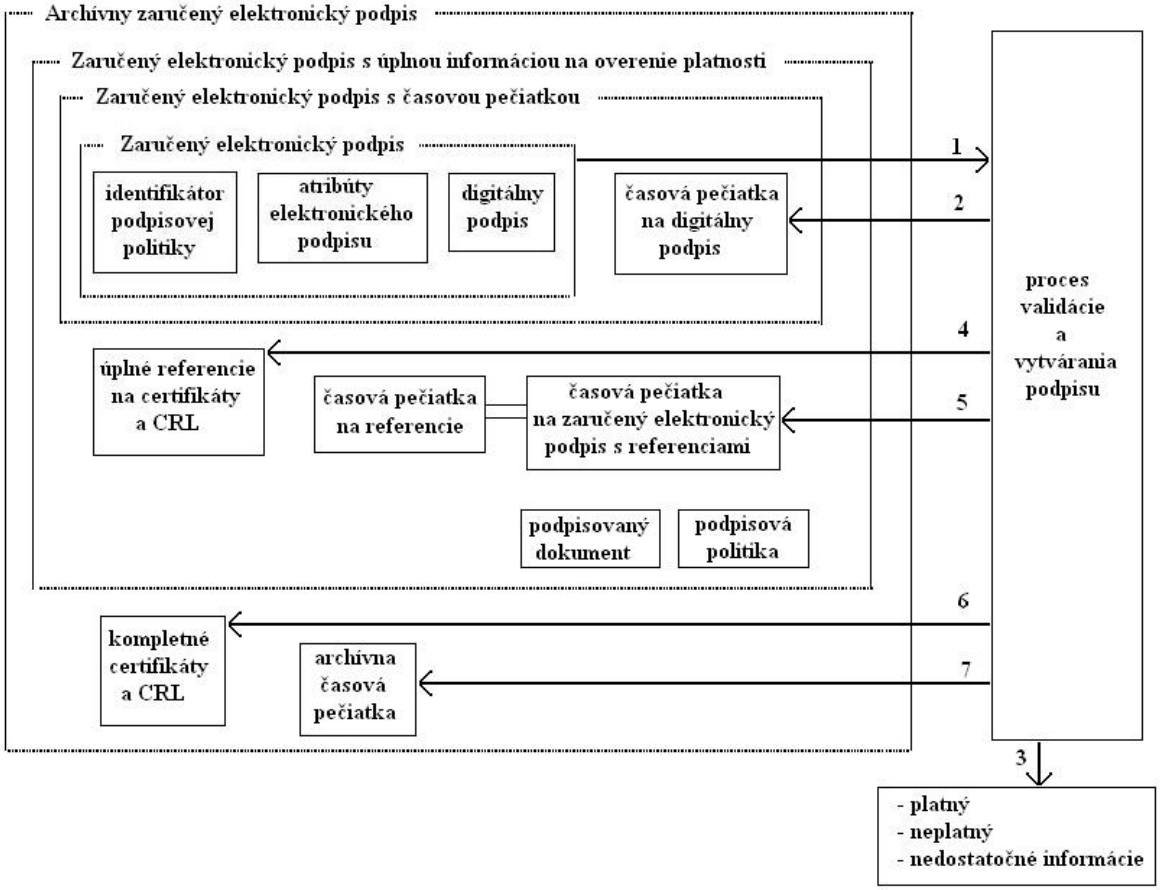
Koncept archívneho zaručeného elektronického podpisu bol navrhnutý, všetky potrebné normy a špecifikácie boli prebraté z európskych noriem, prepracované Národným bezpečnostným úradom, schválené v Zákone č. 215/2002 Zb. o elektronickom podpise a o zmene a doplnení niektorých zákonov [15] a upresnené vo Vyhláške Národného bezpečnostného úradu č. 537/2002 Zb. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky [16]. V praxi však zatiaľ tento koncept nebol odskúšaný a použitý. Predtým, ako k takémuto kroku dôjde, je potrebné analyzovať koncept archívneho zaručeného elektronického podpisu, či je vôbec reálne, čo s ním chceme dosiahnuť. V nasledujúcej časti uvádzam popis, akým spôsobom sa takýto podpis vytvára a overuje. Vychádzam pritom z najnovšej technickej špecifikácie ETSI pre formáty elektronických podpisov [37]. Neskôr sa pozriem aj na možnosti reálneho použitia tohto formátu elektronického podpisu.

### 5.2.1 Proces vytvárania

Keď ideme vytvoriť archívny zaručený elektronický podpis, predovšetkým musíme zozbierať všetky potrebné dáta. V prvom rade sem patrí dokument, ktorý chceme podpísať. Ďalšou dôležitou časťou je kvalifikovaný certifikát verejného kľúča, ktorý musí byť platný a obsahovať všetky predpísané informácie. Musíme si zvoliť podpisovú politiku, podľa ktorej budeme podpis vytvárať. Tým pádom si zvolíme aj hašovaciu funkciu a podpisovací algoritmus. Pripravíme si všetky ostatné údaje, ktoré chceme do podpisu zahrnúť. Môže ísť o údaj o mieste alebo čase vyhotovenia podpisu, môžeme sem uviesť identifikačné údaje osoby podpisujúcej v mene firmy, prípadne iné dôležité informácie.

Keď máme pripravené všetky potrebné údaje, pristúpime k samotnému podpisovaniu. Pomocou hašovacej funkcie vytvoríme digitálny odtlačok dokumentu. Tento následne podpíšeme pomocou podpisovacieho algoritmu so svojím súkromným kľúčom. Získali sme digitálny podpis dokumentu. V tomto momente naša práca končí. Vytvorený digitálny podpis, identifikátor použitej podpisovej politiky a samotný podpisovaný dokument dáme dôveryhodnej certifikačnej autorite na overenie a vytvorenie archívneho zaručeného elektronického podpisu. Súčasne musíme predložiť certifikačnej autorite aj platný kvalifikovaný certifikát, pomocou ktorého sme podpis vytvorili.

Certifikačná autorita po obdržaní týchto údajov pristúpi k procesu validácie a vytvorenia archívneho zaručeného elektronického podpisu. Detailná schéma tohoto postupu je zobrazená na obrázku :




Obr.6 Schéma vytvárania archívneho zaručeného elektronického podpisu.[37]

V prvom kroku certifikačná autorita obdrží údaje od podpisovateľa.

V druhom kroku musí certifikačná autorita overiť hodnotu digitálneho podpisu a vydať časovú pečiatku na digitálny podpis. Súčasne musí overiť elektronický podpis podľa požiadaviek predloženej podpisovej politiky s použitím ďalších údajov - certifikátov, CRL, OCSP a iných.

Ak nie sú k dispozícii všetky potrebné údaje pre overenie elektronického podpisu, v treťom kroku je táto skutočnosť oznámená užívateľovi a proces končí. Ak sú údaje k dispozícii, v procese validácie sa tieto údaje o certifikátoch, CRL a OCSP stiahnu, urobia sa všetky potrebné kontroly platnosti elektronického podpisu a výsledok kontroly sa oznámi užívateľovi. Ak je kon-

trola negatívna, teda elektronický podpis je neplatný, proces vytvárania archívneho zaručeného elektronického podpisu končí.

Ak validácia prebehla bez problémov, v štvrtom kroku sa k podpisu pripoja všetky referencie na certifikáty, CRL a OCSP, ktoré sú potrebné na overenie platnosti elektronického podpisu.

V piatom kroku sa na tieto referencie vyhotoví časová pečiatka. Druhou možnosťou je, že sa časová pečiatka vyhotoví nielen na referencie o certifikátoch, CRL a OCSP, ale na kompletný zaručený elektronický podpis aj s referenciami. Obe možnosti sú ekvivalentné.

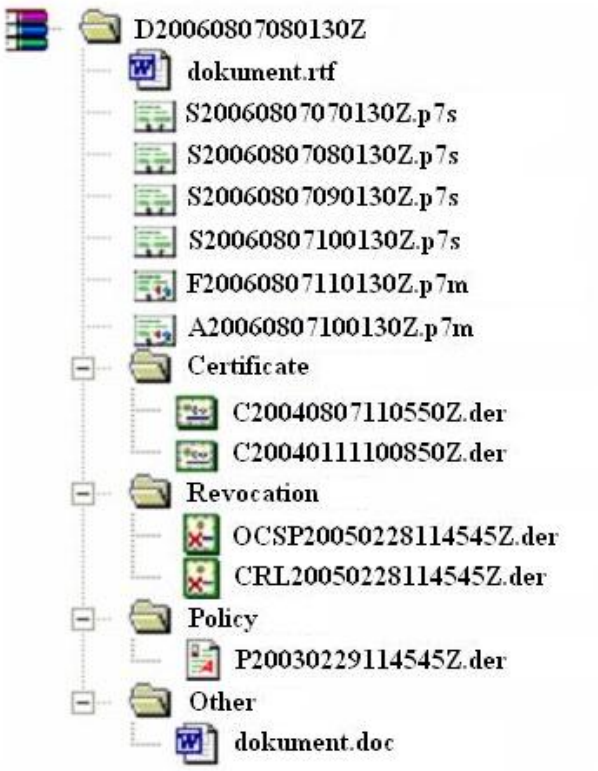
Keďže vytvárame archívny elektronický podpis, ktorý vyžaduje pripojiť všetky potrebné informácie na overenie, v šiestom kroku sú pridané kompletné certifikáty a relevantné CRL alebo OCSP. Zároveň je pripojený samotný podpisovaný dokument a celá podpisová politika.

V poslednom siedmom kroku certifikačná autorita vydá archívnu časovú pečiatku na celý zaručený elektronický podpis aj so všetkými certifikátmi, CRL a OCSP, podpisovaným dokumentom, podpisovou politikou, ako aj všetkými údajmi potrebnými na overenie podpisu. Na vytvorenie archívnej časovej pečiatky je použitý algoritmus s dlhším kľúčom ako je bežne používané.

Na tomto mieste treba podotknúť, že v praxi sa údaje neposielajú certifikačnej autorite a naspäť. Takéto vytváranie archívnych elektronických podpisov by bolo značne neefektívne. Preto certifikačná autorita poskytuje užívateľom softvér, ktorý vykoná celý proces vytvárania podpisu. Podmienkou je samozrejme, prístup na internet za účelom získania potrebných informácií - certifikátov, CRL, OCSP a rovnako za účelom využitia služieb certifikačnej autority, najmä služby časovej pečiatky.

Takýmto spôsobom je vytvorený archívny zaručený elektronický podpis. Samozrejme, ani archívna časová pečiatka nemôže zaručiť bezpečnosť navždy, preto je potrebné vždy v prípade oslabenia bezpečnosti aktuálnej archívnej časovej pečiatky vydať na archívny elektronický podpis novú archívnu časovú pečiatku, zaručujúcu bezpečnosť podpisu opäť na dostatočne dlhú dobu. Samozrejme nesmieme zabudnúť priložiť relevantné certifikáty, CRL a OCSP.

Podpisovaný dokument, jeho podpis, informácie potrebné na overenie podpisu, časové pečiatky a ostatné dokumenty súvisiace s procesom vytvárania podpisu je potrebné spojiť do formátu, ktorého spracovanie je jednoduché a bežne dostupné. Medzi takéto formáty patria S/MIME alebo ZIP. Príklad štruktúry ZIP súboru je na obrázku :




Obr.7 ZIP formát elektronického podpisu.[23]

Názvy jednotlivých položiek obsahujú ako prvé písmeno typ položky, nasleduje čas vo formáte GeneralizedTime, nakoniec môže ísť poradové číslo pre súbory s rovnakým časom a typom. Rozdelenie do adresárov nie je povinné, ale dopomáha k prehľadnosti celej štruktúry súborov.

### 5.2.2 Proces overovania

Overovanie archívneho zaručeného elektronického podpisu je náročný proces, hlavne z dôvodu, že musia byť zachované všetky bezpečnostné opatrenia, overovanie musí prebiehať v bezpečnom prostredí. Spôsob, akým bude overovanie prebiehať vyplýva z toho, akým spôsobom sa takýto elektronický podpis vytváral.

Po obdržaní archívneho zaručeného elektronického podpisu musíme v prvom rade overiť platnosť archívnej časovej pečiatky (niekedy sa zvykne nazývať aj archivačný podpis). Overenie prebehne na základe priloženého certifikátu verejného kľúča príslušnej certifikačnej autority. V prípade, že podpis obsahuje takýchto archívnych časových pečiatok viac, je potrebné overiť všetky v poradí od najnovšej po najstaršiu.

V druhom kroku treba overiť všetky priložené certifikáty celej certifikačnej cesty. Certifikáty overujeme postupne od certifikátu dôveryhodnej (koreňovej alebo inej dostatočne dôveryhodnej) certifikačnej autority až po certifikát podpisovateľa.

Následne overíme časovú pečiatku na referencie o certifikátoch a CRL, prípadne časovú pečiatku na referencie a celý zaručený elektronický podpis, podľa toho, ktorá z týchto pečiatok bola použitá.

V štvrtom kroku overíme časovú pečiatku na digitálny podpis dokumentu. Opäť použijeme verejný kľúč z príslušného priloženého certifikátu.

V poslednom kroku overíme samotný digitálny podpis dokumentu. Súčasne overíme, či elektronický podpis spĺňa požiadavky priloženej podpisovej politiky.

Pri overovaní časových pečiatok ako aj elektronických podpisov používame priložené certifikáty, ktoré rovnako overíme. Samozrejme podľa potreby využívame aj priložený podpisovaný dokument a priloženú podpisovú politiku. Podľa nej identifikujeme použitý podpisovací algoritmus ako aj použitú hašovaciu funkciu na vytvorenie digitálneho odtlačku.

Celý proces overovania môžeme vykonať sami, avšak treba zaručiť bez-

pečné prostredie, alebo môžeme o overenie podpisu alebo niektorej jeho časti požiadať dôveryhodnú certifikačnú autoritu, ktorá poskytuje službu overenia elektronických podpisov. Zlyhanie overovania v ktoromkoľvek kroku znamená, že archívny zaručený elektronický podpis, alebo jeho časť, bol pozmenený, a teda podpis nie je možné považovať za platný.

## 5.3 Množstvo informácie potrebné na vytvorenie a overenie archívneho elektronického podpisu

Na základe predchádzajúceho popisu vytvárania a overovania archívnych zaručených elektronických podpisov v nasledujúcej časti špecifikujeme všetky údaje potrebné na vytvorenie a overenie elektronického podpisu. Zistíme, či množstvo údajov a potrebných dokumentov je konečné, alebo sa môže neohraničene rozrastať. Súčasne odhadneme objem dát, ktoré sú potrebné, a tým aj efektívnosť a možnosť použitia formátu archívneho zaručeného elektronického podpisu.

Na Slovensku je v súčasnosti registrovaných 10 certifikačných autorít, pričom akreditovaných je polovica z tohoto počtu. Infraštruktúra verejného kľúča má dve úrovne. Na vrchole stojí koreňová certifikačná autorita - CA NBÚ, pod ktorou sú priamo všetky ostatné certifikačné autority. To znamená, že každý certifikát každej certifikačnej autority bol vydaný CA NBÚ. Z toho súčasne vyplýva, že pri overovaní zaručeného elektronického podpisu sú okrem kvalifikovaného certifikátu užívateľa potrebné maximálne ďalšie dva certifikáty - certifikát certifikačnej autority, ktorá vydala užívateľovi certifikát a certifikát CA NBÚ ako koreňovej certifikačnej autority. Celá situácia je odzrkadlením skutočného stavu na Slovensku, kde ešte zaručené elektronické podpisy sú len veľmi málo používané aj v takých inštitúciách ako banky, či daňové úrady, nieto u súkromných osôb. Avšak aj v prípade, že sa používanie elektronických podpisov rozšíri a počet certifikačných autorít narastie (ako je tomu v niektorých iných krajinách), predpokladám, že veľkosť archívneho zaručeného elektronického podpisu to významne neovplyvní.

Množstvo informácie potrebné na vytvorenie a overenie archívneho elektronického podpisu odhadnem na základe nasledujúceho fiktívneho príkladu.

Uvažujem modelovú PKI porovnateľnú so súčasnou PKI v podmienkach Slovenskej Republiky a definujem presne veľkosť jednotlivých častí archívneho elektronického podpisu ako aj jeho celkovú veľkosť.

Pán Peter Vzorový je držiteľom certifikátu, ktorý mu vydala spoločnosť D. Trust Certifikačná Autorita, a.s. (ďalej len D. Trust CA), ktorá poskytuje akreditované certifikačné služby. Pán Vzorový si chce nechať vyhotoviť archívny zaručný elektronický podpis na svoju žiadosť o životné poistenie, v ktorej okrem iného uvádza prehlásenie o svojom súčasnom zdravotnom stave. Dokument so žiadosťou *Ziadost_Vzorovy_Peter.doc* má veľkosť 287 kB. Základnou časťou vytváraného archívneho zaručeného elektronického podpisu je samotný zaručený elektronický podpis. Ten sa skladá z identifikátora podpisovej politiky, identifikátorov certifikátov použitých na jeho vytvorenie, digitálneho odtlačku správy a digitálneho podpisu na odtlačok. Všetky tieto údaje sú vložené do jedného súboru *Ziadost_Vzorovy_Peter.p7s* s veľkosťou 4.16 kB. Zaručený elektronický podpis bol vytvorený za použitia hašovacej funkcie SHA-1 a podpisovacieho algoritmu RSA, tak ako to je štandardne zaužívané.

Na overenie tohoto zaručeného elektronického podpisu potrebujeme všetky certifikáty celej certifikačnej cesty. V našom príklade zatiaľ potrebujeme certifikát pána Vzorového *Vzorovy_Peter_01000000000102A334B110.cer* o veľkosti 1 kB, certifikát D. Trust CA *DTrustCA_020000000003452AE71133.cer* s veľkosťou 1.1 kB, ktorý použijeme na overenie podpisu na certifikáte pána Vzorového a certifikát CA NBÚ *NBU_04000000000532A7D19004.cer* s veľkosťou 1.3 kB, pomocou ktorého overíme podpis na certifikáte D. Trust CA.

K zaručenému elektronickému podpisu je pripojená časová pečiatka na digitálny podpis dokumentu. Je obsiahnutá priamo v súbore so zaručeným elektronickým podpisom. Túto časovú pečiatku vydala certifikačná autorita D. Trust CA, ktorej sme zverili aj vydanie archívneho zaručeného elektronického podpisu. Na overenie tejto časovej pečiatky potrebujeme samozrejme certifikát. Keďže na vyhotovovanie časových pečiatok používa D. Trust CA iný pár kľúčov ako na podpisovanie certifikátov, sú potrebné ďalšie dodatočné informácie. V tomto prípade len jeden ďalší certifikát D. Trust CA *DTrustCA_TS_020000000003434114AA4E.cer* s veľkosťou 1.05 kB. Na podpísanie tohto certifikátu bol použitý rovnaký súkromný kľúč CA NBÚ ako na podpísanie prvého spomínaného certifikátu D. Trust CA, takže zatiaľ sa množstvo potrebných certifikátov zastavilo na čísle štyri. Vo všeobecnosti sa môže počet potrebných certifikátov vyšplhať až na niekoľko desiatok súborov.

Ako si určite každý pozorný čitateľ všimol, formáty zaručených elektronických podpisov sú definované tak, že každý formát je rozšírením predchádzajúceho, ak ich usporiadame podľa množstva obsiahnutej informácie. Pri analýze množstva potrebnej informácie priloženej k elektronickému podpisu som sa zatiaľ dostal k zaručenému elektronickému podpisu s časovou pečiatkou. K nemu ďalej pripojíme zoznam identifikátorov všetkých použitých certifikátov. Okrem toho pripojíme aj zoznam identifikátorov relevantných zoznamov CRL alebo OCSP. Rovnako pripojíme časovú pečiatku vydanú na tieto zoznamy. Keďže v príklade uvažujeme na vydanie všetkých časových pečiatok použitie rovnakého kľúča, certifikát potrebný na ich overenie už máme k dispozícii.

Na tomto mieste vymenujem všetky potrebné zoznamy CRL. Na overenie platnosti certifikátu pána Vzorového potrebujeme CRL vydaný D. Trust CA *DTrustCA_2008010100000X1.crl*, ktorého veľkosť je 0.5 kB. Platnosť obidvoch certifikátov tejto CA overíme na základe CRL certifikačnej autority CA NBÚ *NBU_20080101Z7.crl*, ktorý má veľkosť 4.3 kB. Tieto zoznamy CRL sú podpísané kľúčmi z certifikátov, ktoré už máme k dispozícii. To nemusí byť vždy pravda. V prípade, že na podpisovanie CRL používa niektorá certifikačná autorita iný kľúč ako na podpisovanie vydaných certifikátov, je potrebné priložiť relevantný certifikát a samozrejme aj všetky ďalšie certifikáty potrebné na overenie podpisu na tomto certifikáte. Rovnako ku každému ďalšiemu priloženému certifikátu potrebujeme priložiť CRL. Takto môže množstvo certifikátov a CRL narastať. V našom príklade však túto situáciu zatiaľ neuvažujeme. Podrobnejšie sa jej budeme venovať v inom príklade. Rovnako treba spomenúť, že k jednému certifikátu je potrebné priložiť všetky relevantné CRL. Sem patria CRL od dátumu vydania certifikátu (staršie CRL nie sú potrebné, certifkát nemohol byť zrušený pred jeho vydaním) až po aktuálny CRL. V závislosti od spôsobu vydávania CRL certifikačnou autoritou je to buď jeden súbor (ak sú CRL kumulatívne pridávané do jedného súboru pre určité obdobie), alebo viac súborov (ak je pre každý nový CRL vydaný zvlášť súbor). V uvádzanom príklade uvažujem kumulatívne CRL.

V archívnom zaručenom elektronickom podpise je k všetkým doteraz priloženým informáciám pridaná aj kompletná podpisová politika. Súbor s podpisovou politikou *policy_cp_1_03.pdf* má veľkosť 249 kB. Priložené sú aj všetky potrebné certifikáty verejného kľúča a musia byť priložené aj zoznamy zrušených certifikátov (CRL), prípadne informácie o aktuálnom stave platnosti certifikátu (OCSP). Celková veľkosť súborov s certifikátmi a zoznamamy CRL je 9.25 kB.

Ku všetkým spomenutým údajom spolu s podpisovaným dokumentom priložíme certifikát, ktorý je potrebný na overenie archívnej časovej pečiatky *DTrustCA_ATS_0200000000034341 14EE1C.cer* s veľkosťou 1.9 kB a uložíme do jedného súboru *Ziadost_Vzorovy_Peter.p7m*, ktorý obsahuje súčasne aj archívnu časovú pečiatku vydanú na zaručený elektronický podpis so všetkými spomenutými údajmi. Vytvorený zaručený archívny elektronický podpis je vo formáte S/MIME. Súbor má veľkosť 563.4 kB. V tomto bode netreba zabudnúť, že archívnych časových pečiatok môže jeden archívny zaručený elektronický podpis obsahovať aj niekoľko. V prípade potreby sa spolu s novou archívnou časovou pečiatkou doplní aj relevantný certifikát s verejným kľúčom (prípadne viac certifikátov, podľa dĺžky certifikačnej cesty). Napriek tomu, množstvo potrebnej informácie to nejako rapídne neovplyvní, keďže ku kompromitácii certifikačnej autority, či oslabeniu podpisového algoritmu nedochádza tak často. Dokonca aj certifikáty akreditovaných certifikačných autorít sú vydávané na dlhšie časové obdobia ako obyčajné kvalifikované certifikáty.

Na tomto mieste vzniká pochybnosť, či neustálym pridávaním archívnych časových pečiatok nemôže množstvo potrebných údajov narastať donekonečna. Odpoveď je nie. Vzhľadom na doterajšie skúsenosti s elektronickými podpismi, môžeme tvrdiť, že tieto archívne časové pečiatky nebudú pridávané častejšie ako raz za niekoľko rokov. Teda ich celkový počet je možné zhora ohraničiť rozumným číslom, podľa toho, na aké dlhé obdobie chceme zaručiť overiteľnosť archívneho elektronického podpisu.

V tomto príklade bol k dokumentu veľkosti 287 kB vytvorený archívny zaručený elektronický podpis s približne dvojnásobnou veľkosťou. Skúsim sa teraz pozrieť na príklad, v ktorom budem uvažovať rozsiahlejšiu infraštruktúru verejného kľúča, tak ako je tomu napríklad v Nemeckej republike.

Spoločnosť Kommunale Informationsverarbeitung in Hessen podpísala svoju výročnú správu zaručeným elektronickým podpisom s časovou pečiatkou. Správa *KIV_HE_5714.pdf* má veľkosť 2.17 MB a vytvorený zaručený elektronický podpis s časovou pečiatkou *KIV_HE_5714.p7s* veľkosť 4.17 kB.

Teraz uvediem zoznam všetkých certifikátov a CRL, ktoré je potrebné priložiť k elektronickému podpisu :

Na overenie zaručeného elektronického podpisu potrebujeme certifikáty
*KIV_HE_0100000000001128A94B3E0.cer* (0.87 kB)
(vydal GlobalSign ObjectSign CA)
*GlobalSignObjectSignCA_04000000000108D9612448.cer* (1.03 kB)
(vydal GlobalSign Primary Object Publishing CA)
*GlobalSignPrimaryObjectPublishingCA_040000000108D9611CD6.cer* (1.02 kB)
(vydal GlobalSign Root CA)
*GlobalSignRootCA_020000000000D678B79405.cer* (0.89 kB)
(self-signed certifikát)

a k nim relevantné CRL
*GlobalSignObjectSignCA_20080128093738Z.crl* (7.87 kB)
*GlobalSignPrimaryObjectPublishingCA_20080101100000Z.crl* (0.46 kB)
*GlobalSignRootCA_20080101100000Z.crl* (0.47 kB).

Na overenie časovej pečiatky vyhotovenej certifikačnou autoritou D-TRUST TSS CA potrebujeme ďalej certifikáty
*D-TRUST_akkr_TSS-10_20061PN_0103_Bundesnetzagentur.cer* (0.96 kB)
(vydal D-TRUST Qualified CA)
*D-TRUSTQualifiedCA20031PN_1FBF_D-TrustGmbH.cer* (1.01 kB)
(self-signed certifikát)

a k nim nasledovné CRL
*D-TRUSTQualifiedCA12R-CRL_1PN_02_02_00_D0.crl* (104 kB).

Na overenie archívnej časovej pečiatky vyhotovenej certifikačnou autoritou D-TRUST TSS CA potrebujeme ešte certifikát
*D-TRUST_Archive_TSS-10_20061PN_0189_Bundesnetzagentur.cer* (0.99 kB)
(vydal D-TRUST Qualified CA).

Na overenie podpisov na všetkých CRL potrebujeme certifikáty, ktoré už máme k dispozícii. Neskôr rozoberiem prípad, keby tomu tak nebolo. Spolu majú všetky tieto certifikáty a CRL veľkosť 119.57 kB.

Priložíme súbor s kompletnou podpisovou politikou *P_KIVGSDTT_84.pdf* s veľkosťou 414 kB. Súbor s vytvoreným zaručeným elektronickým podpisom *KIV_HE_5714.p7m* má veľkosť 2.98 MB. Množstvo prídavnej informácie predstavuje 810 kB.

Zamyslime sa teraz nad situáciou, že by každá zo spomenutých cetifikačných autorít z predchádzajúceho príkladu použila na podpisovanie CRL zoznamov iný pár kľúčov ako na podpisovanie vydaných certifikátov (napríklad certifikátu skončila platnosť a v súčasnosti sa už používa iný certifikát). V tom prípade máme štyri CRL, ku ktorým potrebujeme priložiť ďalšie informácie. Pre jednoduchosť budem v tomto príklade uvažovať veľkosť každého nového certifikátu 1 kB a veľkosť každého CRL 20 kB. Ku každému zo štyroch CRL potrebujeme priložiť jeden alebo viac certifikátov, podľa certifikačnej cesty. Ak by certifikáty určené na podpisovanie vydaných CRL boli vydané rovnakými certifikačnými autoritami ako certifikáty určené na podpisovanie vydaných certifikátov, tak ku každému novopridanému certifikátu máme ostatné certifikáty certifikačnej cesty ako aj relevantné CRL k dispozícii. V takomto prípade teda potrebujeme spolu len štyri nové certifikáty. Pre lepšiu predstavu, ku *GlobalSignObjectSignCA_20080128093738Z.crl* priložíme certifikát *GlobalSignObjectSignCA_04000000000108D9617843.cer* vydaný GlobalSign Primary Object Publishing CA, pričom ostatné certifikáty certifikačnej cesty ako aj k nemu relevantný CRL od GlobalSign Primary Object Publishing CA už máme k dispozícii.

Treba poznamenať, že v praxi väčšinou certifikačné autority používajú len jeden pár kľúčov na podpisovanie a disponujú len jedným certifikátom. Napriek tomu, aj v tomto príklade bolo k dokumentu veľkosti 2.17 MB potrebné pripojiť len 814 kB.

V poslednom príklade pôjdem ešte viac do hĺbky. Predpokladajme, že na podpísanie každého priloženého certifikátu ako aj každého priloženého CRL bol použitý iný par kľúčov. Označme certifikát užívateľa *C_User_1.cer*, certifikáty certifikačnej cesty *C_GSOS_1.cer*, *C_GSPOP_1.cer* a *C_GSR_1.cer* (self-signed). Platnosť certifikátu *C_User_1.cer* overíme pomocou *R_GSOS_1.crl*, ktorý bol podpísaný kľúčom z certifikátu *C_GSOS_2.cer* (jeho certifikačná cesta obsahuje ďalej certifikáty *C_GSPOP_2.cer* a *C_GSR_2.cer*). Vidíme, že na overenie *n* (v našom prípade 4) certifikátov potrebujeme *n-1* CRL a teda aj *n-1* nových certifikátov. Aplikáciou rekurzie sa ľahko dostaneme k výsledku, koľko certifikátov a CRL potrebujeme. Spolu je to 31 certifikátov a 15 CRL. Rovnakú rekurziu použijeme aj pri certifikátoch na overenie časových pečiatok. Spolu budeme potrebovať 37 certifikátov a 17 CRL. Celková veľkosť týchto dokumentov je 377 kB, pričom množstvo potrebnej informácie pridanej k dokumentu narastie na 1.07 MB.

Vo všetkých príkladoch som uvažoval použitie kumulatívnych CRL. Ak by niektorá certifikačná autorita pre každý nový CRL vydávala zvlášť súbor, počet súborov by mierne narástol, avšak tieto súbory by boli veľkosťou menšie a teda vplyv na celkové množstvo potrebnej informácie by bol zanedbateľný.

Výsledky sú zhrnuté v nasledujúcej tabuľke :

| | Príklad 1 | Príklad 2 | Príklad 3 | Príklad 4 |
|---|---|---|---|---|
| Zaručený elektronický podpis s čas. pečiatkou | 4,16 kB | 4,17 kB | 4,17 kB | 4,17 kB |
| Priložené certifikáty | 5 ks<br>6,35 kB | 7 ks<br>6,77 kB | 11 ks<br>10,77 kB | 37 ks<br>37 kB |
| Priložené CRL | 2 ks<br>4,8 kB | 4 ks<br>112,8 kB | 4 ks<br>112,8 kB | 17 ks<br>340 kB |
| Podpisová politika | 249 kB | 414 kB | 414 kB | 414 kB |
| Podpisovaný dokument | 287 kB | 2,17 MB | 2,17 MB | 2,17 MB |
| Zaručený archívny elektronický podpis | 563,4 kB | 2,98 MB | 2,984 MB | 3,24 MB |
| Prídavná informácia | 276,4 kB | 810 kB | 814 kB | 1,07 MB |

Tab.1 Prehľad výsledkov analýzy

Analýza ukázala, že množstvo informácie potrebnej na overenie archívneho zaručeného elektronického podpisu je porovnateľné veľkosti podpisovaného dokumentu. V priemernom prípade je pomer veľkosti dokumentu ku prídavnej informácii (aj pri zohľadnení rozsiahlej PKI) asi 1 : 1, čo je, myslím si, celkom prijateľné riešenie.

V tomto momente je vhodné zamyslieť sa nad možnosťou zdielania niektorých informácií pre viac archívnych elektronických podpisov. Inými slovami, ak vytvárame dva archívne zaručené elektronické podpisy v rovnakom čase, pripojené informácie potrebné na overenie týchto podpisov sú z veľkej časti rovnaké (certifikáty, CRL, OCSP, podpisová politika). Možno by stálo za zváženie, či nie je efektívnejšie tieto údaje zdielať pre podpisy vytvorené v rovnakom čase. Podobne, ak sú podpisy vytvorené len niekoľko dní alebo

týždňov po sebe, určite dostatočne veľká časť (aj polovicu údajov môžeme považovať za dostatočné veľkú časť) pridanej informácie bude rovnaká. Tieto informácie by bolo vhodné uchovávať v archíve, ktorý by bol na to určený.

Keď sa však zamyslím nad počtom archívnych zaručených elektronických podpisov, ktoré by mohli zdielať spoločné údaje, dochádzam k záveru, že hoci spomenutá myšlienka nie je zlá, realizácia podobného archívu by nebola efektívna. Dôvodom je, že jeho prevádzkové náklady by boli značne vyššie ako jeho význam a skutočný prínos. Aspoň v priebehu najbližších rokov je táto myšlienka nerealizovateľná. Ako príklad uvediem, nech je vytvorených dvesto archívnych podpisov, každý z nich nech obsahuje 800 kB pridanej informácie. Spolu pre všetky podpisy je to 160 MB dát. Pri zdielaní dát a použití archívu, by možno celý archív obsahoval len niekoľko MB údajov. Pre takto malé množstvo dát sa neoplatí vynakladať úsilie a prostriedky na vytváranie archívu, ak navyše vezmem do úvahy, že by sme takto ušetrili celkovo len niekoľko desiatok MB informácií, ktoré sú uložené pri archívnych podpisoch. V budúcnosti, ak sa používanie archívnych podpisov osvedčí a rozšíri, je ale určite zmysluplné zamyslieť sa aj nad takouto formou uchovávania informácií potrebných na overenie archívnych elektronických podpisov.

## 5.4 Analýza bezpečnostných požiadaviek

Pri celej doterajšej analýze som uvažoval, že všetku potrebnú informáciu máme k dispozícii zo spoľahlivých zdrojov. Takýto ideálny prípad ale nebude vždy reálny. V nasledujúcej časti budem analyzovať bezpečnostné požiadavky, čo všetko je potrebné zaistiť, aby sa dala garantovať požadovaná úroveň bezpečnosti. Akým spôsobom je možné zaručiť, že stiahnuté údaje sú skutočne pravé. Identifikujem najzákladnejšie problémy, nájdem miesta, kde by mohlo dôjsť k falšovaniu údajov, a navrhnem spôsoby riešenia týchto problémov.

V prvom rade sa pozriem na proces overovania archívneho zaručeného elektronického podpisu. Ak ideme overiť archívny podpis bez využitia služieb tretej strany (dôveryhodnej CA), musíme najprv zaručiť dostatočne bezpečné prostredie. Tým sa rozumie, že počas procesu overovania nesmie mať nikto okrem overovateľa prístup k akýmkoľvek údajom z archívneho elektronického podpisu. Inak by bolo veľmi jednoduché zmanipulovať overovanie a presvedčiť

overovateľa o korektnosti aj neplatného podpisu. Ak ale budeme na overovanie používať len bezpečné zariadenia v bezpečnom prostredí, prakticky nie je možný akýkoľvek útok ani manipulácia overovaných údajov. Skutočnosť, že žiaden zo súborov, ktoré podpis obsahuje, nebol zmenený, zaručuje archívna časová pečiatka.

Ak proces overenia archívneho elektronického podpisu prenecháme na niektorú z certifikačných autorít oprávnených ponúkať službu overovania, musí táto vedieť zaručiť bezpečné overenie podpisu. Problém nastáva skôr v doručení archívneho podpisu certifikačnej autorite a doručení jej odpovede späť.

Jednou možnosťou útoku je, že útočník odchytí archívny podpis (neplatný, sfalšovaný) pred jeho doručením CA a nechá v mene užívateľa overiť iný archívny podpis (ľubovoľný platný). Užívateľ dostane kladnú odpoveď, archívny podpis bude považovať za platný, hoci tomu tak nebude.

Inou možnosťou útoku je, že útočník jednoducho zabezpečí, aby sa záporná odpoveď od CA nedostala k užívateľovi a pošle mu v mene CA odpoveď kladnú. Rovnako v tomto prípade užívateľ dôveruje sfalšovanému archívnemu podpisu.

V obidvoch spomínaných prípadoch je cieľom útočníka presvedčiť overovateľa, že sfalšovaný archívny elektronický podpis je platný. Niekedy môže byť situácia aj opačná. Úlohou útočníka by bolo presvedčiť overovateľa o neplatnosti korektného podpisu. Priebeh útoku je rovnaký.

Zabrániť tomuto druhu útoku sa dá tak, že akúkoľvek správu, ktorú si bude užívateľ s CA vymieňať, je nutné podpísať zaručeným elektronickým podpisom s platným aktuálnym certifikátom. Tým vylúčime možnosť modifikovať posielané správy. Samozrejme, ak by odpoveď CA bola len z konečnej množiny (platný, neplatný), ľahko by mohol útočník zameniť aj kompletnú podpísanú správu s odpoveďou. Vhodný spôsob ako dostatočne rozšíriť množinu odpovedí je napríklad posielať spolu s odpoveďou naspäť aj overovaný archívny podpis.

V procese vytvárania archívneho elektronického podpisu sa útočník môže snažiť, aby vytvorený podpis nebolo možné overiť. Druhou možnosťou, ktorá je zo strany útočníkov vo všeobecnosti viac žiadaná, je nechať vytvoriť korektný podpis na iný ako pôvodne podpisovaný dokument.

Vytvorenie zaručeného elektronického podpisu dokumentu prebieha v bezpečnom prostredí bez možnosti prístupu cudzej osoby bezproblémovo.

Po poslaní zaručeného elektronického podpisu certifikačnej autorite na validáciu a pred vyhotovením archívneho elektronického podpisu certfikačná autorita zaručený elektronický podpis overí. Ak by bol počas prenosu tento podpis alebo podpisovaný dokument pozmenený, overenie zlyhá. V prípade, že by bol podpis s dokumentom úplne vymenený za iný korektný podpis s iným dokumentom (ale samozrejme overiteľný s iným verejným kľúčom, nie s verejným kľúčom užívateľa), certifikačná autorita túto výmenu nemusí spozorovať. Avšak archívny elektronický podpis by bol takto vyhotovený pre iný dokument a certifikát iného užívateľa (toho, ktorý podpísal vymenený dokument), čo útočníkovi nepomôže. Útočník zväčša potrebuje, aby bol zmenený len dokument, nie aj certifikát užívateľa. V tomto kroku teda možnosť útoku nepozorujeme.

Certifikačná autorita vytvára archívny elektronický podpis v bezpečnom prostredí, takže aj v tomto kroku je riziko neautorizovaných zmien minimálne až nulové. Toto ale nemusí platiť, ak si vyberieme na vyhotovenie archívneho zaručeného elektronického podpisu nedostatočne dôveryhodnú certifikačnú autoritu, prípadne zveríme vytvorenie podpisu neznámej alebo nedôveryhodnej CA. V takomto prípade sa ľahko môže stať, že za certifikačnú autoritu sa bude vydávať útočník, ktorého cieľom je vyhotoviť archívny elektronický podpis na iný dokument ako pôvodný, alebo s možnosťou neskoršej zmeny niektorých údajov priložených v archívnom elektronickom podpise. Jediným možným spôsobom, ako sa brániť pred takýmto konaním útočníka, je dôkladne si preveriť, komu zverujeme vytvorenie archívneho podpisu. Najlepšie je, ak už s danou CA máme vlastné skúsenosti (napr. vydaný kvalifikovaný certifikát). Rovnako dôležité je, aby sme si archívny zaručený elektronický podpis vytvorený certifikačnou autoritou najprv overili, predtým ako ho posunieme druhej strane (obchodnému partnerovi, ...). Overenie archívneho podpisu po jeho obdržaní je dôležité aj preto, aby sme mali istotu, že tento podpis nebol porušený alebo zmenený ani cestou od CA späť.

Vrátim sa ešte k samotnému vyhotoveniu archívneho podpisu certifikačnou autoritou. Nielenže podpisy a časové pečiatky musia byť vyhotovené v bezpečnom prostredí, ale aj priložené údaje, teda certifikáty, CRL a OCSP, musia byť z dôveryhodných zdrojov. Najlepšie by bolo, keby každá certifikačná autorita spravovala databázu vydaných certifikátov, odkiaľ by bolo možné certifikáty získať. Certifikačná autorita by ich na požiadanie posielala v podpísanej správe. Dôležité je hlavne preveriť certifikát podpisovateľa. Podstrčením falošného certifikátu (s identifikačnými údajmi užívateľa a verejným kľúčom útočníka) by bolo možné validovať pod menom užívateľa útočníkom

vytvorený zaručený elektronický podpis na úplne iný dokument a vyhotoviť archívny podpis na tieto falošné údaje. Rovnako podstrčenie falošného CRL by mohlo viesť k použitiu zrušeného certifikátu s diskreditovaným súkromným kľúčom. Tento bod je najkritickejší, je tu najväčšia možnosť falšovania údajov. Každý jeden certifikát a každý jeden CRL musí byť pred priložením do archívneho podpisu dôkladne preverený, je to úlohou certifikačnej autority. Jedinou možnosťou, ako sa vyhnúť sfalšovaniu certifikátu alebo CRL je dôkladne preveriť všetky stiahnuté údaje a nezanedbať žiadnu zo svojich povinností.

V neposlednom rade treba venovať zvýšenú pozornosť certifikátom koreňovej certifikačnej autority. Nazývame ich koreňové certifikáty. Neobsahujú podpis žiadnej vyššej certifikačnej autority (keďže taká neexistuje), ale sú podpísané súkromným kľúčom koreňovej CA (sú to tzv. self-signed certificate). Pre útočníka je ľahké k identifikačným údajom koreňovej certifikačnej autority pripojiť iný verejný kľúč a vytvoriť tak falošný certifikát. Rovnako ľahké je ale aj odhaliť takýto útok, pretože verejný kľúč koreňovej CA je verejne známy a dá sa overiť na internetovej stránke NBÚ alebo priamo v NBÚ. Pri vydávaní a zverejňovaní certifikátov koreňových CA musia byť dodržané prísne normy, aby nebolo možné sfalšovať koreňový certifikát.

# 6 Záver

V nasledujúcej časti zhrniem výsledky analýz o archívnych elektronických podpisoch. Podľa týchto výsledkov dám odpoveď na najzákladnejšiu otázku - či je koncept archívneho elektronického podpisu realizovateľný alebo nie.

Pri analýze informácie potrebnej na overenie archívneho zaručeného elektronického podpisu, ktorá musí byť pripojená ku každému takémuto podpisu, som uviedol tri príklady a odhadol veľkosť dát, ktoré je potrebné k podpisovanému dokumentu pripojiť.

V prvom príklade som sa snažil simulovať súčasnú situáciu na Slovensku. Množstvo prídavnej informácie bolo odhadnuté na 276.4 kB. V druhom príklade som uvažoval súčasnú situáciu v Nemeckej Republike. Na takúto úroveň očakávam, že sa Slovensko dostane v priebehu najbližších rokov až desiatok rokov. V tomto príklade bolo množstvo prídavnej informácie odhadnuté na 810 kB. Tretí príklad bol miernym rozšírením druhého, kedy som zvažoval potrebu použiť na niektorom mieste iný certifikát ako už priložený. Množstvo potrebnej informácie narástlo na 814 kB. Vo štvrtom príklade som uvažoval v rovnakých podmienkach extrémny prípad, kedy na overenie každého CRL bolo potrebné priložiť certifikáty celej certifikačej cesty. Aj v tomto extrémnom prípade bolo množstvo prídavnej informácie odhadnuté len na 1.07 MB.

Výsledkom analýzy potrebnej informácie je, že veľkosť prídavnej informácie je približne na rovnakej alebo menšej úrovni ako veľkosť podpisovaného dokumentu. Záverom analýzy je tvrdenie, že koncept archívneho zaručeného elektronického podpisu je v podmienkach SR realizovateľný.

Analýza bezpečnostných požiadaviek poukázala na možnosti útoku pri vytváraní archívneho zaručeného elektronického podpisu ako aj pri jeho overovaní. Aby sa útokom zamedzilo, aby nebolo možné vytvoriť platný archívny elektronický podpis s identifikačnými údajmi podpisovateľa na iný ako ním podpisovaný dokument a aby nebolo možné overiť neplatný archívny elektronický podpis je potrebné dodržať najmä všetky bezpečnostné opatrenia a nasledovné zásady:

1. vytvorenie archívneho zaručeného elektronického podpisu je nutné zveriť dôveryhodnej certifikačnej autorite,

2. všetky do archívneho podpisu vkladané informácie musia byť z dôveryhodných zdrojov a dôkladne preverené,
3. vytvorený archívny zaručený elektronický podpis je potrebné po jeho obdržaní ihneď overiť,
4. ak pri overovaní využívame službu certifikačnej autority, množina potenciálnych odpovedí CA musí byť dostatočne veľká,
5. akákoľvek komunikácia medzi užívateľom a certifikačnou autoritou musí prebiehať pomocou správ podpísaných zaručenými elektronickými podpismi.

V takomto prípade je proces vytvárania a overovania archívnych zaručených elektronických podpisov chránený pred možnými útokmi.

# 7 Smerovanie v budúcnosti

Pri písaní mojej diplomovej práce som sa dostal k návrhu novely zákona o elektronickom podpise [43], v ktorom NBÚ popisuje pripravované zmeny zákona č. 215/2002 Zb. o elektronickom podpise a o zmene a doplnení niektorých zákonov [15]. Návrh obsahuje 15 bodov, ktoré načrtávajú, akým smerom sa bude používanie elektronických podpisov na Slovensku v budúcnosti vyvýjať. Zatiaľ nie je isté, či a akým spôsobom budú tieto zmeny zapracované. V nasledujúcej časti sa pozriem len na uvažované zmeny súvisiace s formátom archívneho elektronického podpisu a ich prípadný pozitívny či negatívny dopad na procesy vytvárania a overovania archívneho elektronického podpisu.

V bode 2 sa uvažuje o pridaní pojmu dlhodobá archivácia elektronického dokumentu a k nemu vytvoreného zaručeného elektronického podpisu. Tento bod by som absolútne vypustil, vzhľadom k tomu, že archívny elektronický podpis má za úlohu ochranu dokumentu z dlhodobého hľadiska a teda požadovanú funkciu vieme pomocou neho zabezpečiť. Zavedenie tohoto pojmu je preto zbytočné.

Bod 3 by som rovnako vypustil, vzhľadom na nedefinovanie pojmu z bodu 2 a skutočnosť, že overenie archívneho elektronického podpisu nie je potrebné dávať za úlohu notárom.

V bode 5 sa uvažuje nad zmiernením, alebo úplným vypustením kontroly certifikačných autorít vydávajúcich certifikáty. Úplne vypustenie kontroly by som spočiatku určite nezvažoval. Čo sa týka zmiernenia, je potrebné presnejšie definovať, aké konkrétne zmeny sa chystajú. Pri nedostatočnej kontrole sa totiž otvára možnosť útokov a falšovania informácií.

Bod 13 zavádza pojem dobrovoľnej akreditácie. Cieľom tejto zmeny je zjednosdušiť a rozšíriť používanie zaručených elektronických podpisov. Vzhľadom k tomu, že pri komunikácii s orgánmi verejnej správy sa bude používať len kvalifikovaný certifikát, ktorý vydala akreditovaná CA, nevidím v realizácii týchto zmien problém. V konečnom dôsledku, užívateľ si predsa môže vybrať, či použije na vytvorenie podpisu kvalifikovaný certifikát, ktorý vydala akreditovaná CA, alebo mu stačí kvalifikovaný certifikát vydaný certifikačnou autoritou bez akreditácie.

Ostatné body, hoci sa týkajú elektronického podpisu a PKI, nemajú vplyv na formát archívneho elektronického podpisu. Ak by som mal aj napriek tomu vyjadriť svoj názor k týmto navrhovaným zmenám, pozitívne vnímam hlavne body 4, 10 a 14. Rovnako zmeny v bode 6 sú potrebné, pretože uvedené pojmy nie sú v zákone definované, hoci sa v praxi často používajú.

Takéto sú výhliadky do budúcnosti v oblasti elektronických podpisov. Aký efekt bude mať novela zákona o elektronickom podpise však záleží hlavne od spôsobu realizácie navrhovaných zmien. Až vtedy bude možné povedať, aký je ich skutočný prínos. Samozrejme netreba zabúdať na potrebu prehodnotiť možnosti použitia archívneho elektronického podpisu po aplikovaní prípadných zmien v Zákone o elektronickom podpise.

# 8 Zoznam použitých skratiek

**ABA** - American Bar Association

**AES** - Advanced Encryption Standard

**BSI** - Bundesamt für Sicherheit in der Informationstechnik

**CA** - Certifikačná autorita

**CAdES** - CMS Advanced Electronic Signatures

**CEM** - Common Evaluation Methodology

**CMS** - Cryptographic Message Syntax

**CRL** - Certificate Revocation List

**DES** - Data Encryption Standard

**DSA** - Digital Signature Algorithm

**DSS** - Digital Signature Standard

**EESSI** - European Electronic Signature Standardisation Initiative

**ETSI** - European Telecommunications Standards Institute

**ESI** - Electronic Signatures and Infrastructures

**EÚ** - Európska únia

**FIPS** - Federal Information Processing Standards

**IEC** - International Electrotechnical Commission

**IKT** - Informačné a komunikačné technológie

**ISO** - International Organization for Standardisation

**MD5** - Message Digest 5

**NBÚ** - Národný bezpečnostný úrad

**NIST** - National Institute of Standards and Technology

**NR SR** - Národná rada Slovenskej republiky

**OCSP** - Online Certificate Status Provider

**PAG** - PKI Assessmet Guidelines

**PKI** - Public Key Infrastructure

**PKCS** - Public Key Cryptography Standards

**PUB** - Publication

**RSA** - Rivest, Shamir, Adleman

**SHA** - Secure Hash Algorithm

**SHS** - Secure Hash Standard

**SR** - Slovenská republika

**TOE** - Target of Evaluation

**TTP** - Trusted Third Party

**Zb.** - Zbierka zákonov

# 9 Literatúra

[1] Olejár D. - Stanek M. *Úvod do teórie kódovania*. www.dcs.fmph.uniba.sk/studium/tkk/, 2005. stiahnuté 6.2.2006.

[2] Olejár D. - Janáček J. *Bezpečnostné aspekty systémov postavených na Open Source*. 2004.

[3] Stanek M. *Základy kryptológie*. www.dcs.fmph.uniba.sk/~stanek/crypto/, 2004. stiahnuté 8.11.2005.

[4] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Introduction and General Model*, volume 1, ISO/IEC, 1998.

[5] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Security Functional Requirements*, volume 2, ISO/IEC, 1998.

[6] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Annexes*, volume 2a, ISO/IEC, 1998.

[7] *International Standard ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation. Security Assurance Requirements*, volume 3, ISO/IEC, 1998.

[8] *Common Methodology for Information Technology Security Evaluation. Introduction and General Model*, volume 1, CEM 97/017, 1997.

[9] *Common Methodology for Information Technology Security Evaluation. Evaluation Methodology*, volume 2, CEM 99/045, 1999.

[10] *An Introduction to Computer Security. The NIST Handbook*, volume 800-12 of NIST Special Publication, NIST, 1996.

[11] Swanson M. - Guttman B. *Generally Accepted Principles And Practices for Securing Information Technology Systems*, volume 800-14 of NIST Special Publication, NIST, 1996.

[12] Swanson M. *Guide for Developing Security Plans for Information Technology Systems*, volume 800-18 of NIST Special Publication, NIST, 1998.

[13] *Digital Signature Standard (DSS)*. FIPS PUB 186-2 (+ Change Notice 1), NIST, 2000.

[14] *Information Technology - Security Techniques - Guide for the production of protection profiles and security targets*, ISO/IEC, 2000.

[15] *Zákon 215/2002 Zb. o elektronickom podpise a o zmene a doplnení niektorých zákonov*. www.zbierka.sk, 2002. stiahnuté 11.9.2006.

[16] *Vyhláška Národného bezpečnostného úradu č. 537/2002 Zb. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky*. www.zbierka.sk, 2002. stiahnuté 15.9.2006.

[17] *Vyhláška Národného bezpečnostného úradu č. 538/2002 Zb. o kvalifikovaných certifikátoch*. www.zbierka.sk, 2002. stiahnuté 15.9.2006.

[18] *Security Considerations with Electronic Commerce*, volume 10, BSI, 1999.

[19] *BSI Manual for Digital Signatures*. BSI, 1997.

[20] *PKI Assessment Guidelines*. PAG v0.30 Public Draft for Comment, ABA, 2001.

[21] *Public Key Infrastructure Study*. NIST, The MITRE Corporation, 1994.

[22] Branchaud M. *A Survey of Public-Key Infrastructures*. McGill University Montreal, 1997.

[23] *Formáty zaručených elektronických podpisov*. Verzia 1.2, NBÚ, 2005.

[24] *PKCS#1 : RSA Cryptography Standard*. v2.1, RSA Laboratories, 2001.

[25] *PKCS#3 : Diffie-Hellman Key-Agreement Standard*. v1.4, RSA La-

boratories, 1993.

[26] *PKCS#5 : Password-Based Cryptography Standard.* v2.0, RSA Laboratories, 1999.

[27] *PKCS#6 : Extended-Certificate Syntax Standard.* v1.5, RSA Laboratories, 1993.

[28] *PKCS#7 : Cryptographic Message Syntax Standard.* v1.5, RSA Laboratories, 1993.

[29] *PKCS#8 : Private-Key Information Syntax Standard.* v1.2, RSA Laboratories, 1993.

[30] *PKCS#9 : Selected Object Classes and Attribute Types.* v2.0, RSA Laboratories, 2000.

[31] *PKCS#10 : Certification Request Syntax Standard.* v1.7, RSA Laboratories, 2000.

[32] *PKCS#11 : Cryptographic Token Interface Standard.* v2.11, RSA Laboratories, 2001.

[33] *PKCS#12 : Personal Information Exchange Syntax.* v1.0, RSA Laboratories, 1999.

[34] *PKCS#15 : Cryptographic Token Information Syntax Standard.* v1.1, RSA Laboratories, 2000.

[35] *Final Report of the EESSI Expert Team.* EESSI, 1999.

[36] *Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats.* Technical Specification ETSI TS 101 733 v1.5.1, ETSI, 2003.

[37] *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).* Technical Specification ETSI TS 101 733 v1.7.3, ETSI, 2007.

[38] *Zákon 576/2004 Zb. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov.* www.zbierka.sk, 2004. stiahnuté 11.9.2006.

[39] Forišek M. *Archív elektronických dokumentov.* diplomová práca, 2004.

[40] Kováčik J. *Výklad informačnej bezpečnosti pre malé organizácie.* diplomová práca, 2003.

[41] Vaško J. *Časové značky v prostredí Slovenska.* diplomová práca, 2004.

[42] Sabol T. - Delina R. *Elektronický podpis.* www.zbierka.sk, 2002. stiahnuté 15.9.2006.

[43] *Hlavné body návrhu novely Zákona o elektronickom podpise.* NBÚ, 2007. - súčasť prílohy

# 10 Prílohy

### Príloha - Hlavné body návrhu novely zákona, ktorým sa mení a dopĺňa zákon č. 215/2002 Z.z. o elektronickom podpise z pohľadu NBÚ

1. Doplniť ekvivalent osvedčeného podpisu v elektronickej podobe (t.j. ekvivalent úradne osvedčeného podpisu a podpisu osvedčeného notárom).

2. Pridať pojem dlhodobá archivácia elektronického dokumentu a k nemu vytvoreného zaručeného elektronického podpisu, ktorá zaručí overenie zaručeného elektronického podpisu aj po exspirovaní kvalifikovaného certifikátu slúžiaceho na overenie zaručeného elektronického podpis.

3. Pridať povinnosti notárom, aby na požiadanie zabezpečili dlhodobé overenie zaručeného elektronického podpisu elektronického dokumentu na vopred dohodnutú dobu aj po exspirovaní kvalifikovaného certifikátu slúžiaceho na overenie zaručeného elektronického podpisu.

4. Právne a technické riešenie elektronického doručovania, elektronickej doručenky a potvrdenia prijatia elektronického dokumentu.

5. Upraviť výkon kontroly certifikačných autorít, predovšetkým zmierniť, resp. úplne vypustiť kontrolu certifikačných autorít vydávajúcich certifikáty.

6. Doplniť definície vybraných pojmov (koreňová certifikačná autorita, certifikačná cesta, podpisová politika).

7. § 7 zákona: definície kvalifikovaných certifikátov uviesť do súladu s medzinárodnými štandardmi - kvalifikovaným certifikátom je len certifikát podpisovateľa (len end-user certifikát) elektronického dokumentu a nie je to certifikát CA a ani certifikát na overenie OCSP alebo CRL. Kvalifikovaný certifikát musí obsahovať identifikátor certifikačnej politiky, ktorá jednoznačne identifikuje pravidlá vydania a použitia kvalifikovaného certifikátu.

8. § 12 ods. 2: zrušiť poskytovanie certifikačných služieb ako výkon podnikateľskej činnosti.

9. § 11 ods. 4 písm. a) bod 1 vypustiť bezpečnostnú spoľahlivosť certifikačnej autority s odkazom na zákon o ochrane utajovaných skutočností.

10. § 15 ods. 1 (zrušovanie certifikátov) rozšíriť o možnosť zamestnávateľa zrušiť zamestnancovi zamestnanecký certifikát v prípade skončenie pracovného alebo iného obdobného pomeru, v prípade zmeny podpisových právomocí zamestnanca atď.

11. Upraviť poskytovanie kvalifikovaných certifikačných služieb Národným bezpečnostným úradom pre vybrané orgány štátnej správy (silové rezorty).

12. Pojem časová pečiatka nebude v zákone definovaný, rovnako ako iné certifikáty než kvalifikované, aby sa neobmedzilo bežné komerčné použitie rôznych typov certifikátov a časových pečiatok + zaviesť pojem kvalifikovaná časová pečiatka. (Kvalifikovaná časová pečiatka je EP spájajúci čas prijatia žiadosti o vytvorenie časovej pečiatky s údajmi umožňujúcimi jednoznačné potvrdenie, že údaje, ktoré identifikuje existovali v danom čase a zmenu týchto údajov je možné odhaliť. Certifikát na overenie kvalifikovanej časovej pečiatky musí vydať ACA a v certifikáte musí byť minimálne uvedený identifikátor certifikačnej politiky, ktorý jednoznačne identifikuje pravidlá vydania a použitia certifikátu časovej pečiatky akreditovanou certifikačnou autoritou).

13. Zavedenie dobrovoľnej akreditácie (kvalifikované certifikáty budú spĺňať požiadavky zákona a každý, kto tieto požiadavky splní, môže bez obmedzenia vydávať kvalifikované certifikáty bez potreby akreditovania) a paralelné ustanovenie povinnosti, že na overenie ZEP pri komunikácii s orgánmi verejnej správy slúži len kvalifikovaný certifikát, ktorý vydala akreditovaná CA akreditovaná podľa zákona.

14. Vypustenie technických špecifikácií z vykonávacích predpisov (vyhlášky NBÚ č. 537-542/2002 Z.z.) a ich ustanovenie v štandardoch (kvôli väčšej flexibilite aktuálnych zmien týkajúcich sa dĺžky kľúčov, algoritmov, formátov dokumentov, ktoré je možné podpisovať ZEP atď).

15. § 11 doplniť prenesný výkon kontroly na základe zmluvy alebo možnosť prizvať iné fyzické alebo právnické osoby na výkon kontroly (ako riešenie výkonu fyzickej kontroly tam, kde tento výkon nie je možný pracovníkmi úradu).

**Obsah priloženého CD**

- *diplomova praca.pdf* - súbor s diplomovou prácou vo formáte PDF
- *Literatura*
  - *01 - codebook.pdf* - [1]
  - *02 - BezpecnostITsystemov.pdf* - [2]
  - *03 - krypto.pdf* - [3]
  - *04 - p1-v2.pdf* - [4]
  - *05 - p2-v2.pdf* - [5]
  - *06 - p2n-v2.pdf* - [6]
  - *07 - p3-v2.pdf* - [7]
  - *08 - cem97017.pdf* - [8]
  - *09 - cem-p2v10.pdf* - [9]
  - *10 - sp-800-12.pdf* - [10]
  - *11 - 800-14.pdf* - [11]
  - *12 - 800-18 Planguide.pdf* - [12]
  - *13 - dss_fips186-2-change1.pdf* - [13]
  - *14 - 27n2449.pdf* - [14]
  - *15 - zakon215_2002.pdf* - [15]
  - *16 - vy_nbu_537_02_zep.pdf* - [16]
  - *17 - vy_nbu_538_02_zep.pdf* - [17]
  - *18 - ecom_es.pdf* - [18]
  - *19 - bsi-e-signature.pdf* - [19]
  - *20 - hodn_pki.pdf* - [20]
  - *21 - mitre.ps* - [21]
  - *22 - PKI-Thesis.pdf* - [22]
  - *23 - formaty_zep.pdf* - [23]
  - *24 - pkcs-1v2-1d2.pdf* - [24]
  - *25 - pkcs-3.ps* - [25]

- *26 - pkcs5v2-0.pdf* - [26]
- *27 - pkcs-6.ps* - [27]
- *28 - pkcs-7.ps* - [28]
- *29 - pkcs-8.ps* - [29]
- *30 - pkcs-9.pdf* - [30]
- *31 - pkcs-10v1_7.pdf* - [31]
- *32 - pkcs-11v2-11r1.pdf* - [32]
- *33 - pkcs-12v1.pdf* - [33]
- *34 - pkcs-15v1_1.pdf* - [34]
- *35 - EESSI Final-Report_dig_signat.pdf* - [35]
- *36 - ts_101733v010501p.pdf* - [36]
- *37 - ts_101733v010703p.pdf* - [37]
- *38 - zakon576-04.pdf* - [38]
- *39 - e_arcihvy.ps* - [39]
- *40 - bezpecnost.pdf* - [40]
- *41 - cas.pdf* - [41]
- *42 - Elektronický podpis.doc* - [42]
- *43 - Hlavne body novely ZoEP_vNBU-1.doc* - [43]