Slovenská technická univerzita

Fakulta elektrotechniky a informatiky

Katedra informatiky a výpočtovej techniky

Podpora dištančného vzdelávania v predmete Systémové programovanie a asemblery

Tímový projekt

Členovia tímu:

Bc.

2003/2004 Tím č.10

Zadanie

Počet tímov: 2

Vedúci tímov: Ing. Adrián Bagala

Pre pedagogické účely vytvorte WEB aplikáciu demonštrujúc princípy a činnosti PKI. Taktiež demonštrujte použitie certifikátov verejného kľúča na podpisovanie a overovanie podpisov elektronických dokumentov u koncových používateľov.

Navrhnite a implementujte PKI a aplikáciu na podpisovanie a overenie podpisu elektronického dokumentu u koncového používateľa.

Pri návrhu rešpektujte platné štandardy.

Obsah

1 Úvod

Pri využívaní informácií a komunikačných technológií a neustálom zvyšovaní ich bezpečnosti, sa z týchto technológií stávajú veľmi silné a efektívne nástroje. Vďaka ich pôsobeniu nastávajú významné zmeny vo vnútornej organizácii rôznych inštitúcií, v požiadavkách na kvalifikáciu a v organizácii práce a taktiež vo vzťahu medzi občanmi a štátnou či verejnou správou.

Pri elektronickom spracovaní údajov sú v súčasnosti zvládnuté fázy prípravy dokumentov, manipulácia s nimi a ich distribúcia elektronickou cestou. Aby bolo možné bez problémov využívať tieto údaje pri prenose dokumentu, je potrebné zabezpečiť aj autenticitu a identifikáciu autora resp. odosielateľa. Toto umožňuje elektronický podpis, ktorý je z právneho hľadiska porovnateľný s klasickým „papierovým“ podpisom. Podľa platnej legislatívy je elektronický podpis akceptovaný aj pri súdnom konaní. Elektronický podpis umožňuje rôzne úrovne bezpečnosti, vzhľadom na povahu informácií, ktoré sa nachádzajú v dokumente.

2 Elektronický podpis - EP

2.1 Základné pojmy z oblasti PKI

Certifikačná autorita - poskytovateľ certifikačných služieb, ktorý spravuje certifikáty a vykonáva certifikačnú činnosť.

Certifikačná služba - najmä vydávanie certifikátov, zrušovanie platnosti certifikátov, poskytovanie zoznamu zrušených certifikátov, potvrdzovanie existencie a platnosti certifikátov, vyhľadávanie a poskytovanie vydaných certifikátov.

Digitálny dokument - číselne kódovaná ľubovoľná konečná neprázdna postupnosť znakov.

Podpísaný elektronický dokument - elektronický dokument, pre ktorý bol vyhotovený elektronický podpis, ak je tento elektronický dokument dostupný spolu s elektronickým podpisom daného dokumentu.

Súkromný kľúč - tajná informácia, ktorá slúži na vyhotovenie elektronického podpisu elektronického dokumentu.

Verejný kľúč - informácia dostupná overovateľovi, ktorá slúži na overenie správnosti elektronického podpisu vyhotoveného pomocou súkromného kľúča patriaceho k danému verejnému kľúču.

Elektronický podpis - 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 použitým na jej vyhotovenie.

Certifikát - Certifikát verejného kľúča (ďalej len „certifikát“) je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný. Certifikát sa skladá z tela certifikátu a z elektronického podpisu tela certifikátu. Telo certifikátu je elektronický dokument, ktorý obsahuje:

- identifikačné údaje,
- vydavateľa certifikátu,
- identifikačné číslo certifikátu,
- identifikačné údaje držiteľa certifikátu,
- dátum a čas začiatku a konca platnosti certifikátu,
- verejný kľúč držiteľa certifikátu,
- identifikáciu algoritmov, pre ktoré je uvedený verejný kľúč určený,
- identifikáciu algoritmov použitých pri vyhotovení elektronického podpisu tela certifikátu

Elektronický podpis tela certifikátu sa vyhotoví použitím súkromného kľúča, ktorý je na to určený.

Princíp šifrovania a digitálneho podpisu - Šifrovanie nie je metódou ochrany vlastnou len elektronickej komunikácii. Používalo sa dávno pred tým, než sa elektronická komunikácia začala rozvíjať. Šifrovanie je transformácia informácie do podoby, ktorá je nezrozumiteľná, ale z ktorej je možné získať pôvodnú formu použitím inverznej transformácie - dešifrovania. Príslušnú dešifrovaciu transformáciu musia poznať len osoby, ktoré majú mať možnosť správe rozumieť. V praxi sa často používa niekoľko verejne známych (de)šifrovacích algoritmov, ktoré realizujú transformáciu určenú (de)šifrovacím kľúčom. Dešifrovací kľúč je potom tým, čo musí poznať len adresát (prípadne aj autor) správy. Takéto algoritmy možno rozdeliť do dvoch kategórii - symetrické a asymetrické.

2.2 Analýza súčasného stavu

Dôveryhodnosť elektronického podpisu je zabezpečovaná tzv. pyramídou dôvery, umožňujúcej spoľahlivé overenie odosielateľa dokumentu (PKI, Public Key Infrastructure). Na jej vrchole je koreňová certifikačná autorita, ktorú spravuje NBÚ.

Pri prijatí zákona o o EP a vyhláškach naňho nadväzujúcich bol v elektronický dokument uznaný za rovnocenný s papierovým. Pri uvedení koreňovej certifikačnej autority NBÚ do prevádzky, boli vytvorené podmienky pre praktické využívanie elektronického podpisu. Toto sú však len prvé kroky, ktorých cieľom je zavedenie elektronického podpisu do praxe.

Analýza súčasného stavu však ukazuje, že to sú nevyhnutné, ale len prvé kroky na zavedenie elektronického podpisu do praxe.

Legislatívna úprava elektronického podpisu sa opiera o Smernicu EÚ č. 1999/93/EC z decembra roku 1999. Pri aplikácii zákona oEP v praxi vzniklo veľa rozporov, ktoré bude potrebné riešiť až po prípadnú novelizáciu príslušnej legislatívy. Prudký vývoj v tejto oblasti bude prinášať zmeny vo filozofii prístupu k elektronickému podpisu, takže bude dôležité zachovať kontinuitu procesu nasadzovania a využívania elektronického podpisu s cieľom zabrániť znehodnocovaniu investícií v tejto oblasti.

Bezpečnosť elektronického podpisu závisí okrem iného aj na použitých prostriedkoch. Legislatíva stanovuje podmienky pre ich použitie aj prostredníctvom certifikácie. Je zrejmé, že Slovensko, rovnako ako väčšina štátov vo svete, nemá a nebude schopné vytvoriť podmienky pre plošnú certifikáciu prostriedkov. Dôvodom je nielen finančná náročnosť, ale najmä nedostatok skúsených špecialistov a metodické zázemie. V konečnom dôsledku ide o dôveryhodnosť certifikátu a tá je úzko spojená s tradíciou a imidžom certifikačnej inštitúcie resp. skúšobne.

Akreditácia certifikačnej autority je vlastne potvrdenie najvyššej dôveryhodnosti a bezpečnosti inštitúcie, ktorá ju prevádzkuje. Kapitálové výdavky na jej zriadenie sa pohybujú na úrovni 100 – 150 mil. Sk. Rentabilita jej činnosti predpokladá spravovanie cca 300 až 500 tisíc certifikátov. Je zrejmé, že na slovenskom trhu nebude veľa subjektov, ktoré budú schopné takéto služby poskytovať. Potvrdzuje to aj doterajší vývoj. Skôr je možné očakávať infiltráciu zahraničných subjektov. To bude spojené s riešením mnohých problémov v záujme udržania dôveryhodnosti prostredia a použiteľnosti certifikátov.

Elektronizácia a spolu s ňou aj elektronický podpis sa budú rýchle rozvíjať. V rámci medzinárodného spoločenstva budú stále viac akcentované tlaky na normalizáciu a štandardizáciu v snahe zabezpečiť kompatibilitu použitia elektronického podpisu v čo najväčšom rozsahu. Dôležité bude zachytávať zmeny už v štádiu ich prípravy v záujme včasnej legislatívnej a technologickej prípravy.

Platobné karty, mobilné telefóny a elektronický podpis majú spoločnú vlastnosť, ktorou je ich plošné rozšírenie. Gestorom platobných kariet sú banky, mobilných telefónov telekomunikační operátori. Elektronický podpis takého gestora nemá. Zo zákona však vyplýva, že orgánom štátnej správy, zodpovedným za oblasť elektronického podpisu je NBÚ. Je potrebné aktivizovať jeho priamy vplyv na štátnu správu spolu s nepriamym vplyvom na certifikačné služby prostredníctvom ustanovení zákona. Logicky z toho vyplýva, že bezprostrednou úlohou je

nasadenie elektronického podpisu na samotnom úrade.

Zo zákona priamo vyplýva kontrola jeho ustanovení. Aktivity v oblasti elektronického podpisu boli až do prijatia zákona viac menej záležitosťou „zdravej“ úvahy. Váha, ktorú získal elektronický podpis prijatím zákona však vyžaduje vytvorenie korektného prostredia s vysokým stupňom bezpečnosti a tým aj dôvery. Kontrola, nasmerovaná na udržanie „čistoty“ prostredia t.j. jeho bezpečnosti, by nemala mať reštrinktívny charakter (aj keď sa tomu nebude dať vždy zabrániť). Mala by predovšetkým smerovať k rozvoju elektronického podpisu a podpore všetkých aktivít, ktoré smerujú ku konečnému výsledku – vytvoreniu prostredia, založeného na elektronickej správe dokumentov.

Keďže elektronický podpis je „prierezový“ fenomén, dotýkajúci sa všetkých sfér aktivít spoločnosti, je potrebné prepájať resp. koordinovať, aktivity, spojené s jeho rozvojom, s aktivitami v iných oblastiach, nadväzujúcich na neho.

2.3 Teoretický základ elektronického podpisu

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

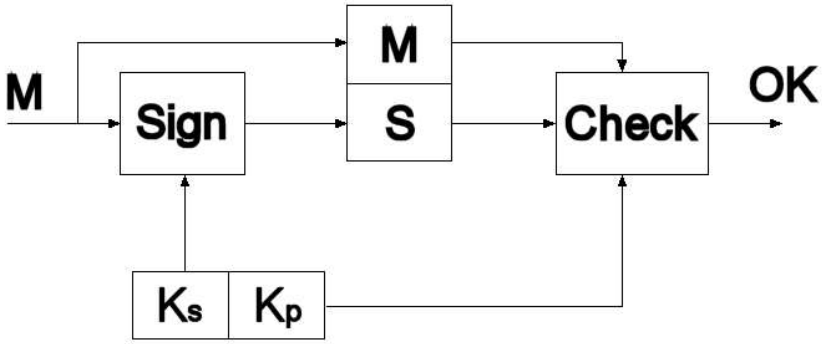
Nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu.

Na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie, jednoduchšie povedané, je to mechanizmus na zaistenie dôkazu pravosti dát (dokumentov).

Z právneho hľadiska sú „podpis“ a „elektronický podpis“ ekvivalentné. Elektronický podpis však zaručuje, že dokument od okamihu podpisu nebol zmenený, jednoznačne identifikuje podpisovateľa a, ak je to potrebné, aj čas podpisu.

Po matematickej stránke je elektronický podpis funkciou obsahu správy (M) a súkromného kľúča (Obr. 1). Výstupom tejto funkcie je hodnota (S), ktorá sa väčšinou pripojí na koniec

správy a je spolu so správou odoslaná. Príjemca správy môže na základe vlastníctva verejného kľúča odosielateľa overiť platnosť podpisu. Keďže elektronický podpis je funkciou správy, modifikácia správy po jej podpísaní spôsobí neplatnosť podpisu.



Obr. 1: Elektronický podpis zjednodušená schéma

2.4 Základné vlastnosti elektronického podpisu

Identifikácia autora - spôsob vyhotovenia a overenia elektronického podpisu umožňuje spoľahlivo určiť, ktorá fyzická osoba el. podpis vyhotovila.

Integrita - neporušenosť dokumentu, pozitívne overenie el. podpis zaručuje, že dokument nebol po podpise, napr. počas prenosu zmenený, upravovaný alebo poškodený.

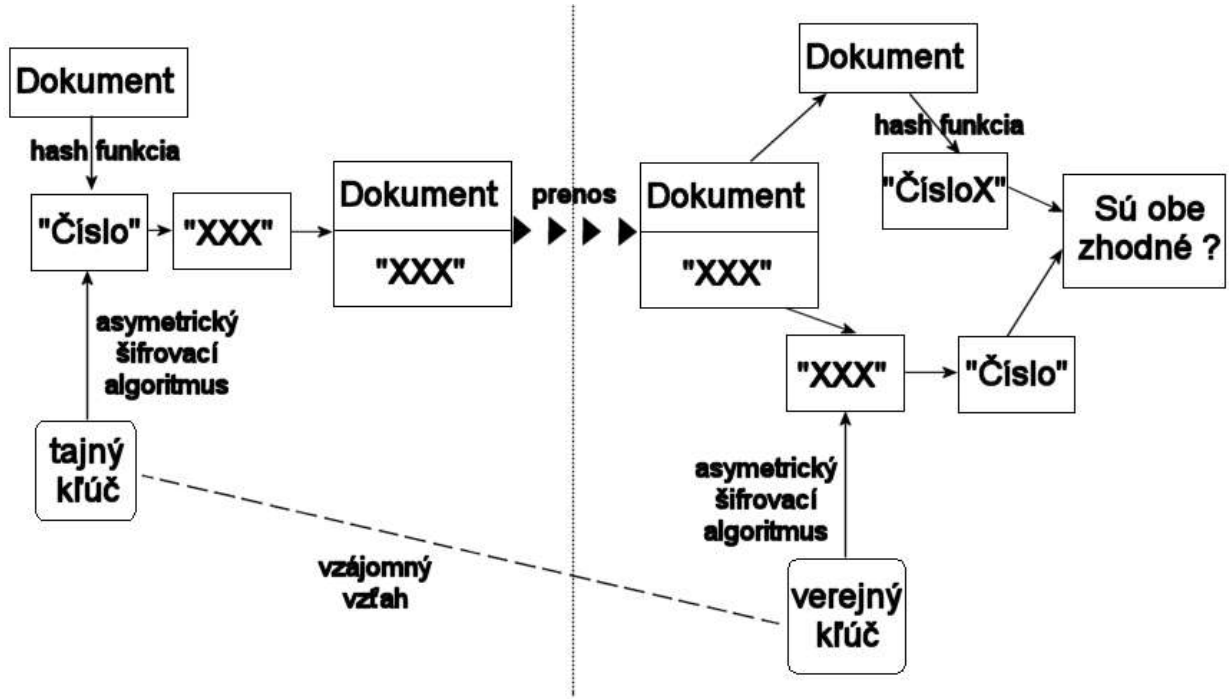
Nepopierateľnosť autorstva - jednoznačné priradenie autorstva dokumentu podpisovateľovi, nemožnosť odoprenia autorstva dokumentu.

Nemožnosť podpísať prázdny dokument - je vylúčené, resp. nie je možné podpísať „bianco“ dokumentu.

Elektronický podpis má podobu krátkeho elektronického súboru. (Nie „zoskenovaný“ ručný podpis.) Vznikne spracovaním podpisovaného elektronického dokumentu a súkromného kľúča v prostriedku, ktorého jediným a výlučným vlastníkom je podpisovateľ. Takto spracovaný elektronický súbor sa napokon pripojí k podpisovanému dokumentu (viď. obr. č. 2).

Základným princípom elektronického podpisu je vypočítanie „čísla“ (hash alebo odtlačok) z dokumentu, ktorý chceme podpísať. Algoritmus výpočtu tohto „čísla“ zaručuje, že pre každý dokument dostaneme iné, jedinečné „číslo“, t. j. aj v prípade keď sa dva dokumenty líšia len v jednom jedinom znaku, po výpočte dostanem pre každý dokument rozdielne „čísla“. Pravdepodobnosť, že existujú dva dokumenty s rovnakým „číslom“ je veľmi nízka. Aj keď je

teoretická možnosť vzniku dvoch kolíznych dokumentov je veľmi nepravdepodobné, že by mali zmyslu plný obsah.



Obr. 2: princíp elektronického podpisu

Elektronický podpis v stručnosti povedané je asymetrické zašifrovanie uvedeného „čísla“ osobouA pomocou tajného kľúča a pripojenie tohto zašifrovaného „čísla“ k dokumentu, čím sa toto zašifrované „číslo“ stáva elektronickým podpisom. Keďže je toto „číslo“ zašifrované asymetricky, nemožno ho odšifrovať tajným kľúčom použitým na šifrovanie ale je možné ho odšifrovať verejný kľúčom, ktorý s tajným kľúčom úzko súvisí a ktorý osobaA zverejnila.

Overenie takéhoto podpisu je potom možné na základe znalosti dokumentu, algoritmu pre výpočet „čísla“ a na základe znalosti verejného kľúča.

Osoba B, ktorá overuje podpis, si môže po prijatí dokumentu „číslo“ vypočítať pomocou toho istého algoritmu ako použila osoba A, čím dostane „číslo X“. Po odšifrovaní zašifrovaného „čísla“ pripojeného k dokumentu pomocou verejného kľúča a po porovnaní tohto odšifrovaného „čísla“ s vypočítaným „číslom X“ môžeme povedať:

1. ak sa vypočítané „číslo X“ s odšifrovaným „číslom“ zhoduje je zrejmé, že uvedený dokument podpísala uvedená osoba a dokument nebol pri prenose zmenený,

2. ak sa vypočítané „číslo X“ s odšifrovaným „číslom“ nezhoduje je zrejmé, že uvedený dokument alebo uvedená osoba nepodpísala alebo bol pri prenose zmenený.

Elektronický podpis robí dôkaz pravosti na základe vlastníctva súkromného (tajného) kľúča. Je teda nutné, aby sme vlastné súkromné kľúče dobre strážili. Strata kľúča pre nás znamená kompromitáciu obdobnú so zámenou odtlačkov v registri trestov, resp. sfalšovaniu fotky na našom občianskom preukaze.

Tajný kľúč a verejný kľúč sa označuje ako „kľúčový pár“. Oba kľúče si vytvára vlastník, napr. pomocou kryptografickej karty, generujú sa spolu, a ako už bolo povedané, je medzi nimi úzky vzájomný vzťah. Aby vlastník kľúčového páru nemusel každej osobe, s ktorou chce komunikovať s využitím elektronického podpisu osobne doručovať svoj verejný kľúč, bola vytvorená tzv. „infraštruktúra verejného kľúča (PKI – Public Key Infrastructure).

Táto infraštruktúra zahŕňa okrem osôb používajúcich elektronický podpis aj certifikačné autority (CA) a registračné autority (RA).

Úlohou registračnej autority je prevzatie verejného kľúča od klientov, overovanie totožnosti a osobných údajov klientov, posielanie žiadostí certifikačnej autorite o vydanie certifikátu verejného kľúča, odovzdanie klientského certifikátu a odovzdanie certifikátu verejného kľúča certifikačnej autority klientom.

Certifikát verejného kľúča obsahuje najmä základné identifikačné údaje o vlastníkovi verejného kľúča, samotný verejný kľúč, údaje o certifikačnej autorite, ktorá certifikát vydala, dobu platnosti certifikátu a samozrejme elektronický podpis certifikátu vytvorený tajným kľúčom certifikačnej autority.

Overenie certifikátu a tým aj overenie osoby, ktorej je certifikát vydaný spolu s overením verejného kľúča osoby prebieha podobne ako overenie dokumentu. Pred overením samotného dokumentu je teda najskôr potrebné, pomocou verejného kľúča certifikačnej autority, overiť totožnosť osoby, ktorá dokument podpísala.

Pre používanie elektronického podpisu, ktorý môže byť použitý v administratívnom styku so štátnou správou je však podľa zákona o elektronickom podpise potrebná ešte jedna certifikačná autorita, tzv. „Koreňová Certifikačná Autorita“, ktorú spravuje NBÚ.

„Koreňová Certifikačná Autorita“ sa nachádza na vrchole pyramídy infraštruktúry verejného kľúča. Úlohou „Koreňovej Certifikačnej Autority“ je vydávať certifikáty pre úradom akreditované certifikačné autority a verejný kľúč tejto certifikačnej autority slúži na overenie si pravosti certifikátu akreditovanej certifikačnej autority.

2.5 Certifikácia verejného kľúča

Mechanizmus boja proti podvrhnutiu verejného kľúča je certifikácia verejného kľúča, tj. pomocou certifikátu. Po vygenerovaní kľúčového páru si tajný kľúč dôkladne uložíme ako naše tajomstvo. Verejný kľúč neposielame priamo ďalším osobám, tie ich dostanú ako súčasť certifikátu. Certifikát vydáva certifikačná autorita. Najskôr musí Osoba A spraviť „žiadosť o certifikát“ – štruktúra obsahujúce identifikačné údaje Osoby A, ako občana (= predmet certifikátu), verejný kľúč Osoby A a poprípade ďalšie dáta. Túto štruktúru digitálne podpíše svojím práve vygenerovaným súkromným kľúčom a predá certifikačnej autorite. Certifikačná autorita si môže overiť totožnosť Osoby A na základe jej osobných dokumentov. Ak uzná certifikačná autorita žiadosť, že je v poriadku tak jej potom autorita vydá certifikát.

2.6 Časová pečiatka

Keď sa dokument posiela klasickou poštou, môže byť posielaný doporučene, tj, odosielateľ obdrží na pošte podací lístok, ktorý môže neskôr použiť ako dôkaz, že poslal dokument v konkrétnom čase.

Keďže systémový čas na počítači je veľmi ľahko zmeniteľný, mohla by OsobaA pri podpise elektronického dokumentu bez prítomnosti tretej osoby vložiť, akýkoľvek dátum. Preto pre podanie daňového priznania jednoduchý elektronický dokument nestačí. Problém transparentného určovania času rieši časové pečiatky (time stamps) a tzv. DV-certifikáty, čo je potvrdenie o existencii, držaní, resp. pravosti podpisu dokumentu v danom čase.

Časová pečiatka informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorú musela vyhotovyť akreditovaná CA použitím súkromného kľúča určeného na tento účel. Na verejný kľúč patriaci k uvedenému súkromnému kľúču bol vydaný kvalifikovaný certifikát. Časová pečiatka môže byť vyhotovená len použitím bezpečného zariadenia na vyhotovovanie časovej pečiatky a umožňuje jednoznačne identifikovať dátum a

čas kedy bola vyhotovená.

Časová pečiatka sa vyhotovuje na hash (odtlačok) dokumentu. Hash hodnota dokumentu sa doplní o požadovaný časový údaj (dátum a čas) z referenčného, zaručeného zdroja času akreditovanej CA. Takto upravený, doplnený hash sa podpíše zaručeným EP pomocou súkromného kľúča na tento účel určeného. Podobne ako EP aj časová pečiatka sa pripája k dokumentu, pre ktorý bola vyhotovená.

Dátová štruktúra časovej pečiatky obsahuje:

- Identifikácia bezpečnostnej politiky, pod ktorou bola pečiatka vydaná – politika pre vydávanie časových pečiatok
- Kontrolný súčet (hash) zaslaný klientom (skopírovaný zo žiadosti o časovú pečiatku)
- Jednoznačné sériové číslo časovej pečiatky
- Čas vydania pečiatky
- Prípadné rozšírenia časového razítka

Názov autority, ktorá pečiatku vydala môže byť uvedená v rozšírení, ale väčšinou je uvedená len v certifikáte, ktorým sa verifikuje elektronický podpis časovej pečiatky. Časová pečiatka je len dôkaz o existencii dokumentu v danom čase, nič nehovorí o vlastníctve dokumentu nejakého subjektu v danom čase, takže z reálneho prostredia –ešte nemáme samotný podací lístok, len razítko s časom. Samotný podací lístok v elektronickej podobe je DV-certifikát.

2.7 DV-certifikát

Je nutné mať elektronickú podobu podacieho lístku. Tou je DV-certifikát. Má podobnú štruktúru ako časová pečiatka, preto si ho mnohí zamieňajú so samotnou časovou pečiatkou. DV-certifikáty vydáva nezávislá autorita označovaná ako DVSC, ktorá prijíma žiadosti o vydanie DV-certifikátu nejakým bezpečným spôsobom, či už pomocou HTTPS, alebo S/MIME. Žiadosti sú elektronicky podpísané, takže DVCS robí autentifikáciu žiadateľa.

Rozlišujeme nasledujúce 4 typy služieb, certifikátov:

1. DV-časová pečiatka tj. potvrdenie o existencii kontrolného súčtu (hash) dokumentu v danom čase. Časová pečiatka od DVCS má kvalitatívne iné parametre ako bežná časová pečiatka. Základný rozdiel je v tom, že DVCS autentifikoval žiadateľa. DVCS môže vystaviť

- Anonymnú pečiatku – obdoba časovej pečiatky. Identifikácia prebieha inou cestou, napr. na základe súdneho rozhodnutia.
- Časová pečiatka obsahujúca identifikáciu používateľa, tj. potvrdenie o tom ,že daný žiadateľ mal v konkrétnom čase vo svojom držaní konkrétny dokument. Toto bude to, čo nahradzuje podací lístok.

2. Potvrdenie o držaní celého dokumentu v danom čase, tj. nie len kontrolný súčet. Opäť môže byť anonymný aj neanonymný.
3. Overovanie platnosti elektronického podpisu dokumentu. Je to veľmi netriviálna úloha a pravdepodobne vyžaduje aj, aby bol dokument po podpise uložený v bezpečnom úložisku dát, ku ktorému bude mať DVCS prístup a voči ktorému bude DVCS porovnávať.
4. Vydanie DV-certifikátu o tom, že nejaký klasický certifikát bol v danom čase platný, nebol odvolaný.

2.8 PKI

PKI (Public Key Infrastructure) je sústava technických, ale hlavne organizačných opatrení spojených s vydávaním, správou a, používaním a odvolávaním platnosti kryptografických kľúčov, certifikátov. Jednou z možných noriem PKI definuje sada internetových štandardov RFC popisujúcich základní využitia asymetrickej kryptografie na Internete, naväzujú na ne normy týkajúce sa bezpečnej pošty S/MIME a iné.

Treba zdôrazniť, že normy PKI vychádzajú z noriem ITU-T rady X.500 (konkrétne X.509 pre popis certifikátu), ale špecifikujú konkrétnu množinu parametrov a praktík určených pre Internet. Teda nie všetky rozšírenia certifikátov popísaných v norme X.509. Preto by sme nemali používať spojenie „certifikát podľa X.509v3“, ale „certifikát podľa RFC-3280“.

Pre priblíženie uvediem zopár informácii o X.509.

X.509 je štandardom ITU-T (International Telecommunication Union) pre infraštruktúru verejného kľúča. X.509 medzi iným špecifikuje štandardné formáty pre certifikáty verejných kľúčov a „certification path validation algorithm“ – to je algoritmus, ktorý verifikuje autenticitu CA. Začína s tým čo podpísal daný certifikát a ide až k ROOT CA.

X.509 začalo v náveznosti na štandard X.500 a prevzal hierarchický systém certifikačných

autorít na vydávanie certifikátov. To je v protiklade s „web of trust“ modelom, ako PGP, kde hocikto (nie iba CA) môže podpísať (a takto potvrdiť validitu) iné certifikáty. Verzia 3, štandardu X.509 zahŕňa aj flexibilitu v podpore iných typológii napr. „bridge“ a „mesh“. Môže byť použitý aj v P2P spojeniach, aj v „OpenPGP-like web of trust“, ale týmto spôsobom sa teraz skoro vôbec nepoužíva. Systém X.500 nikdy nebol naplno implementovaný, a IETF PKI „working group“ prijalo štandardy k flexibilnejšej organizácii internetu. V skutočnosti termín certifikátu z X.509 obyčajne sa obyčajne spája s profilom štandardu z X.509 v3.

V systéme s X.509 CA vydáva certifikát, v ktorom sa zviaže verejný kľúč s daným „Distinguished name“ v tradícii X.500, alebo k alternatívnemu menu ako email, alebo DNS-položka. Trusted root certifikát nejakej organizácie, môže byť distribuovaný všetkým svojim zamestnancom, ktorí tak môžu využívať podnikový PKI systém. Prehliadače ako Microsoft Internet Explorer Netscape/Mozilla a Opera sa dodávajú s pred-inštalovanými koreňovými SSL certifikátmi, veľkých spoločností, ktoré tak majú výhodu že budú prístupné bez problémov.

2.9 Certifikačná Autorita - CA

Nasledujúce odstavce by mali poskytnúť pohľad na základné funkcie certifikačných autorít a princípov na ktorých sú založené.

Certifikačná autorita je základným stavebným prvkom hierarchickej štruktúry PKI. Hlavnou úlohou certifikačnej autority je vydávať, spravovať a rušiť certifikáty svojich klientov. Klientmi certifikačnej autority môžu byť buď koncový používatelia, alebo certifikačné autority nižšej úrovne.

CA má 4 najdôležitejšie aktíva, ktoré si musí dôkladne strážiť:

1) Súkromný kľúč CA je tým najväčším aktívom. Jeho kompromitácia je pre CA katastrofa, po ktorej už nemá zmysel opätovne činnosť CA obnovovať. Okrem súkromného kľúča musí CA chrániť aj sekvenciu vydaných čísel certifikátov, lebo vydanie 2 certifikátov s tým istým sériovým číslom je rovnakou katastrofou.
2) Databázu používateľov musí CA chrániť z hneď 2 dôvodov
   - CA nesmie vydať 2 osobám certifikát s takým istým predmetom
   - Databáza obsahuje osobné údaje ako rodné čísla, čísla občianskych preukazov
3) Archív súkromných šifrovacích kľúčov používateľov, ak takúto službu CA poskytuje

nesmie dopustiť zneužitie týchto súkromných kľúčov

4) Archív listín uložených na CA, archív vydaných certifikátov a CRL. V prípade certifikátov a CRL sa síce jedná o verejné informácie, ale údaje musia byť poskytované minimálne po celú dobu činnosti CA, aby bolo možné overiť dokumenty, ktoré boli podpísané certifikátmi vydanými touto CA.

Certifikáty je možné vydať takmer pre čokoľvek. Certifikát môže potvrdzovať totožnosť fyzickej osoby (napr. „John Doe“), funkcie v spoločnosti („AnyThing Help Desk“), Organizácie alebo časti organizácie („IT division, AnyThing inc.“) alebo môže potvrdzovať identitu server na Internete („www.anything.com“), alebo dokonca autenticitu a neporušenosť softvérového produktu.

Ako už bolo povedané, certifikát spája údaje o identite subjektu a jeho verejný kľúč. Ak tieto údaje o identite jednoznačne identifikujú objekt alebo subjekt reálneho sveta, takémuto certifikátu sa „digitálny identifikátor“ alebo „DigitalID“. V súčasnosti sa takmer výlučne používajú certifikáty vo formáte X.509, ktorého povinnou súčasťou je meno vo formáte „distinguished name“, ktoré obsahuje úplné informácie o subjekte, ako sú napríklad jeho meno, organizácia do ktorej patrí, lokalita, krajina, atď. Toto meno je zhodné s menom subjektu v adresárovej službe X.500, čo uľahčuje zaradenie certifikátov do existujúcich adresárov a iných informačných systémov.

Okrem mena subjektu obsahuje digitálne ID aj informácie o čase jeho platnosti, certifikačnej autorite ktorá ho vydala, použitých kryptografických algoritmoch a ďalšie rozšírenia upresňujúce alebo obmedzujúce jeho použitie. Najdôležitejšie z týchto rozšírení špecifikuje, či vydaný certifikát môže byť použitý ako certifikát podradenej certifikačnej autority alebo je to certifikát konečného používateľa.

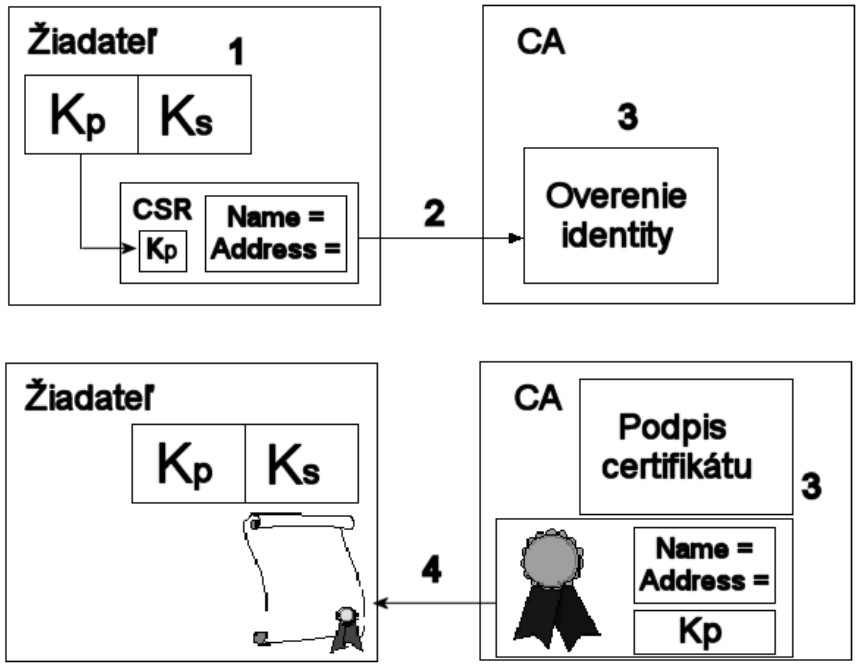
Proces certifikácie - Spôsob, akým certifikačná autorita vydáva certifikáty sa nazýva proces certifikácie (certificate enrollment). Tento proces pozostáva z niekoľkých krokov (Tab. 1).

Krok 1	Generovanie páru kľúčov
Krok 2	Odoslanie žiadosti o certifikát (certification request)

Krok 3	Overenie totožnosti žiadateľa certifikačnou autoritou a podpísanie certifikátu
Krok 4	Odoslanie certifikátu žiadateľovi

Tab. 1: Proces certifikácie

Prvým krokom je generovanie kľúčového páru na strane žiadateľa o certifikát. Vygenerovaný súkromný kľúč sa bezpečne uloží na strane žiadateľa a neprenáša sa na stranu certifikačnej autority, takže certifikačná autorita nemusí, a ani by nikdy nemala, poznať súkromný kľúč žiadateľa o certifikát. Druhým krokom je generovanie žiadosti o certifikát. Žiadosť o certifikát pozostáva z verejného kľúča žiadateľa o certifikát a informácií o jeho identite, celé podpísané súkromným kľúčom žiadateľa.



Obr. 3: Žiadosť o certifikát a podpis certifikátu

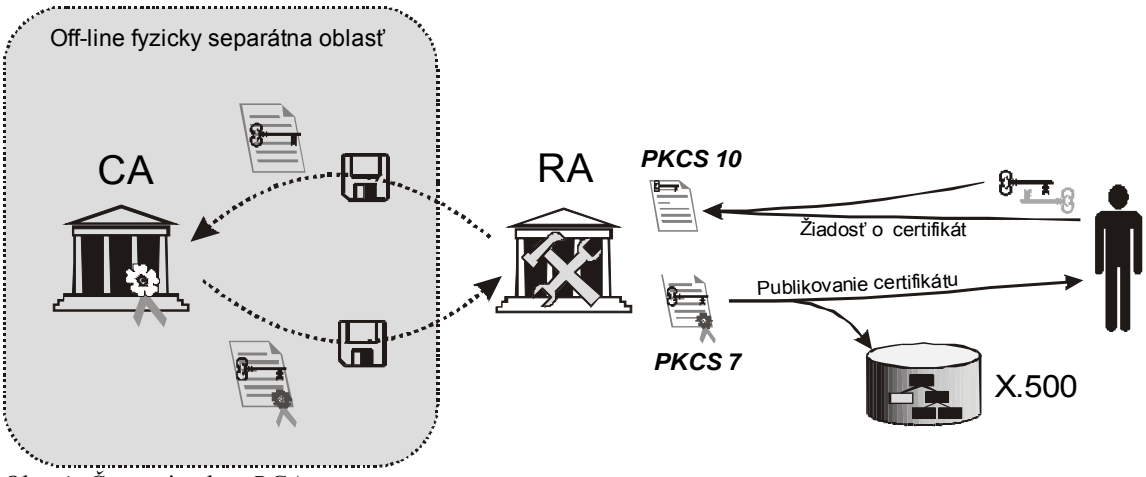
Táto žiadosť o certifikát je odoslaná certifikačnej autorite. V treťom kroku si certifikačná autorita overí identitu žiadateľa o certifikát (Obr. 3). Toto overenie môže siahať od jednoduchých metód ako napríklad poslanie správy s heslom na e-mailovú adresu žiadateľa až po nutnosť osobného kontaktu žiadateľa a zástupcu CA. Po úspešnej autentifikácií žiadateľa certifikačná autorita podpíše verejný kľúč žiadateľa spolu s informáciami o jeho identite

uloženými vo formáte X.509, čím vznikne výsledný certifikát (Obr. 3). Posledným krokom je odoslanie certifikátu žiadateľovi.

2.10 Registračná autorita – RA, iné súčasti CA

CA môže ďalej mať:

- Registračnú autoritu - prijíma žiadosti o vydanie certifikátu. Kontroluje súlad údajov v žiadosti o certifikát s údajmi v predloženom preukaze totožnosti žiadateľa o vydanie certifikátu. RA komunikuje s CA pomocou protokolu CMP, alebo protokolom CMC. Žiadateľ môže na registračnú autoritu priniesť priamo žiadosť o certifikát, RA overí totožnosť žiadateľa, verifikuje žiadosť o certifikát a predá žiadosť (podpísanú RA) CA. CA overí údaje z žiadosti používateľa a údaje doplnené RA a vydá/nevydá príslušný certifikát. Vydaný certifikát môže byť vrátený na RA, kde môže byť predaný žiadateľovi. Iný spôsob je pomocou jednorázového hesla, vydaného od RA, na vydanie certifikátu a užívateľ žiadosť o certifikát pošle elektronicky cez Online RA.
- Online RA slúži na k prijímaniu žiadostí elektronickou cestou, komunikuje pomocou protokolov CMC, resp, CMP. Typy žiadostí sú:
  - Obnovenie Certifikátu v dobe platnosti starého certifikátu používateľa
  - Vydanie nového (prvého) certifikátu na základe jednorázového hesla pre vydanie certifikátu
  - V prípade, že vlastní platný podpisový certifikát, môže žiadať o ďalšie.
  - Zálohovanie/obnovovanie svojho súkromného šifrovacieho kľúča na CA
  - CRL alebo iný certifikát vydaný CA.
- IVR, alebo telefónny záznamník slúžiaci na odvolávanie certifikátov inou cestou (telefón). používateľ sa autentifikuje jednorázovým heslom pre odvolávanie certifikátu. Odvolané certifikáty sa jednak radia do fronty certifikátov čakajúcich na odvolanie a tiež je možné Online transakciou informácie o odvolaní sprostredkovať OSCP serveru.
- Adresárové služby poskytujúce informácie o užívateľoch, ktoré si oni sami želajú aby boli zverejňované – hlavne vydané certifikáty a CRL.



Obr. 4: Činnosť online RCA

2.11 Žiadosť o odobranie certifikátu

Ak prídeme o súkromný kľúč, resp. sa vyzradí alebo iným spôsobom dôjde k jeho kompromitácii. Potom je nutné príslušný certifikát odvolať. Tu nezáleží na normách, ale na rýchlosti. Elektronickou formou je možné odvolať certifikát, pokiaľ máme certifikát na overovanie elektronického podpisu. Iný postup je možný napr. telefonicky, faxom, web-formulár za použitia jednorázového hesla, ktoré nám dá CA pri vydávaní certifikátu. Ak nieje možné ani to, treba ísť osobne s dokladmi k registračnej autorite.

2.12 Zneplatnené certifikáty - CRL

Certifikát môže sa zneplatniť jednak uplynutím času – validity uvedenom v certifikáte, ďalej z iniciatívy samotnej CA.

V praxi sa môže stať, že vydaný certifikát je nutné zneplatniť ešte pred vypršaním doby jeho platnosti. Keďže certifikát je informácia, ktorá sa dá voľne kopírovať, nedá sa držiteľovi priamo „odobrať“. Za účelom zneplatňovania certifikátov, ktorých doba platnosti ešte neskončila, si certifikačná autorita udržuje zoznamy zneplatnených certifikátov, (CRL, Certificate Revocation List). Ak má byť certifikát zneplatnený, je umiestnený na tento zoznam. Ak niekto robí dôležité operácie pri ktorých sa spolieha na certifikát, mal by si skontrolovať jeho platnosť prehľadaním zoznamu zneplatnených certifikátov.

Mechanizmus odvolávania,zverejňovania certifikátov zverejňuje CA v dokumente „Certifikačná politika CA“.

CRL obsahuje sériové čísla odvolaných certifikátov (CRL môže byť aj prázdy). Odvolané certifikáty sa zverejňujú v CRL až do vypršania ich pôvodnej platnosti (notAfter).

Štruktúra CRL pre internet je popísaná v RFC-3280, kt. vychádza doporučení X.509v2.Formáty CRL, resp. obmedzenia podľa NBU sú uvedené v prílohe a boli získané z NBU. Môžeme si spomenúť, že musí obsahovať:

- Pravdepodobný dátum a čas vydania ďaľšieho CRL
- číslo CRL, uvedené v príslušnom rozšírení CRL
- rozšírenie „Identifikátor kľúča certifikačnej autority“

```
CertificateList ::= SEQUENCE {
    tbsCertList TBSCertList,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue BIT STRING
}

TBSCertList ::= SEQUENCE {
    Version Version OPTIONAL,
    Siganture AlgorithmIdentifier,
    Isuuer Name,
    thisUpdate Time,
    nextUpdate Time OPTIONAL,
    revokedCertificates SEQUENCE {
      userCertificate CertificateSerialNumber,
      revocationDate Time,
      crlEntryExtensions Extensions OPTIONAL
    } OPTIONAL,
    crlExtensions [0] EXPLICIT Extensions OPTIONAL
}
```

Definícia CRL je podobná ako definícia certifikátu. Definuje sa postupnosť CertificateList, kt. hovorí že CRL je elektronicky podpísaná postupnosť. Zaujímavé je aké položky obsahuje TBSCertList.

- Prvá položka version je síce podľa X.509 voliteľná, ale RFC-3280 predpisuje, že musí byť v CRL použité a musí mať celočíselnú hodnotu 1.
- Položka signature obsahuje identifikátor algoritmov použitých pre EP CRL
- Položka issuer identifikuje, kto tento CRL vydal
- Položka thisUpdate –čas vydania CRL
- nextUpdate - čas ďalšieho vydania CRL

- revokedCertificates – vlastný zoznam odvolaných certifikátov

2.12.1 Rozšírenie CRL

Tieto rozšírenia môžeme nazvať ako kritické, RFC-3280 explicitne určuje 5 rozšírení:

- Číslo CRL
- Prírastkový CRL
- Identifikátor kľúča CA
- Alternatívne meno vydavateľa
- Disrtribučné miesto CRL –nejde o kompetné CRL

2.12.2 Rozšírenie položky CRL

Okrem samotného odvolania certifikátu, môže byť zaujímavý dôvod odvolania, resp. ďalšie informácie. Tieto rozšírenia by nemali byť označované ako kritické:

- Dôvod odvolania certifikátu
- Inštrukcie pre prípad odvolania certifikátu
- Dátum a čas kompromitácie súkromného kľúča
- Vydavateľ certifikátu

2.13 Online zisťovanie platnosti certifikátov - OCSP

V prípade, že držiteľ certifikátu zistí, že jeho súkromný kľúč bol skompromitovaný, tak mechanizmus CRL mu vyhovovať nebude, lebo do vydania ďalšieho CRL môže byť jeho súkromný kľuč zneužitý. Ak certifkát používa len v jednej aplikácii napr. komunikácia s bankou stačí ak informuje banku a CRL vôbec nepotrebuje. Ak však používa certifikát vo viacerých aplikáciách, požaduje zneplatnenie certifikátu od CA. Túto problematiku rieši protokol OCSP popísaný v RFC2560 . OSCP je protokol, ktorý sa používa na sprostredkovávanie real-time validácii statusu certifikátovOSCP je protokol typu klient/server . OSCP odpoveď je použitá na požiadavky o zistenie statusu certifikátu. Odpoveďou môže byť platný, neplatný, unknown. Táto odpoveď je vytvorená buď OCSP serverom samotnej CA, alebo CA môže delegovať svoju právomoc na iný server.

Vo svojej podstate môže byť OCSP užitočný aj v prípade, keď je CRL príliš veľký. Pri

každej manipulácii s certifikátom znamenalo prechádzanie celého CRL, čo by zabralo príliš veľa času, ale OCSP na jednoduchý dotaz odpovie jednoduchým výsledkom.

2.13.1 OSCP požiadavka

OSCP dotaz môže byť digitálne podpísaný, avšak elektronický podpis nie je povinný. OSCP server však môže nepodpísané dotazy odmietnuť.

```
OSCPRequest ::= SEQUENCE {
   tbsRequest TBSRequest,
   optionalSignature [0] EXOLICIT Signature OPTIONAL
}

Signature ::= SEQUENCE {
   signatureAlgorithm AlgorithmIdentifier,
   signature BIT STRING,
   certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL
}
```

Vnútro OSCP dotazu je sekvencia s položkami:

- Verzia
- Voliteľná položka requestorName, môže obsahovať identifikáciu OSCP klienta
- Položka requesteList obsahuje dotazy na platnosť jednotlivých certifikátov. Identifikácia certifikátov sa skladá z čísla certifikátu (serialNumber) a kontrolného súčtu, z mena CA issuer, a kontrolného súčtu z verejného kľúča CA (issuerKeyHash)

2.13.2 OSCP odpoveď

```
OSCPResponse ::= SEQUENCE {
   responseStatus OSCPStatus,
   responseBytes [0] EXPLICIT ResponseBytes OPTIONAL
}
```

Odpoveď sa skladá z obálky a tela odpovede. OSCP obálka obsahuje status odpovede a stavový kód môže byť:

- succesfull – odpoveď obsahuje informácie o platnosti požadovaných certifikátov
- malformedRequest – v dotaze bola syntaktická chyba
- internalError – chyba servera, odpoveď treba hľadať na alternatívnom serveri
- tryLater – server je momentálne nedostupný
- sigRequired – server akceptuje len podpísané dotazy, a klient poslal nepodpísaný
- unauthorized – klient nie je autorizovaný na takýto dotaz

Telo odpovede, je použiteľné pre niekoľko typov odpovedí, preto je v tvare:

```
ResponseBytes ::= SEQUENCE {
    responseType OBJECT IDENTIFIER,
    response OCTET STRING
}
```

Základná odpoveď :

```
BasicOSCPResponse ::= SEQUENCE {
    tbsResponseData ResponseData,
    signatureAlgorithm AlgorithmIdentifier,
    signature BIT STRING,
    certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL
}
```

Vnútro digitálne podpísanej správy (ResponseData) má nasledovné položky:

- Version – číslo verzie správy
- responserID – ID OSCP servera – buď jedinečné meno, alebo SHA-1 hash z verejného kľúča
- producedAt – čas podpisu OSCP odpovede
- responses – obsahuje sekvenciu odpovedí na platnosti jednotlivý certifikátov, pre každý certifikát odpovie sekvenciou pozostávajúcou z:
- certID – ID certifikátu udaného v dotaze
- certStatus – odpoveď či je certifikát : good, revoked, unknow. V prípade revoked obsahuje aj čas, resp. Dôvod
- thisUpdate – odpovedá thisUpdate v CRL
- nextUpdate – ak je čas na lokálnom OSCP systéme neskorší ako hodnota nextUpdate, odpoveď sa považuje za nevierohodnú

2.14 Zneplatnenie certifikátov

Následky zneplatnenia certifikátov na rôznej úrovni hierarchie certifikačných autorít sú rôzne v závislosti od toho aký a čí certifikát je zneplatnený. Všetky publikované zoznamy CRL a ARL musia byť široko dostupné pre všetkých používateľov PKI, aby bol zabezpečený prístup k týmto zoznamom, ktoré sú kľúčové na autentifikáciu a overovanie.

2.14.1 Zneplatnenie certifikátu koncovej entity

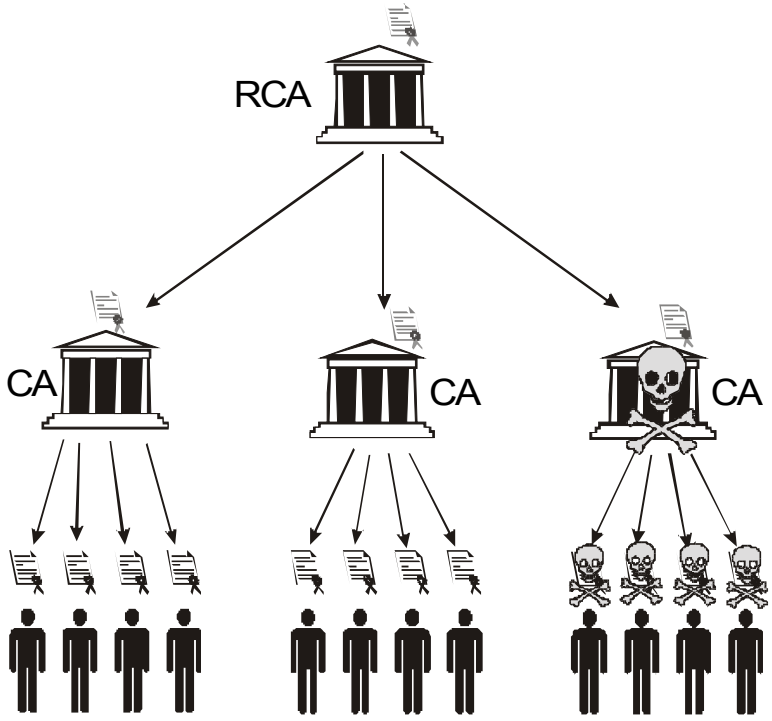
Zneplatnenie osobného certifikátu sa zaznamenáva do CRL vydanej CA, ktorá vydala certifikát používateľovi. CRL je potom pomocou X.500 alebo AD distribuovaná po celej sieti. Vydanie novej CRL, ktorá zneplatňuje certifikáty, sa uskutočňuje pre každú CA osobitne v pravidelných intervaloch. Pre koncové CA postačuje interval vydávania CRL (v zmysle zákona NR SR č. 215/2002 Z.z. o elektronickom podpise) 24 hodín. V prípade nutnosti zneplatnenia významného certifikátu ale môže byť požadované vydať CRL aj mimo tento čas a to okamžite. Ak dôjde k vydaniu CRL, je preto nutné zabezpečiť urýchlenú distribúciu tohto aktualizovaného zoznamu po celej sieti tak, aby bol okamžite dostupný pre všetky entity PKI.

Dôsledkom zneplatnenia certifikátu koncovej entity je nemožnosť vykonávania tej činnosti tejto entity, na ktorú potrebovala podporu PKI. V prípade podpisovania je entita upozornená (ak má už aktuálne CRL), že jej podpisový kľúč, ku ktorému bol vydaný certifikát, nie je považovaný za bezpečný. V prípade autentifikácie pomocou PKI bude entite zamietnutý prístup. V prípade, že certifikát využíva na iniciovanie šifrovaného spojenia, nedôjde k vzniku šifrovaného tunelu.

Keďže došlo k nedôvere kľúčov entity, je pre jej ďalšiu činnosť nutné vykonať nové vydanie všetkých jej certifikátov, ktoré boli prehlásené za neplatné. Pre nový certifikát, v prípade že došlo ku kompromitácii privátneho kľúča, je taktiež nutné vygenerovanie nového kľúčového páru.

2.14.2 Zneplatnenie certifikátu podriadenej CA

Zneplatnenie certifikátu podriadenej certifikačnej autority vykonáva RCA ako vydavateľ jej certifikátu. Zneplatnený certifikát je na zozname ARL, ktorý sa publikuje okamžite po vydaní rozkazu na zneplatnenie certifikátu podriadenej certifikačnej autority. Priamym dôsledkom zneplatnenia certifikátu nadriadenej certifikačnej autority je automatická nedôvera ku všetkým certifikátom vydaným touto autoritou.



Obr. 5: Dôsledok zneplatnenia certifikátu podriadenej CA

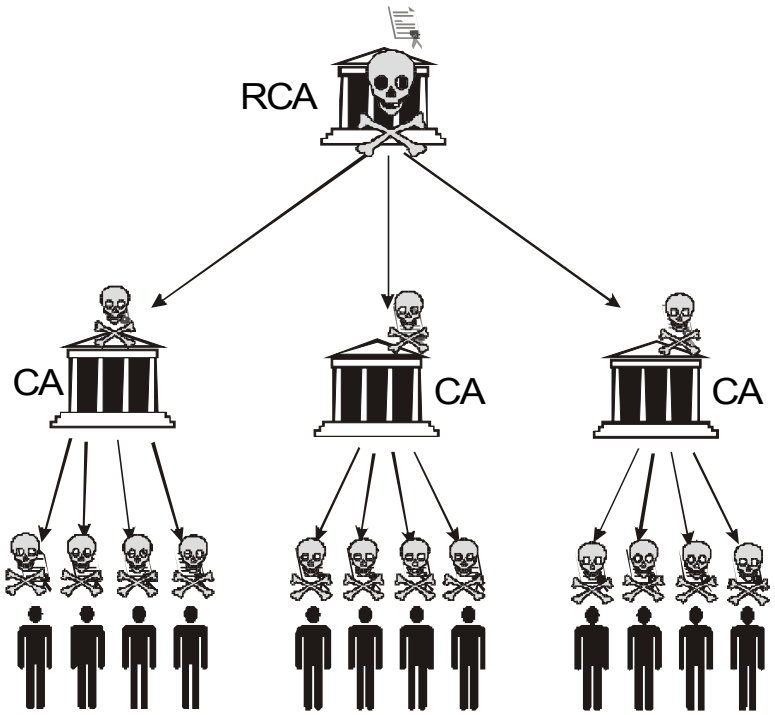
V čase obnovy činnosti certifikačnej autority je nutné opätovne vygenerovať kľúčový pár certifikačnej autority a ten dať podpísať nadradenej CA. Keďže pravdepodobne došlo aj ku kompromitácii hlavného úložiska obnovy kľúčov koncových entít, bude okrem opätovnej recertifikácie koncových entít a ich podpisovacích verejných kľúčov, nutné vygenerovať nové kľúčové páry používané na šifrovanie.

2.14.3 Zneplatnenie certifikátu RCA

Vydanie príkazu na zneplatnenie certifikátu RCA má závažný dopad na celú architektúru PKI. RCA ako hlavná certifikačná autorita certifikuje podriadené CA a tie potom vydávajú certifikáty koncovým entitám. Vzhľadom na dedičnosť dôvery v architektúre má zneplatnenie certifikátu RCA za následok nedôveru vo všetky certifikáty.

Na obnovu stavu po zneplatnení je nutné vykonať opätovnú certifikáciu podriadených CA, vystavenie ich pôvodných certifikátov na ARL a distribúciu týchto nových certifikátov smerom ku koncovým entitám. Vo všeobecnosti sa jedná o obdobný postup ako pri zneplatnení nižšie postavených certifikátov. Keďže došlo k zneplatneniu certifikátu RCA a potom k následnému

zneplatneniu smerom dole, nie je nutné opätovne generovať kľúčové páry pre podriadené CA vzhľadom na to, že nedošlo ani k potenciálnej kompromitácii ich kľúčov. Je však nutné vykonať opätovnú certifikáciu všetkých podriadených autorít. Ideálnym riešením je však úplná inicializácia celej štruktúry PKI.



Obr. 6: Dopad zneplatnenia certifikátu RCA na štruktúru PKI

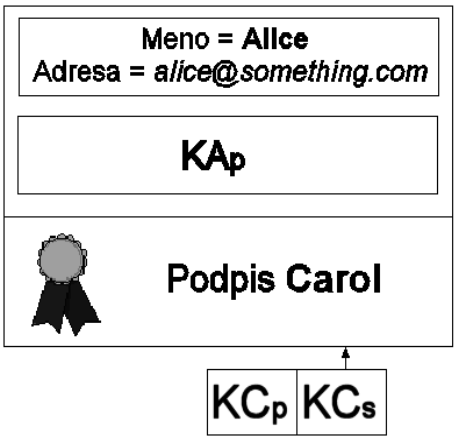
Práve z týchto dôvodov je kladený vysoký dôraz na fyzickú a personálnu bezpečnosť pri RCA, aby nedošlo k situácii, kedy je nutné zneplatniť certifikát RCA.

2.15 Certifikáty

Certifikát je DER kódovaná štruktúra a je to spojenie identity subjektu (meno, adresa, ...) a verejného kľúča patriaceho subjektu. Toto spojenie je digitálne viazané elektronickým podpisom dôveryhodnej tretej strany –certifikačnej autority. Ak by sme chceli uviesť certifikát pre Alice , ktorý vydal Carol tak by vyzeral , ako je zobrazený na Obr. 7.

Certifikát obsahuje údaje o Alicinej identite, čiže jej meno a elektronickú adresu. K týmto údajom je pripojený Alicin verejný kľúč (KAp) a celá táto štruktúra je podpísaná pomocou súkromného kľúča Carol (KCs). Elektronický podpis chráni integritu celej štruktúry certifikátu

pred modifikáciou. Takto zostavený certifikát môže byť bezpečne uložený na ktoromkoľvek verejnom mieste. Každý, kto vlastní kľúč Carol, bude vedieť overiť správnosť Alicinho kľúča a bude môcť s Alicou bezpečne komunikovať. Teraz sa Carol de facto stáva jednoduchou certifikačnou autoritou.



Obr. 7: Certifikát

Certifikát nemusí byť využívaný len pre potreby elektronického podpisu, túto možnosť popisujú protokoly CMP a CMC.

Certifikačná autorita môže overiť totožnosť používateľa, ale v každom prípade musí verifikovať elektronický podpis na žiadosť o certifikát. Keď uzná certifikačná autorita, že žiadosť je v poriadku vystaví certifikačná autorita certifikát.

Certifikát obsahuje mimo iného informácie o tom, kto ho vydal, sériové číslo certifikátu, identifikačný údaj používateľa, platnosť certifikátu a pochopiteľne verejný kľúč používateľa. Certifikát je digitálne podpísaný súkromným kľúčom certifikačnej autority.

Certifikát je často prirovnávaný k občianskemu preukazu, ktorý je vydávaný v tlačovej podobe, certifikát sa popisuje ako štruktúra v jazyku ASN.1 a medzi počítačmi je prenášaná v DER kódovaní.

Internetový formát certifikátu je popísaný normou RFC-3280. Táto norma je odvodená od doporučení ITU X.509. Pôvodná verzia X.509 č.1 vyšla v roku 1988 a bola postupne rozširovaná až do dnešnej verzie č.3. Verzia č.3 má tiež svoju históriu, bola revidovaná v roku 2000, ku ktorej boli ešte neskôr doplnené ďalšie dodatky. X.509 je veľmi zviazaná s adresárovou štruktúrou (napr. LDAP). V RFC-3280 sa od takýchto väzieb upustilo, ale použitie sa nevylučuje. X.509 je obsiahnutý v 3 normách:

- RFC-3279 - Algoritmus and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, ktorá špecifikuje použité kryptografické algoritmy.
- RFC-3280 – Internet X.509 Public Key Infrastructure Certificate and Revocation List (CRL) Profile, ktorá špecifikuje certifikáty a CRL.
- RFC-3281 – An Internet Attribute Certificate Profile for Authorization, ktorá špecifikuje atribútové certifikáty.

2.16 Štruktúra certifikátu

Štruktúru certifikátu podľa RFC-3280 zapisujeme v jazyku ASN.1:

```
Certificate ::= SEQUNCE {
    tbsCertificate TBSCertificate,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue BIT STRING
}
```

Certifikát je sekveciou vlastných sát certifikátu (tbsCertificate), algoritmu použitého certifikačnou autoritou pre elektronický podpis a certifikátu a (AlgorithmIdentifier) a vlastného elektronického podpisu.

Položka AlgorithmIdentifier je sama sekvenciou skladajúcou sa z identifikátoru objektu použitého algoritmu a jeho parametrov.

```
AlgorithmIdentifier ::= SEQUENCE {
    algorithm OBJECT IDENTIFIER,
    parameters ANY DEFINED BY algorithm OPTIONAL
}
```

Identifikátor objektu použitého pre elektronický podpis vždy identifikuje dvojicu: asymetrický algoritmus a algoritmus pre výpočet kontrolného súčtu.

Nás však zaujíma vnútro certifikátu:

```
TBSCertificate ::= SEQUENCE {
    version [0] EXPLICIT Version Default v1,
    serialNumber CertificateSerialNumber,
    signature AlgorithmIdentifier,
    issuer Name,
    validity Validity,
    subject Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL, – if
```

```
present, version shall be v2, or v3
   subjectUniqueID[2] IMPLICIT UniqueIdentifier OPTIONAL, - if
present, version shall be v2, or v3
   extensions [3] EXPLICIT Extensions OPTIONAL - if present version
shall be  v3
}
```

2.16.1 Verzia certifikátu

súvisí od verzie normy X.509 od ktorej je certifikát odvodený v1,v2,v3.

Vesion ::= INTEGER { v1(0), v2(1), v3(2) }

V prípade, v1 je hodnota 0 a táto položka sa vynecháva, lebo certifikát je v DER a DER kódovanie vynecháva položky, ktoré nadobúdajú implicitné hodnoty. Dnes sa snažíme, aby boli certifikáty vo verzii 3 a vyššie.

2.16.2 Sériové číslo certifikátu

Je definované ako celé nezáporné číslo: CertificateSerialNumber ::= Integer

Toto číslo musí byť jednoznačné v rámci danej certifikačnej autority – nesmú byť dva s rovnakým číslom. Dvojica serialNumber a issuer jednoznačne identifikujú certifikát. Max dĺžka sériového čísla nesmie byť viac ako 20 bajtov.

2.16.3 Algoritmus

Položka signature obsahuje algoritmus použitý CA pre vytvorenie elektronického podpisu certifikátu. Toto pole musí obsahovať rovnaký identifikátor, ako je v položke signatureAlgorithm – v štruktúre Certificate .

2.16.4 Platnosť certifikátu

Položka validity, určujúca platnosť certifikátu sa definuje:

```
Validity ::= SEQUENCE {
   notBefore Time,
   notAfter Time
}

Time ::= CHOICE {
   uctTIME UCTTime,
   generalTime GeneralizedTime
}
```

Táto položka má hlavne bezpečnostný charakter. Životnosť certifikátu by mala byť výrazne kratšia ako čas potrebný na prelomenie použitých algoritmov. Po uplynutí stanoveného obdobia však je nutné certifikáty stále uchovávať, aby bolo stále možné overovať dokumenty vytvorené v dobe platnosti certifikátu.

Doba platnosti je jedna vec a niečo iné je rozšírenie certifikátu „Doba platnosti súkromného kľúča“ – toto má asi najväčší význam pre elektronický podpis a obmedzuje dobu použitia súkromného kľúča patriaceho k verejnému kľúču uverejnenom v certifikáte. Doba platnosti súkromného kľúča je kratšia ako doba platnosti certifikátu. Vo formáte UTCTime môžeme uvádzať čas len do roku 2049 a potom už vo formáte generalisedTime.

2.16.5 Jedinečné mená

Jedinečné mená sa používajú pre podpis vystavovateľa certifikátu aj pre podpis predmetu certifikátu. Jedinečné meno (Distinguished name) je typu Name zavadeného normou X.501.

Oficiálna definícia jedinečného mena je:

```
Name ::= CHOICE { RDNSequence }
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
   Type AttributeType,
   Value AttributeValue
}

AttributeType ::=  OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

DirectoryString ::= CHOICE {
teletexString TeletexString (SIZE (1..MAX)),
printableString PrintableString (SIZE (1..MAX)),
universalString UniversalString (SIZE (1..MAX)),
utf8String UTF8String (SIZE (1..MAX)),
bmpString BMPString (SIZE (1..MAX)) }
```

Cieľom noriem rady X.500 je vytvoriť celosvetovú adresárovú štruktúru. Adresár predstavuje zoznam adries. Jeden záznam v takomto zozname potom zodpovedá jedinečnému

menu. Podobne aj jedinečné meno (tiež absolútne jedinečné meno, alebo RDNSequence) bude tvorené postupnosťou relatívnych jedinečných mien (Relative Distinguished Name).

Relatívne jedinečné meno je množina dvojíc tvorených z identifikátorov objektov (napr. Country, Organization, CommmonNAme apod.) a reťazcom (napr. SK).

Pomocou jedinečného mena špecifikujeme osobu. Rôzne štáty majú svoje pravidlá pre pomenovanie osôb, preto konkrétne využitie jednotlivých atribútov závisí na aplikácii. V prípade certifikátov potom na certifikačnej politike konkrétnej CA. Obecne by CA nemala meniť jedinečné meno pri kopírovaní žiadosti o certifikát do certifikátu. Výnimkou sú iba iba DNQualifier a SerialNumber, tie naopak bude s najväčšou pravdepodobnosťou CA doplňovať.

DNQualifier rozlišujeme 2 osoby, ktoré by inak mali taký istý subjekt.

SerialNumber rozlišujeme 2 certifikáty tej istej osoby.

Internetový profil certifikátu RFC-3280 predpisuje nasledujúcu podporu atribútov:

- Všetky aplikácie musia byť schopné v mene vydavateľa a predmete certifikátu spracovať nasledovné atribúty:
  - Country
  - Organization
  - Organization Unit
  - Dnqualifier
  - State or Province
  - Common Name
  - Serial Number
  - Domain Componet
- Aplikácia by mali byť schopné v mene vydavateľa a predmete certifikátu spracovať nasledovné atribúty:
  - Locality
  - Title
  - Surname
  - Given Name

- Initials
- Pseudonym
- Generation Qualifier

E-mail tu uvedený nie je, tá by mala byť v rozšírení „Alternatívne meno predmetu“ (rfc822Name)

2.16.6 Identifikátor údaju CA – Issuer

Položka issuer, po slovensky vydavateľ, alebo vydavateľ certifikátu, obsahuje jedinečné meno certifikačnej autority, ktoré ako celok tiež identifikáciou certifikačnej autority ako takej. Identifikátor musí byť jednoznačný.

2.16.7 Identifikátor údaju používateľa – subject

Položka subject sa do slovenčiny prekladá ako predmet certifikátu. Táto položka obsahuje jedinečné meno objektu, ktorému je certifikát vydaný – držiteľ certifikátu. Bližší popis nájdete zaoberajúcou sa jedinečnými menami.

Treba však zdôrazniť, že koreňové autority sú tzv. „self-signed“ – subject aj issuer majú rovnakú hodnotu. To znamená že koreňová autorita sama sebe podpisuje certifikáty.

2.16.8 Verejný kľúč

```
SubjectPublicKeyInfo ::= SEQUENCE {
Algorithm AlgorithmIdentifier,
subjectPublicKey BIT STRING }
```

Obsahuje SubjectPublicKeyInfo, čo je identifikátor algoritmu, pre ktorý je verejný kľúč určený, a samotný verejný kľúč.

2.16.9 Jedinečné identifikátory

Norma X.509v2 zaviedla 2 ďalšie položky certifikátu:

- IssuerUniqueID, kt. je určený na jednoznačné určenie vydavateľa certifikátu – ak položka issuer nepostačuje
- SubjectUniqueID, kt je určený na jednoznačné určenie predmetu správy – ak položka subject nestačí

RFC-3280 doporučuje tieto položky nepoužívať.

2.16.10 Štandardné rozšírenie certifikátu

Ak nám nestačia predchádzajúce položky, snažíme sa informácie uložiť do niektorého z rozšírení.

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
extnID OBJECT IDENTIFIER,
critical BOOLEAN DEFAULT FALSE,
extnValue OCTET STRING }
```

Softvér pracujúci s certifikátom musí poznať všetky kritické rozšírenia, inak musí certifikát odmientuť. Podľa RFC-3280 musí aplikácia minimálne rozoznať nasledovné rozšírenia:

- Key Usage
- Certificate Policies
- Subject Alternative Name
- Basic Constrains
- Name Constrains
- Policy Constrains
- Ext Key Usage
- Inhibit Any Policy

Mali by rozoznať

- authorityKeyIdentifier
- subjectKeyIdentifier

2.16.11 Privátne rozšírenia certifikátu

Toto rozšírenie je zavedené v RFC-3280(nie v X.509) a používajú sa nasledovné objekty:
id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6) internet(1) security (5) mechanizmus(5) pkix(7) }
id-pe OBJECT IDENTIFIER ::= { id-pkix 1 }
id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }

Toto rozšírenie obsahuje informácie o tom, ako pristupovať k informáciám a službám CA.

2.16.12 Rozšírenia používané Microsoftom

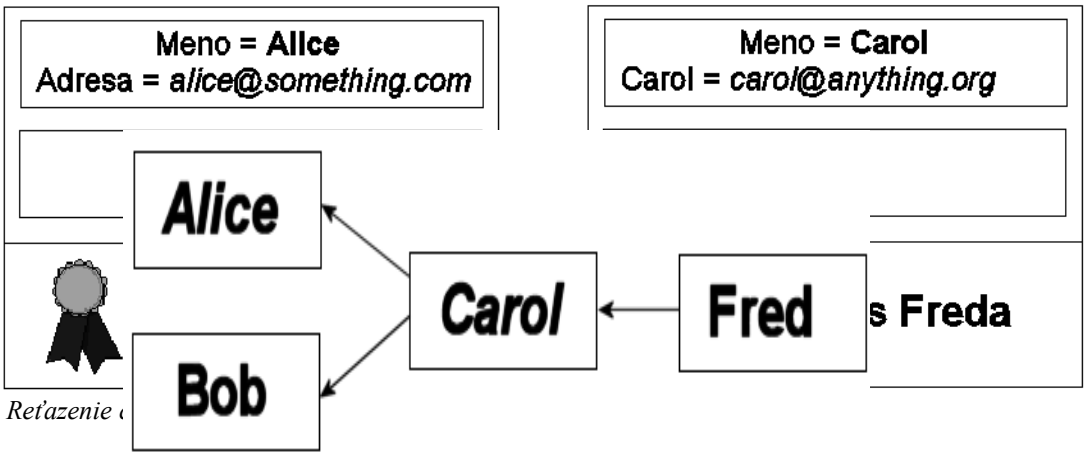
Microsoft vo svojich produktoch používa ešte iné rozšírenia – šablóna certifikátu. OID (extnID) ={1.3.6.1.4.1.311.20.2}

2.17 Kvalifikované certifikáty

Kvalifikovaný certifikát je zvláštny typ certifikátu, ktorý používa Európska únia aj Slovenská Republika vo svojej legislatíve. Zvláštny nie je syntaxom – je podmnožinou certifikátu popísanom v predošlej pod-kapitole, tj certifikátu podľa RFC-3280. Zvláštnosť je v právnej oblasti. Cieľom je zrovnoprávniť elektronický podpis a fyzický podpis rokov. Zaoberá sa tým RFC-3039. Kvalifikovaný certifikát sa vydáva konkrétnemu človeku (nie serveru). U kvalifikovaných certifikátov nestačí, aby mali 2 osoby iba jednoznačné a rôzne predmety, ale musia mať aj rozdielne verejné kľúče. V SR je použitie kvalifikovaného certifikátu vymedzené zákonom o elektronickom podpise, ktorý je rozobraný v inej kapitole. Takisto foráty kvalifikovaného certifikátu sú uvedené v prílohe tak, ako sú určené Národným Bezpečnostným Úradom Slovenskej Republiky.

2.18 Reťazenie certifikátov

Vzťah, ktorý vznikol medzi Alice a Carol vydaním certifikátu pre Alice, je možné definovať ako priamy vzťah dôvery, keďže Alice priamo pozná Carol a verí jej. Carol však sama môže mať certifikát, potvrdzujúci jej identitu (Obr. 8). Takto vzniká reťazenie certifikátov a tým pádom aj tranzitívny, nepriamy vzťah dôvery medzi Alice a Fredom. Z celkového pohľadu je celá takto vzniknutá štruktúra zobrazená na Obr. 9. Takáto hierarchická štruktúra nemá ďaleko od skutočne používaných štruktúr vytvorených pomocou reťazenia certifikátov. Takýmto štruktúram sa všeobecne hovorí „infraštruktúra verejných kľúčov“ alebo PKI (Public Key Infrastructure).



Obr. 8: Reťazenie c

Obr. 9: Príklad hierarchie certifikátov

Na prenos informácie o nadradených certifikačných autoritách a teda certifikátoch týchto autorít v PKI sa používa zreťazovanie certifikátov (PKCS-7 certificate chain). V praxi sa potom k správe okrem certifikátu, ktorým prebehlo podpisovanie, priloží aj certifikát entity, ktorá podpísala certifikát a tak rekurzívne ďalej. Táto reťaz nemusí byť vždy úplná za podmienky, že príjemca má možnosť získať PKC nadradených entít. Príjemca potom na overenie potrebuje overiť všetky podpisy. Okrem priloženia celého certifikátu je možné vložiť iba odkaz na certifikát vo forme unikátneho identifikátora certifikátu a certifikačnej autority, ktorá ho vydala.

2.19 PKI – Infraštruktúra

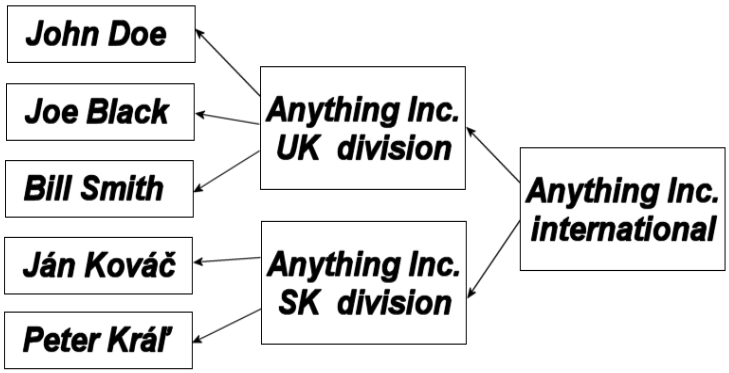
V predchádzajúcich odstavcoch sme si ukázali čo je to certifikát a ako možno vytvárať štruktúry pomocou reťazenia certifikátov. Aká celková štruktúra sa nakoniec vytvorí je závislé od procedúr vydávania certifikátov jednotlivými subjektami. Ak napríklad majú právo vydávať certifikáty všetky subjekty, môže sa vytvoriť štruktúra zodpovedajúca všeobecnému orientovanému grafu (pavučina). Ak však certifikáty vydávajú len niektoré subjekty (certifikačné autority), môže vzniknúť prísna hierarchia alebo niekoľko oddelených stromov.

Najbežnejšie používané infraštruktúry verejných kľúčov (PKI) budú popísané v nasledujúcich odstavcoch.

2.19.1 Hierarchia

Štruktúra, ktorú vytvárajú certifikačné autority sa nazýva hierarchia. Táto stromová štruktúra

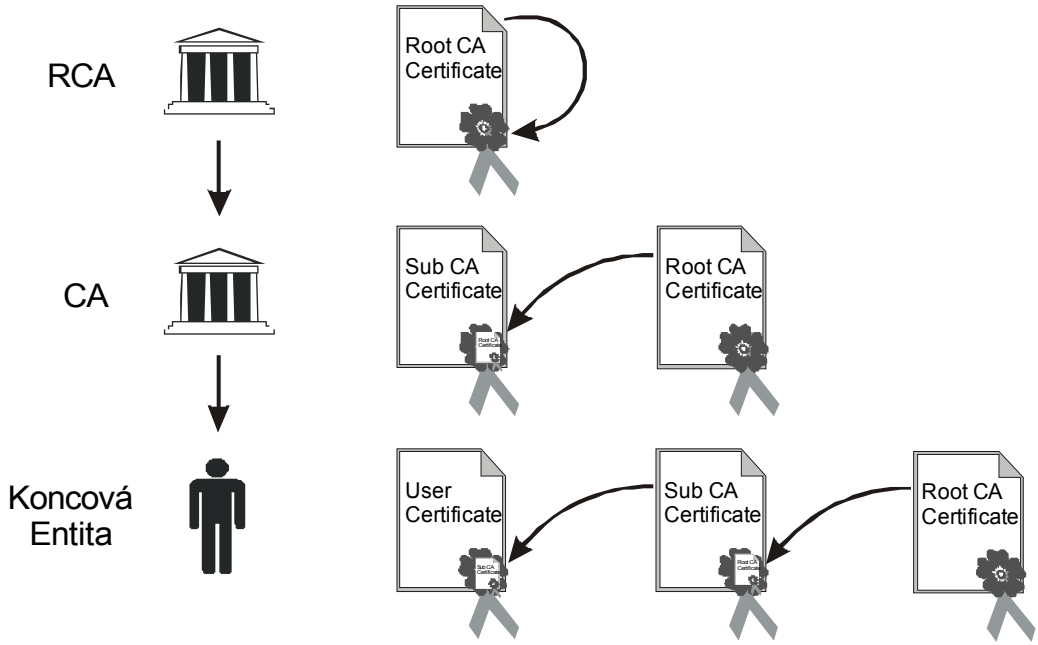
väčšinou zodpovedá hierarchií autorít reálneho sveta. Certifikačné autority vznikajú v miestach, ktoré prirodzene môžu overovať svojich klientov. Firmy certifikujú svojich zamestnancov, školy svojich študentov, obce svojich obyvateľov. Tieto lokálne certifikačné autority sú certifikované nadradenými certifikačnými autoritami s väčšou územnou pôsobnosťou. Napríklad certifikačná autorita univerzity vydá certifikát pre podradenú certifikačnú autoritu fakulty. Certifikačná autorita regiónu bude certifikovať certifikačné autority obcí. Príklad takto vytvorenej hierarchie je ilustrované na Obr. 10. V praxi existuje väčšinou niekoľko nezávislých hierarchií a jedna fyzická osoba môže mať niekoľko nezávislých identít certifikovaných v nezávislých stromoch. Napríklad, obchodný riaditeľ firmy bude mať certifikát vydaný na „John Doe, Sales Director, AnyThing, Inc“, ktorý bude používať na služobnú komunikáciu a druhý certifikát vydaný na „John Doe, Baker Street 222, London, UK“ používaný na súkromnú komunikáciu.



Obr. 10: Príklad hierarchie certifikačných autorít

Hierarchia certifikačných autorít je vlastne usporiadaním rôznych CA na základe dôvery do obmedzujúceho vzťahu dôvery. Hierarchia je znázorňovaná pomocou stromovej štruktúry nadriadenosti a podriadenosti CA. CA v umiestnené v rámci hierarchie využívajú ako základ dôvery práve RCA, ktorá tvorí vrchol stromu. RCA ako vrchol podpisuje certifikáty certifikačným autoritám, ktoré sú priamo jej podriadené a zároveň si podpisuje certifikát sama sebe.

Infraštruktúra certifikačných autorít vytvára obmedzenú možnosť vydávania certifikátov, preto iba dôveryhodné systémy môžu vydávať certifikáty, čím je zabránené nekontrolovanému vydávaniu certifikátov.



Obr. 11: príklad postupného podpisovania certifikátov pri hierarchii

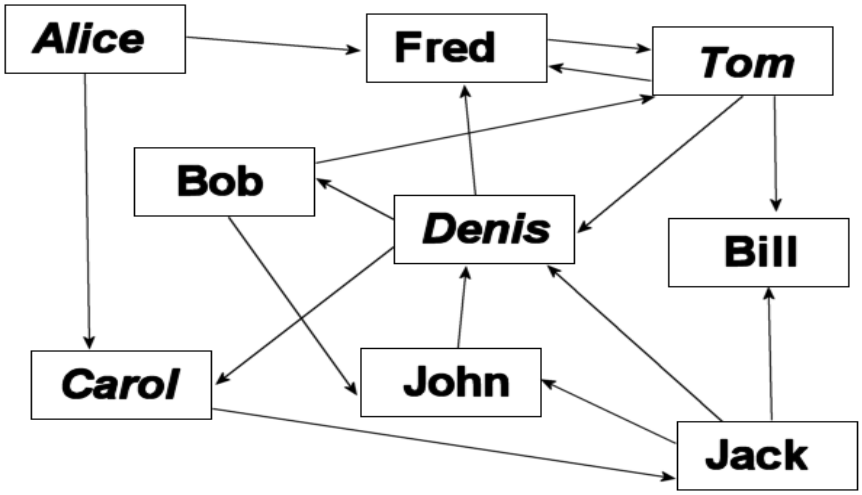
Hierarchická štruktúra umožňuje vymieňať si medzi sebou dôveru. Dve organizácie si môžu navzájom uznávať certifikáty, ak certifikačná autorita jednej organizácie podpíše PKC certifikačnej autority druhej organizácie a naopak. Týmto pádom, ak niekto v organizácii A obdrží správu z organizácie B, vie overiť pravosť certifikátu a teda autenticitu a integritu dokumentu.

Hierarchia je najbežnejšia používaná štruktúra PKI, pretože dobre modeluje existujúce štruktúry reálneho sveta. Táto štruktúra je podporovaná štandardmi X.509, SSL, S/MIME, IPsec a mnohými ďalšími.

2.19.2 Pavučina

V prípade, že neplatia žiadne regulácie a obmedzenia vydávania certifikátov, vznikne štruktúra bez formy podobná pavučine. V tejto štruktúre môže každý subjekt vydávať certifikáty a tak môžu vzniknúť zložité vzťahy dôvery medzi subjektami v štruktúre. Príklad takejto štruktúry je uvedený na obrázku Obr. 25. Na vyhodnocovanie dôvery v takto zložitej štruktúre sú často potrebné zložité algoritmy a celkovo sa vzťahy ťažko hľadajú. Takáto štruktúra vzniká najmä v prostrediach, kde neexistujú prirodzené autority schopné certifikácie. Pavučina dôvery je prirodzená štruktúra používaná systémom PGP (Pretty Good Privacy).

Štruktúra Web of Trust je vhodná pre prostredie, kde dochádza k vysokému stupňu vzájomnej dôvery jednotlivých členov siete. Jednotlivý členovia doverujú svojmu okoliu.



Obr. 12: Pavučina dôvery (web-of-Trust)

Vzhľadom na vysokú voľnosť vo vydávaní certifikátov táto schéma nie je vhodná na nasadenie v prostredí vysokej dôvernosti prenášaných informácií. Chýba centrálny bod od ktorého všetci odvádzajú svoju dôveru. Neobmedzovanie možnosti vydávania certifikátov pri Web-of-trust tvorí organizovaný chaos ohľadom certifikátov. Nový certifikát pri takejto štruktúre môže vydať ľubovolná entita. Vydávanie certifikátov nie je pri tejto hierarchii vôbec obmedzované. Dôležitá je iba dôvera medzi jednotlivými susediacimi entitami v sieti.

2.20 Vzťahy medzi certifikačnými autoritami

V predchádzajúcich bodoch boli popísané rôzne architektúry, ktoré sú používané pri stavbe PKI. Ich popis bol zameraný hlavne na spôsob distribúcie dôvery v rámci štruktúry certifikačných autorít. Nasledovná kapitola detailne analyzuje vzťahy, ktoré môžu vznikať pri hierarchii certifikačných autorít.

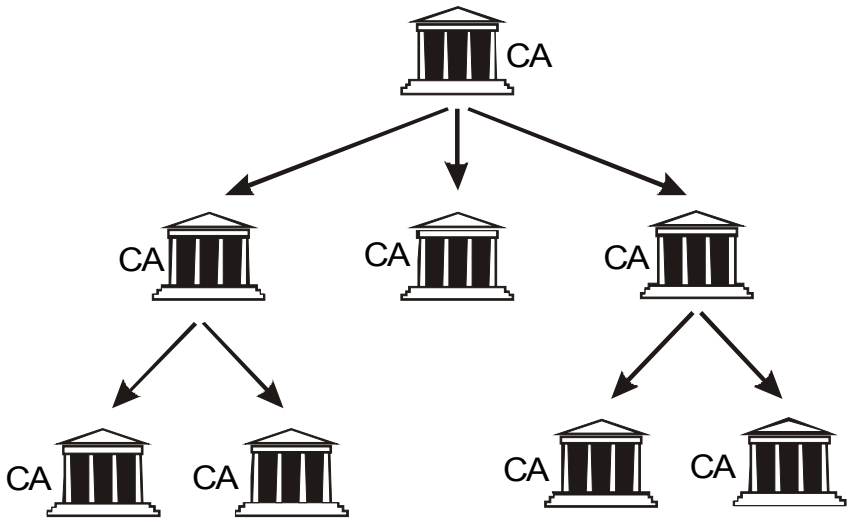
2.20.1 Podriadenosť CA

Relácia podriadenosti certifikačných autorít vzniká ak máme jednu nadradenú certifikačnú autoritu a jej podriadime ostatné. Tento vzťah najlepšie vidno práve pri RCA, kedy RCA tvorí vrchol stromu certifikačných autorít a je postavená nad všetky autority. V takomto prípade môže RCA ako vrchol stromu ktorému, všetci dôverujú, definovať bezpečnostnú politiku akceptácie certifikátov medzi jednotlivými podriadenými certifikačnými autoritami. Vzhľadom na dedičnosť dôvery stačí, ak všetky entity budú dôverovať vrcholu štruktúry PKI teda RCA.

Typickým príkladom vytvorenia politiky akceptácie certifikátov je oddelenie certifikátov pre zariadenia od certifikátov vydávaných osobám a certifikátov na zabezpečenie komunikácie. V takomto prípade môžeme vytvoriť politiku, ktorá bude definovať, aké certifikáty a kde sa budú akceptovať. Napríklad, ak by niekto náhodou získal certifikát a privátny kľúč zo zariadenia, tak pomocou týchto údajov sa nemôže maskovať ako používateľská entita.

Vo výsledku to môže uľahčiť monitorovanie bezpečnosti prevádzky a odhaľovanie chýb. Základnou metódou na definíciu bezpečnostnej politiky certifikátov je obmedzovanie buď dĺžky certifikačnej cesty, alebo akceptácia iba jednej, alebo viacerých vetiev X.500 mien. Napríklad ak používateľ má dn c=sk, o=asr, ou=pechota, cn=Jozef Pravda, potom môžeme vytvoriť politiku len na akceptáciu certifikátov, ktoré majú ou=pechota. V takomto prípade sa budú medzi sebou akceptovať len certifikáty, ktoré majú v ceste ou=pechota.

Vlastná podriadenosť certifikačnej autority nijako neobmedzuje jej činnosť prípadne koncové entity v rámci komunikácie v podstrome hierarchie certifikačných autorít. Na začiatku svojej činnosti CA vygeneruje požiadavku o certifikáciu svojho verejného kľúča nadradenej certifikačnej autorite. Certifikačná autorita potom pri podpisovaní certifikátov prikladá okrem svojho certifikátu aj certifikát nadradenej certifikačnej autority.

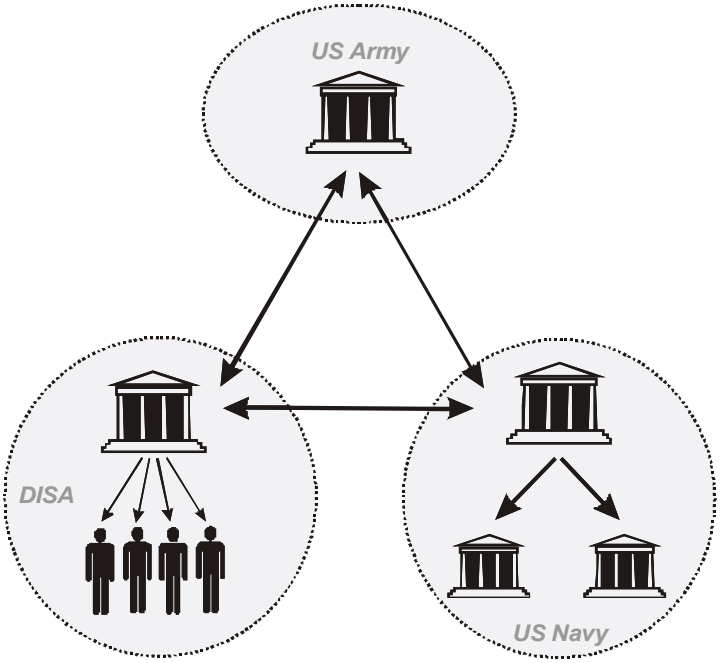


Obr. 13: Príklad podriadenosti certifikačných autorít

2.20.2 Krížová certifikácia

Krížová certifikácia slúži na vzájomnú akceptáciu certifikátov vydaných v dvoch doteraz nespojených organizáciách. Príkladom môže byť prepojenie časti informačného systému slovenského generálneho štábu so štábom NATO v Bruseli. Keďže obe organizácie majú vybudovanú vlastnú infraštruktúru PKI a rôznu architektúru hierarchie, nie je možné (žiadúce) aby ich zastrešovala jedna RCA. V takomto prípade je vhodné vykonať krížovú certifikáciu. Táto krížová certifikácia umožní vzájomnú komunikáciu a akceptáciu certifikátov vydaných v štruktúrach PKI jednej alebo druhej organizácie. Zároveň umožňuje definovať bezpečnostnú politiku využívania certifikátov hosťovskej organizácie v rámci domácej štruktúry. Obmedzenia využívania hosťovských certifikátov v domácej štruktúre definuje vždy domáca CA, ktorá vykonala krížovú certifikáciu.

Krížová certifikácia vytvára dôveru na princípe rovný s rovným. Hlavnou výhodou takejto certifikácie je možnosť spolupráce medzi organizáciami bez straty vlastnej autonómnosti a vzniku závislosti na certifikačnej autorite protistrany. Vzťah dôvery existuje podľa potrieb jednotlivých strán. Princíp dôvery nie je úplný a jednotlivé strany si definujú rozsah akceptácie certifikátov druhej strany. Typickým príkladom je akceptácie iba certifikátov vydaných pre zamestnancov určitého oddelenia. (c=us, o=army, ou=justice, ou=staff).



Obr. 14: Príklad krížovej certifikácie medzi organizáciami

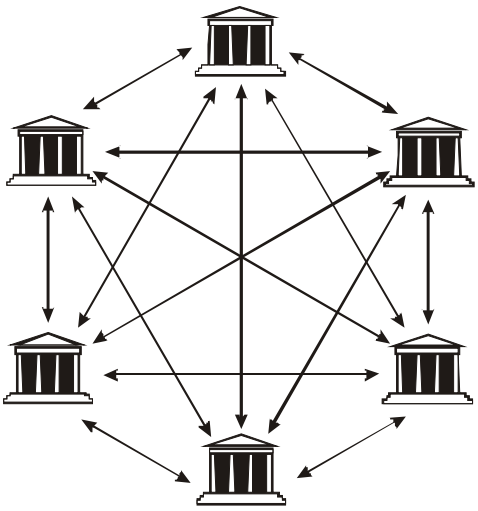
Priebeh krížového certifikovania je podobný ako priebeh certifikovania podriadenej CA s tým rozdielom, že obe autority certifikujú protistranu. Obe strany vygenerujú požiadavku o vykonanie certifikácie „podriadenej“ autority do „nadradenej“. Vďaka tomuto a definícii bezpečnostnej politiky môžu obe strany navzájom komunikovať.

Politika akceptácie certifikátov je obdobná ako pri definícii politiky podriadených CA. V takomto prípade sa ale doporučuje obmedziť okrem DN aj dĺžku certifikačnej cesty tak, aby sa netvorili nekontrolované cesty výmeny certifikátov. Na obrázku č. 13 sú zobrazené 3 organizácie. V prípade že používateľ z US Navy chce overiť certifikát vydaný v DISA, má možnosť certifikačnej cesty US Navy > DISA alebo US Navy >> US Army >> DISA. Obe cestu sú správne a môže dôjsť k overeniu, ale líšia sa dĺžkou. Práve z tohto dôvodu sa obmedzuje certifikačná cesta.

2.20.3 Premostenie

V prípade prepojenia viacerých organizácií a krížového certifikovania sa ich certifikačných autorít, vzniká podobný problém ako pri symetrickej kryptografii z komunikačnými kľúčmi. Počet nutných krížových certifikácií rastie podľa vzťahu $(n^2-n)/2$ a počet nutných certifikátov je

n^2-n. Pri takomto množstve nutných vykonaných certifikácií môže dôjsť ľahko ku chybe a opomenutiu niekoho certifikovať. Okrem toho, v prípade rozšírenia participujúcich CA, je nutný zásah na všetkých CA, aby bola akceptovaná nová CA. Ak by náhodou došlo ku zneplatneniu certifikátu jednej zo zúčastnených CA, šírenie tejto informácie je vďaka komplexnosti vzťahov problematické.



Obr. 15: Príklad nutnej krížovej certifikácie 6. certifikačných autorít

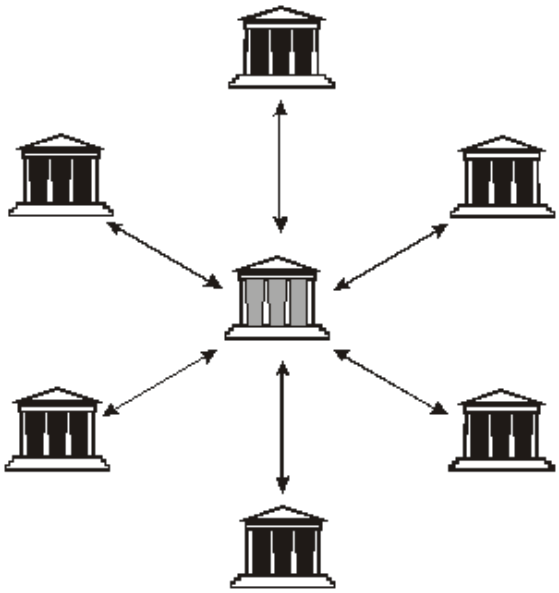
Riešením pre akceptáciu certifikátov väčšieho množstva organizácii v rámci rovnocenného vzťahu je vytvorenie premosťovacej certifikačnej autority, ktorá slúži na krížovú certifikáciu. Každá zo zúčastnených strán sa nebude krížovo certifikovať s ostatnými, ale len s premosťovacou CA. V takomto prípade vzniká jednoduchšia štruktúra, ktorá je ľahšie manažovateľná.

Premosťovacia CA definuje globálnu bezpečnostnú politiku akceptácie certifikátov medzi organizáciami a jednotlivé organizácie vzhľadom na jednoduché pripojenie k ostatným ľahko definujú svoju vlastnú bezpečnostnú politiky akceptácie certifikátov. V prípade, že by došlo k zneplatneniu certifikátu jednej z participujúcich CA, stačí ak tento fakt bude zverejnený na ARL vydaným premosťovacou CA.

Požiadavky na premosťovaciu CA sú obdobné požiadavkám kladeným na RCA. Je vhodné, aby premosťovacia CA bola tiež off-line, prípadne aby pomocou on-line RA poskytovala službu OCSP a publikáciu ARL.

Premosťovacia CA okrem iného môže poskytovať možnosť konverzie pri overovaní certifikátov v prípade, keď jednotlivé organizácie používajú rôzne algoritmy na podpisovanie. Napr. RSA-MD5 na DSA-SHA1 a pod.

Využívanie premosťovacej CA nevytvára prirodzenú hierarchiu. Krížová certifikácia, ktorá sa používa pri premosťovacej CA, je relácia rovný-s-rovným a nie podriadenej a nadriadenej



Obr. 16: Zjednodušenie architektúry pri použití premosťovacej CA

CA. Zneplatnením certifikátu premosťovacej CA nedochádza ku strate dôvery v rámci štruktúr, ktoré spája. Dochádza iba ku strate vzájomnej dôvery medzi týmito štruktúrami.

2.21 Životnosť zreťazených certifikátov

Vzhľadom na väzby medzi certifikátmi v CC je nutné zabezpečiť, aby životnosť jednotlivých certifikátov bola adekvátna k ich používaniu a pozícii v hierarchii pri architektúre RCA a aby certifikát nemal dlhšiu platnosť ako nadradený certifikát. Je nevhodným stavom, aby certifikát CA vypršal skôr ako certifikát koncovej entity, pretože v prípade exspirácie certifikátu CA môže dôjsť k zastaveniu činnosti entity.

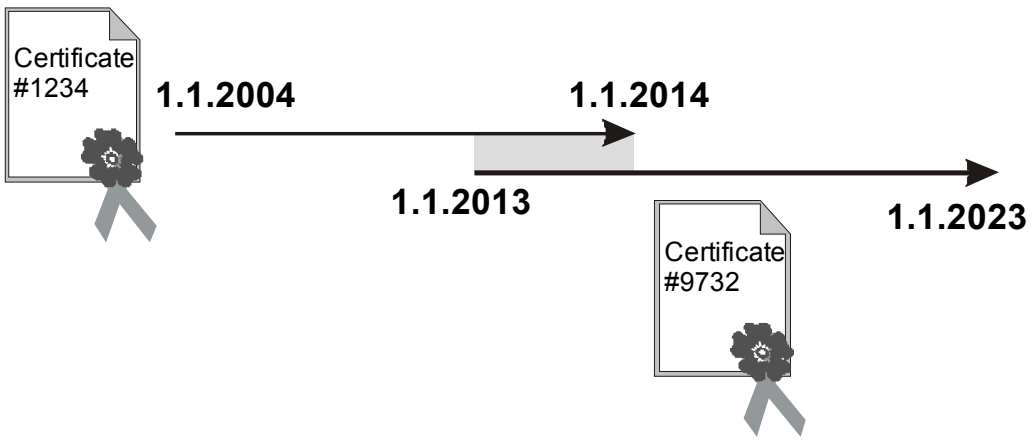
Odporúčané životnosti certifikátov sa preto v praxi odvádzajú od množstva ich využívania pri podpisovaní a šifrovaní. Každým ďalším šifrovaním údajov poskytujeme možnosť prípadnému útočníkovi vykonať kryptoanalýzu dát a tak získať privátny kľúč alebo získať

chránené údaje. Práve z toho dôvodu sa aj v certifikátoch uvádzajú dva kľúče – jeden pre šifrovanie a druhý pre podpisovanie. Okrem toho môže byť dôvodom na existenciu dvoch kľúčových párov, zvlášť na šifrovanie a zvlášť na podpisovanie, aj nutnosť zálohovania šifrovacích kľúčových párov v CA.

Ďalším kritériom pre životnosť certifikátu je relevantnosť v ňom uvedených údajov. Ak budú certifikáty kopírovať organizačnú štruktúru, potom používanie osobných certifikátov obsahuje relevantné údaje o pozícii entity. V prípade, že dôjde ku zmene zaradenia, bude nutné zneplatňovať pôvodný certifikát koncovej entity a vydať nový certifikát. Ak je náhodou táto zmena len dočasná, je potom opäť nutné vydať nový certifikát a zneplatniť predchádzajúci.

Tento postup zbytočne predlžuje kontrolu overovania platnosti certifikátu, nakoľko zoznam CRL bude veľmi dlhý (certifikát musí byť na CRL uvedený do doby, kým neexspiruje) a tak isto zaťažuje prenosové média.

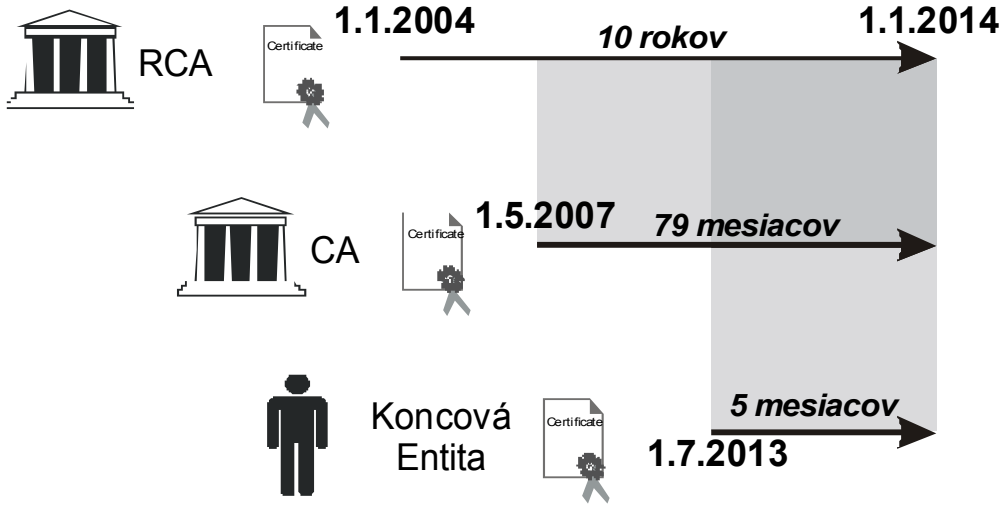
Okrem plánovanej životnosti je pre kontinuálnu prevádzku nutné naplánovať aj čas obnovy certifikátu, aby nedošlo prerušeniu činnosti z dôvodu exspirácie certifikátu. Tento proces zabezpečí kontinuálnu existenciu certifikátu. V istom časovom úseku budú pre entitu existovať dva rovnaké certifikáty, ale každý s inou exspiračnou dobou.



Obr. 17: Príklad prekrytia platnosti nadväzujúceho certifikátu entity

Na obrázku č. 18 je znázornené, ako treba nastavovať životnosť certifikátov vznikajúcich v čase s ohľadom na už existujúce CA v hierarchii a zostávajúcu životnosť ich certifikátov, aby platnosť vydaného certifikátu nekončila neskôr ako platnosť certifikátu vydavateľa. Na obrázku

č. 19 je spôsob, ako zabezpečiť kontinualitu vydávania certifikátov s využitím časového prekryvu certifikátov CA. V tomto prípade by bol koncovej entite z obrázku č. 18 vydaný certifikát na normálne obdobie 2 roky, ale na podpisovanie by sa použil nový certifikát CA.



Obr. 18: Príklad definície životnosti certifikátu vzhľadom na nadradenú CA

Kategória	Odporúčaná min. exspiračná doba	Odporúčaná max. exspiračná doba
Koreňová certifikačná autorita	20 rokov	50 rokov
Podriadená CA I. úrovne	10 rokov	15 rokov
Podriadená CA II. úrovne	5 rokov	10 rokov
CA spolupracujúcej organizácie krížový certifikát	Doba existencie kontraktu max. 10 rokov	
Osobný certifikát	1 rok	Doba kontraktu/3 roky
Autentifikačný certifikát zariadenia	1 rok	2 roky
Certifikát zariadenia na šifrovanie	6 mesiacov	1 rok
Dočasný osobný certifikát	Presne stanovená doba prístupu	

Tabuľka 1: Odporúčané životnosti certifikátov pre jednotlivé entity v hierarchii RCA

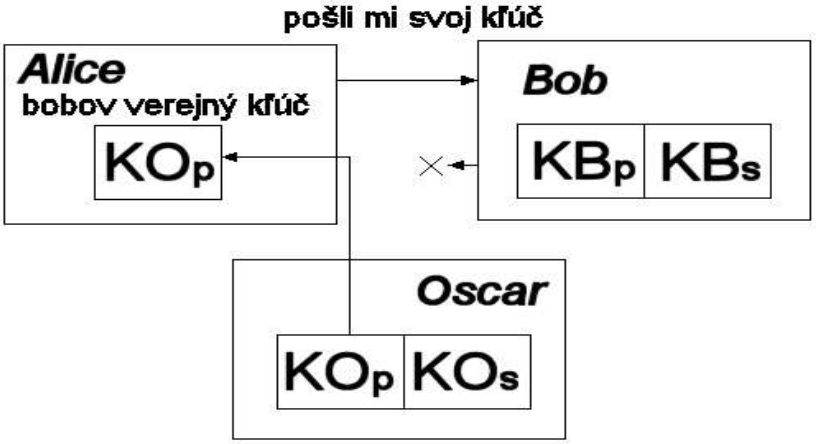
Dĺžka platnosti certifikátov by mala zahŕňať fakty, ktoré majú vplyv na možnú kompromitáciu privátneho kľúča, ako aj nutnú existenciu certifikátu.

2.22 Manažment kľúčov

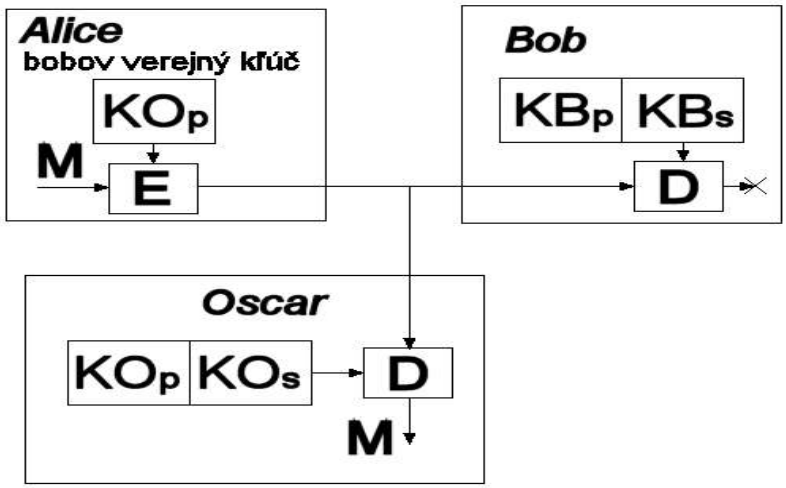
Sila každej šifry je v hlavnej miere založená na správnom zaobchádzaní s kľúčovým materiálom. Pri symetrických šifrách musí byť kľúč držaný v tajnosti, pretože kto vlastní kľúč, môže dešifrovať správu. Pri asymetrických šifrách je privátny (tajný) kľúč najcitlivejšou časťou systému. Vytváraním, spravovaním, metódami používania a transportu kľúčového materiálu sa zaoberá manažment kľúčov.

2.22.1 Získavanie kľúčov

Ako už bolo spomenuté, uloženie tajných kľúčov je nesmierne dôležité pre bezpečnosť kryptosystému. Avšak ani verejné kľúče, aj keď sú verejné, nemôžu byť šírené sami o sebe. Predstavme si nasledujúci modelový prípad (Obr. 19).



Obr. 19: Zámena kľúcov I.

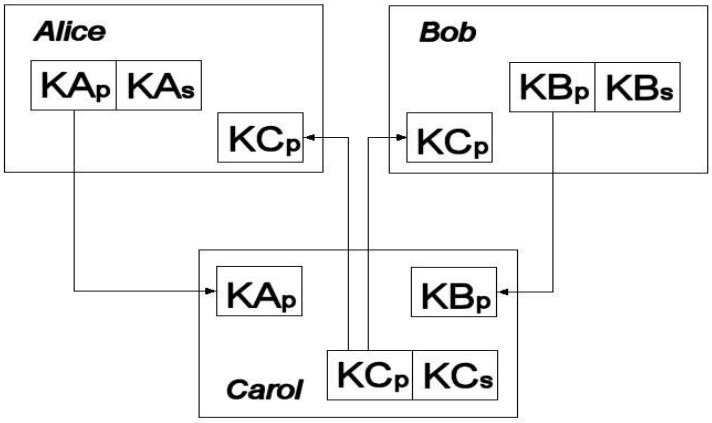


Obr. 20: Zámena kľúčov II.

Alice chce komunikovať s Bobom, a tak si vyžiada Bobov verejný kľúč. Bob odošle svoj verejný kľúč Alici. Oscar zachytí Bobovu správu s jeho verejným kľúčom, a namiesto Bobovho kľúča pošle Alici svoj verejný kľúč. Správa inak zostane pôvodná. Alica dostane správu, ktorá vyzerá že prišla od Boba a obsahuje „Bobov“ verejný kľúč (v skutočnosti je Oscarov kľúč). Alice teda tento kľúč použije na zašifrovanie správy M (Obr. 20) a správu odošle Bobovi. Toto vysielanie zachytí aj Oscar. Keďže Oscar vlastní súkromný kľúč, ktorý patrí k verejnému kľúču použitému na zašifrovanie správy, môže správu prečítať.

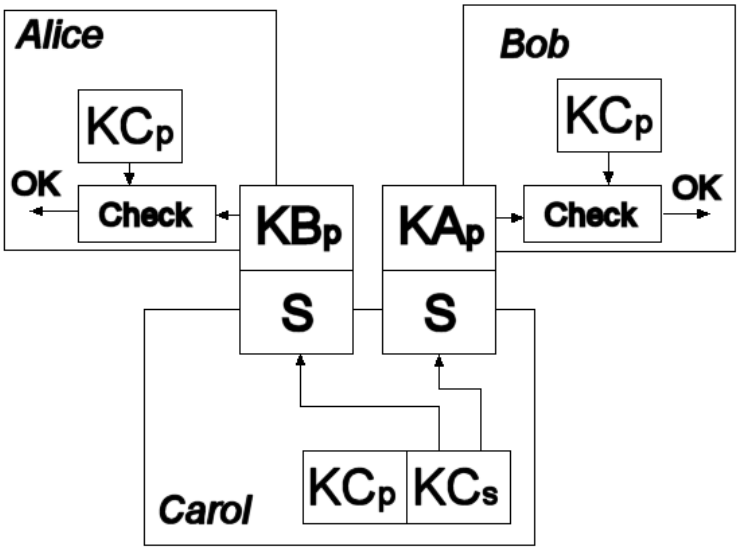
Tento útok je založený na zámene verejných kľúčov. Odvrátenie tohto útoku klasickými metódami by vyžadovalo dodatočný bezpečný kanál medzi Alicou a Bobom, napríklad by si museli skontrolovať správnosť kľúčov cez telefón alebo osobným stretnutím. Takéto overovanie je však veľmi nepraktické, pretože komunikujúce strany sa vôbec nemusia navzájom osobne poznať. Navyše ak vezmeme do úvahy veľké množstvo komunikujúcich strán, musí prebehnúť overovanie medzi každou komunikujúcou dvojicou nezávisle.

Predchádzajúci problém zámeny kľúčov možno riešiť pomocou sprostredkovateľa. Sprostredkovateľ je subjekt, ktorému obe komunikujúce strany veria (dôveryhodná tretia strana). Predstavme si, že Alice a Bob sa osobne nepoznajú, ale majú spoločného priateľa, Carol. Carol pozná osobne Boba aj Alicu, osobne sa s nimi stretla a vlastní ich overené verejné kľúče. Rovnako Bob aj Alica vlastnia osobne overený verejný kľúč Carol (Obr. 21).



Obr. 21: Sprostredkovateľ - počiatočná výmena kľúčov

Teraz môže Carol „digitálne zoznámiť“ Boba a Alice tak, že Bobovi pošle podpísanú správu obsahujúcu verejný kľúč Alice a naopak Alici pošle podpísaný Bobov kľúč (Obr. 22).



Obr. 22: Sprostredkovateľ - distribúcia kľúčov

Alica aj Bob si môžu spoľahlivo overiť Carolin podpis (S), keďže vlastnia jej verejný kľúč (KCp). Takýmto spôsobom sa k Alici dostane overený verejný kľúč Boba, a k Bobovi overený verejný kľúč Alice. Alica a Bob môže odteraz spolu bezpečne komunikovať bez toho aby sa museli osobne stretnúť.

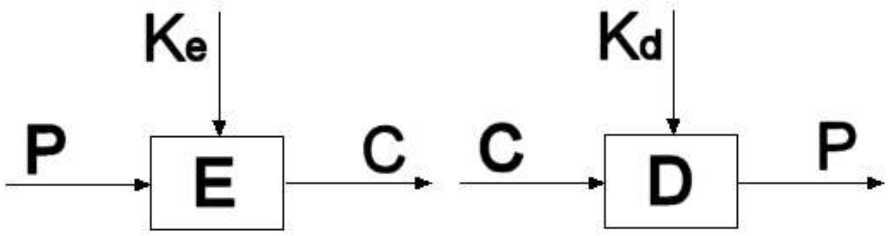
2.23 Základy kryptografie

Kryptografia už od čias staroveku slúžila na ochranu citlivých informácií. Najväčší rozvoj však dosiahla až s nástupom počítačovej techniky. Výkonné výpočtové systémy umožnili realizovať nesmierne zložité algoritmy a kryptografia sa stáva samostatným vedným odborom.

Na pochopenie činnosti certifikačných autorít je nutné pochopiť aspoň základné princípy použitia kryptografických technológií. Niektoré z týchto princípov si v skratke priblížime v nasledujúcich odstavcoch.

Šifra, ako ju poznáme z klasickej kryptografie, pozostáva z šifrovacieho a dešifrovacieho algoritmu. Šifrovací algoritmus transformuje správu vo forme otvoreného textu (P) na zašifrovanú správu (C). Na túto transformáciu je použitý šifrovací kľúč (Ke). Dešifrovací algoritmus naopak transformuje šifrovanú správu (C) na správu v otvorenom tvare (P) pomocou dešifrovacieho kľúča (Kd). Schematicky je šifra zobrazené na obrázku Obr. 23.

Správa v šifrovanom tvare (C) je čitateľná len pre toho, kto vlastní dešifrovací kľúč (Kd). Šifrovací aj dešifrovací algoritmus sú v o väčšine prípadov verejne k dispozícii a jediná tajná informácia sú použité kľúče.



Obr. 23: Šifra

2.23.1 Symetrické šifrovanie

Klasické historické šifry a aj mnoho súčasných šifier používa rovnaký kľúč na šifrovanie aj dešifrovanie (Ke = Kd). Kľúč v tomto prípade predstavuje zdieľané tajomstvo medzi komunikujúcimi stranami. Ktokoľvek, kto vlastní kľúč, je schopný správu prečítať. Tieto šifry sa nazývajú symetrické alebo šifry s tajným kľúčom, keďže kľúč predstavuje zdieľané tajomstvo a na jeho utajení je založená bezpečnosť celej šifry. Väčšinou je nutné pred začatím komunikácie dohodnúť spoločný kľúč pomocou bezpečného kanálu. Medzi súčasných zástupcov

symetrických šifier patria dobre známe šifry DES, RC4, IDEA, BLOWFISH a iné.

Symetrické šifrovacie algoritmy sú také, kde dešifrovací a šifrovací kľúč sú rovnaké, resp. zo seba ľahko odvoditeľné. Symetrické šifrovacie algoritmy sú spravidla rýchlejšie, no problémom je prenos kľúča od autora k adresátovi. Je to postup, ktorým jednoznačne zašifrujeme pomocou kľúča K zvolenú správu M na zašifrovaný text C za podmienky, že pri šifrovaní musíme poznať použitý kľúč. Proces šifrovania môžeme vyjadriť ako:

$$E(M,K) = C$$

Proces dešifrovania môžeme vyjadriť:

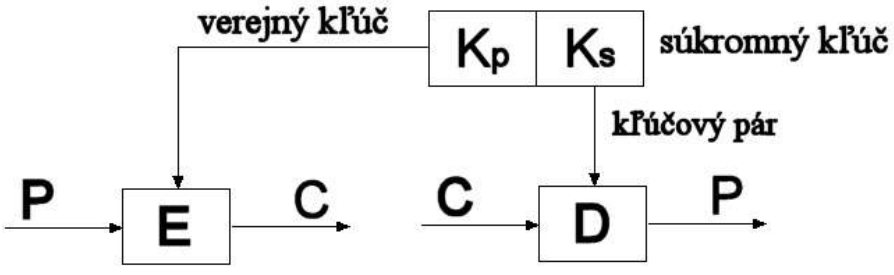
$$D(C,K) = M$$

Pričom E a D je u väčšiny symetrických algoritmov rovnaká funkcia, takže sa používa rovnaký postup na šifrovania aj dešifrovanie.

2.23.2 Asymetrické šifrovanie

Na druhej strane pri asymetrických šifrách je šifrovací a dešifrovací kľúč rozdielny (Ke Kd). Šifrovací kľúč sa nazýva verejný kľúč a dešifrovací kľúč sa nazýva súkromný kľúč. Pri asymetrických šifrách je zaujímavý fakt, že ten kto správu zašifruje, už ju ani sám nevie prečítať. Šifrovanie je jednosmerná operácia. Na prečítanie zašifrovanej správy je potrebný súkromný kľúč. Verejný kľúč je teda možné voľne šíriť, a ktokoľvek bude potrebovať poslať správu, môže ním správu zašifrovať. Nikto iný okrem majiteľa súkromného kľúča však správu neprečíta.

Súkromný a verejný kľúč sú na sebe matematicky závislé. Pri tom však platí, že pomocou verejného kľúča nie je možné zistiť súkromný kľúč. Verejný a súkromný kľúč, ktoré patria k sebe sa nazývajú kľúčový pár. Základné použitie asymetrickej šifry ilustruje obrázok č. 24.



Obr. 24: Asymetrická šifra

Asymetrické šifry odbúravajú nutnosť udržovať spoločné tajomstvo, keďže verejný kľúč nemusí byť držaný v tajnosti a nie je potrebný bezpečný kanál na výmenu kľúčov. Medzi najznámejšie súčasné šifry s verejným kľúčom patria RSA, Diffie-Hellman, ElGamal a iné.

Asymetrické šifrovacie algoritmy sú také, kde sa dešifrovací a šifrovací kľúč líšia a je ťažké, t.j. prakticky nemožné, ich zo seba vypočítať. Asymetrické algoritmy sa zakladajú na princípe verejných a privátnych (tajných) kľúčov - verejný kľúč každého účastníka komunikácie je známy a používa sa na šifrovanie správ jemu adresovaných. Na ich dešifrovanie potom použije svoj privátny kľúč. Tým sa zabezpečí, že ak autor pozná verejný kľúč adresáta, môže mu poslať správu, ktorú nikto iný nedokáže v rozumnom čase za rozumnú cenu prečítať. Asymetrické šifrovanie, je v podstate séria postupov, pri ktorých jednoznačne premeníme text T1 na text T2 pomocou kľúča Kn. Skladá sa z dvoch častí – prvá časť premení text M na text C pričom použije kľúč K1 (označovaný oko verejný kľúč). Druhá časť premení text C na text M, pričom použije kľúč K2 (označovaný ako privátny kľúč). V zásade platí, že z K1 sa žiadnym matematickým postupom nedá získať K2. K1 je kľúč, ktorý je volne k dispozícii komukoľvek, zatiaľ čo K2 vlastní človek, ktorému je správa určená. Text M zašifrovaný pomocou kľúča K1 sa dá dešifrovať len pomocou kľúča K2 (z toho vyplýva, že text C na text M nemôže dešifrovať ani ten, kto ho zašifroval, pretože nemá privátny kľúč K2). Proces môžeme jednoducho znázorniť:

$$E(M, K1) = C$$

$$D(C, K2) = M$$

$$K2 \neq f(K1)$$

Nevýhodou asymetrických šifrovacích algoritmov je, že sú často pomalé. Preto sa používajú skôr na výmenu kľúčov pre symetrické algoritmy, ktoré sa následne použijú na šifrovanie samotnej správy. Takéto šifrovacie systémy sa nazývajú hybridné. Problémom ostáva spoľahlivá identifikácia autora. Tento problém riešia digitálne podpisy.

Bezpečnosť algoritmu (t.j. za aký čas je možné prelomiť algoritmus a dostať sa k pôvodnej správe bez znalosti druhého kľúča) jednoznačne závisí od dĺžky kľúča. Dĺžky kľúčov sa pohybujú od 512 do 2048 bitov, pričom 1024 bitový kľúč je dnes považovaný za neprelomiteľný v reálnom čase pri využití súčasných výkonov počítačov. Ako sa postupne zvyšuje výkon, bude sa postupne zvyšovať aj dĺžka kľúčov.

2.23.2.1 Digitálny podpis

Digitálne podpisy sú metódou umožňujúcou spoľahlivo identifikovať autora dokumentu. Sú analógiou vlastnoručných podpisov pri klasickej komunikácii. Zakladajú sa najčastejšie, podobne ako asymetrické šifrovacie algoritmy, na verejných a privátnych kľúčoch. Keď sa k dokumentu pripojí digitálny podpis, ktokoľvek, kto pozná verejný kľúč autora, si môže ľahko overiť, že dokument nebol po podpísaní modifikovaný a podpísal ho niekto, kto pozná tajný kľúč autora.

2.23.2.2 Problém digitálneho podpisu

Digitálne podpisy poskytujú dostatočnú ochranu komunikácie medzi vlastníkmi príslušných kľúčov. Neriešia však sami problém väzby verejného kľúča na konkrétnu osobu alebo iný objekt. Pokiaľ adresát správy nemá možnosť spoľahlivo zistiť verejný kľúč autora, tak vlastne nemôže overiť, že správu naozaj poslal ten, kto sa vydáva za autora. Teda je potrebné mať nejaký dôveryhodný zdroj verejných kľúčov a spoľahlivú metódu prístupu k nemu.

2.23.3 Šifrovacie Algoritmy a indentifikátory používané v x.509

V tejto časti sú popísané jednosmerné hashovacie funkcie a algoritmy pre digitálny podpis používané pre podpísanie certifikátov a CRL. Tiež slúžia na identifikáciu identifikátorov objektov (OID) pre verejný kľúč uchovávané v certifikátoch.

Jednosmerné hashovacie funkcie sú tiež nazývané message digest algoritmy. Využitie sa dá ľahko ukázať na nasledovnej modelovej situácii. Chceme poslať zašifrovanú správu, aby jej obsah bol dostupný pre čítanie, len konkrétnemu doručiteľovi. To ale nezaručuje, že po ceste by niekto mohol obsah správy modifikovať a príjemcovi prišla správa modifikovaná, čo znamená veľké riziko. Práve pre tento prípad sa používa špeciálna kontrolný sumarizačný kód správy, ktorý je doručený príjemcovi spolu s originálnou správou. Príjemca si znovu spraví sumarizáciu správy a porovná prijatý kód s kódom ktorý si vygeneroval z prijatej správy. V prípade, že kódy sú totožné, znamená to, že správa nebola modifikovaná a jej obsah je rovnaký ako ho poslal odosielateľ. Ak kódy nie sú totožné je správa buď poškodená, alebo modifikovaná. Takáto sumarizácia sa nazýva Message Digest (MD) alebo hashovacia funkcia. MD vytvára krátku reprezentáciu s rovnakou dĺžkou, zo správ s rôznymi dĺžkami. MD algoritmus bol navrhnutý tak, aby generoval unikátnu sumarizačnú značku pre rozdielne správy. Algoritmus je navrhnutý tak,

aby sa z neho spätne nedalo získať správu z ktorej bol vytvorený. Rovnako je ťažké nájsť dve rôzne správy, z ktorých by bola vygenerovaná rovnaká sumarizácia- aj keď je to teoreticky možné. SHA-1 je preferovanou jednosmernou hashovacou funkciou pre Internet X.509 PKI. Privacy-Enhanced Mail (PEM) používa MD2 pre certifikáty a MD5 sa používa v ďalších „dedičných“ aplikáciách.

2.23.3.1 MD2

MD2 vynašiel Ron Rivest pre firmu RSA Security. Neskôr RSA Security sprístupnila MD2 algoritmus širokej verejnosti. Predtým RSA Data Security uvolnila licenciu pre používanie MD2 v nekomerčných internetových PEM. Aj keď dodnes sa MD2 používa v PEM certifikátoch, uprednostňovaný je SHA-1 algoritmus. MD2 vykonáva 128bitový hash vstupných údajov.

Na konferencii Selected Areas in Cryptography '95 z mája 1995 Rogier a Chauvaud prezentovali útok na MD2. Zistilo sa, že keď sa podarí nájsť dve rozdielne správy, ktoré generujú rovnaký MD vzniká kolízia. V tomto prípade je checksum jediná zostávajúca ochrana pred zneužitím, prípadne útokom. Z tohto dôvodu novšie aplikácia zabraňujú použitie MD2. Stále je tu ale dôvod pre používanie MD2 na overovanie existujúcich podpisov. Aj keď je tu možnosť kolízie, útočníkovi má zníženú možnosť zneužitia, pretože nové správy nemôžu mať generovaný hash skôr, ako vzniknú.

2.23.3.2 MD5

MD5 vynašiel Ron Rivest pre firmu RSA Security. Neskôr RSA Security sprístupnila MD5 algoritmus širokej verejnosti. MD5 vykonáva 128bitový hash vstupných údajov.

MD5 algoritmus bol navrhnutý pre výkonné 32bitové stroje. Navyše, MD5 algoritmus nevyžaduje žiadne veľké substitučné tabuľky, je naprogramovaný veľmi kompaktne. Je to vlastne rozšírenie MD4 algoritmu. Aj keď je trochu pomalší ako MD4 využíva niektoré konzervatívne prvky vo svojej konštrukcii. Napriek svojej pomalosti MD5 poskytuje zvýšenú bezpečnosť, pretože na rozdiel od MD4, ktorý bol navrhnutý predovšetkým kvôli rýchlosti, u MD5 je dôraz kladený na bezpečnosť. Zahŕňa mnohé zlepšenia, dopracované recenzentmi a je značne optimalizovaný.

Den Boer a Bosselaers našli pseudo kolíziu pre MD5 avšak neprinieslo to žiadne ďalšie kryptoanalytické závery. Niektoré novšie aplikácia zabraňujú použitie MD5. Stále je tu ale

dôvod pre používanie MD5 na overovanie existujúcich podpisov.

2.23.3.3 SHA-1

Tento algoritmus bol vynájdený vládou Spojených štátov. SHA-1 produkuje 160bitový hash zo vstupnej informácie. Vychádza z rovnakých základov a princípov, ktoré použil profesor Ronald L. Rivest z univerzity MIT keď navrhoval MD4 algoritmus. SHA-1 je nazývaný bezpečným, pretože je doposiaľ známymi výpočtovými metódami neuskutočniteľné nájsť správu, ktorá zodpovedá hashovanej správe, alebo nájsť dve rozdielne správy ktoré by generovali rovnaký hash. Akékoľvek zmeny ktoré sa uskutočnia na správe počas prenosu, budú s vysokou pravdepodobnosťou mať za následok rozdielny hash, a tým bude podpis po verifikácii vyhlásený za neplatný.

2.23.4 Algoritmy používané na podpisovanie

Máme zabezpečenú správu proti modifikácii, no je tu ďalšie riziko, ktoré môže viesť k bezpečnostnému incidentu. Ako zaručiť, že prijatá správa je naozaj od deklarovaného odosielateľa. Tento problém rieši digitálny podpis, ktorý je pribalený ku správe. Digitálny podpis je tvorený z kódovaného obsahu správy a ďalších informácií (napríklad poradového čísla správy) pomocou prívátneho kľúča odosielateľa.

Certifikáty alebo CRL môžu byť podpísané ktorýmkoľvek podpisovacím algoritmom pre verejné kľúče. V certifikáte alebo v CRL je identifikátor OID, ktorý určuje, aký algoritmus bol použitý. Zvyčajne sú tam ešte ďalšie upresňujúce parametre.

Podpisovacie algoritmy sa vždy používajú v konjunkcii s jednosmernými hash algoritmami. Dáta ktoré chceme podpísať (napríklad výstup z nejakého jednosmerného hash algoritmu) sa naformátujú na požadovaný tvar pre konkrétny podpisovací algoritmus, ktorý chceme použiť. Potom sa použije proces privátneho kľúča (napríklad RSA enkrypcia) na vytvorenie podpisu. Táto časť je potom zakódovaná ako ASN.1 bit string a vložená do certifikátu, alebo listu certifikátov v poli pre podpis.

2.23.4.1 RSA

Pomenovanie zdedil po svojich tvorcoch Rivest, Shamir a Adleman. Zaujímavosťou je, že patent na tento algoritmus skončil rokom 2000. Ron Rives a Adi Shamir sa dodnes aktívne venujú kryptografii a sú považovaní za významné osobnosti v oblasti šifrovania.

Najzložitejšou časťou algoritmu je práve generovanie kľúča. Jedná sa o pomerne komplikovaný proces, tak sa ho pokúsim popísať čo najjednoduchšie. Na začiatku je potrebné zvoliť náhodné veľmi veľké prvočísla. Tieto prvočísla (označme ich p a q) by mali byť zvolené rádovo rovnako veľké.

Vypočíta sa ich súčin:

$$n = pq$$

Potom sa náhodne zvolí číslo e (časť šifrovacieho kľúča) tak, aby čísla e a (p-1)(q-1) boli nesúdeliteľné. Nakoniec sa pomocou rozšíreného Euclidovho algoritmu vypočíta číslo d (časť dešifrovacieho kľúča), tak aby platilo:

$$d = e - 1 \ mod((p-1)(q-1))$$

Čísla d a e musia byť tiež nesúdeliteľné.

Algoritmus RSA je bezpečný pri veľkých dĺžkach kľúča. Jeho bezpečnosť založená na tom, že je časovo náročné rozložiť obrovské číslo na prvočinitele. Ak by sa nám podarilo rozložiť číslo n na p a q, mohli by sme dostať z e číslo d. Tento dohad nebol dôkladne podložený, pretože sa matematiky nedokázalo, že k odvodeniu m z c je potrebné urobiť rozklad čísla n. Kryptoanalýza RSA sa môže prevádzkovať aj hľadaním hodnoty (p-1)(q-1). Tento spôsob nie je o nič ľahší ako hľadanie rozkladu n. Pokiaľ máme k dispozícii dostatočne veľké množstvá množín {m,c} je tu možnosť diferenčnej kryptoanalýzy. Z praktického hľadiska môžeme bezpečnostné faktory zhrnúť do niekoľkých bodov, ktoré spôsobia, že používanie RSA bude bezpečnejšie.

Používať dobrý (nepredvídateľný) generátor

Voliť dostatočne veľké p a q, uistiť sa, že sú to naozaj prvočísla

Po vygenerovaní kľúčov treba p a q odstrániť a zaistiť, aby nezostali nikde uložené

Zabezpečiť, aby číslo d zostalo utajené

2.23.4.2 DSA

Digital Signature Algorithm je definovaný v DSS (Digital Signature Standard). Bol vynájdený vládou Spojených štátov a používa sa v konjunkcii s SHA-1 jednosmerným hash algoritmom. Keď sa vytvára podpis, DSA algoritmus vygeneruje dve hodnoty r a s. Aby sa z týchto dvoch hodnôt stal jeden podpis sú zakódované cez ASN.1 s použitím tejto štruktúry:

```
Dss-Sig-Value  ::=  SEQUENCE  {
     r       INTEGER,
     s       INTEGER
 }
```

2.23.4.3 ECDSA

Elliptic Curve Digital Signature Algorithm sa používa spolu s SHA-1 jednosmerným hash algoritmom. V poli ubjectPublicKeyInfo sú zaznamenané eclliptic curve parametre ktoré sa používajú na verifikáciu podpisu. Pri podpisovaní, ECDSA algoritmus vygeneruje dve hodnoty zvyčajne označované r a s. Na transformovanie týchto dvoch hodnôt na jeden podpis sa podobne ako pri DSA použije ASN.1 kódovanie pomocou nasledujúcej štruktúry:

```
Ecdsa-Sig-Value  ::=  SEQUENCE  {
        r     INTEGER,
        s     INTEGER  }
```

2.23.5 Algoritmy používané pre verejný kľúč

Certifikáty spĺňajúce RFC 3280 prenášať verejný kľúč pre akýkoľvek algoritmus verejného kľúča. Certifikát indikuje použitý algoritmus pomocou identifikátora algoritmu. V zásade sa používajú RSA, DSA, Diffie-Hellman, KEA, ECDSA a ECDH algoritmy.

Základné funkcie PKI (Public Key Infrastructure)

V tejto časti sú definované základné postupy pre bezpečnú komunikáciu s využitím služieb certifikačnej autority.

2.23.5.1 Vytvorenie kľúčového páru a žiadosť o certifikát

Používateľ si musí vytvoriť verejný a privátny kľúč pomocou používaných algoritmov (napr. RSA). Potom je potrebné vytvoriť žiadosť o certifikát, čo je samotný certifikát, ale zatiaľ nepodpísaný certifikačnou autoritou. Certifikát obsahuje informácie o užívateľovi, ako je jeho meno, adresa, telefónne číslo a emailová adresa. Taktiež obsahuje verejný kľúč používateľa.

Pokiaľ sa nejedná o certifikát pre konkrétnu osobu, ale pre nejakú inú všeobecnú entitu, napríklad www server, mailový server alebo iné sieťové zariadenie, do informácií v certifikáte sa uvádza URL servera, kontakt na administrátora a pod.

2.23.5.2 Podpísanie žiadosti o certifikát Certifikačnou Autoritou

Vytvorenú žiadosť je potrebné doručiť Registračnej Autorite (RA) aby zabezpečila jej podpísanie. To či je žiadosť prijatá, alebo zamietnutá je riešené práve v Registračnej Autorite. V prípade schválenia, RA postúpi žiadosť Certifikačnej Autorite podľa schvaľovacej politiky a aby mohla byť žiadosť podpísaná. Výsledkom je samotný Certifikát, ktorý je doručený naspäť žiadateľovi pomocou Registračnej Autority. Zároveň je certifikát evidovaný a uložený na servery Certifikačnej Autority.

3 EP prakticky

Čo je potrebné k praktickému použitiu elektronického podpisu?

K praktickému použitiu elektronického podpisu je potrebné PC pripojené do siete Internet s aplikáciami MS Explorer a MS Outlook alebo podobnými, znalosti o ich používaní a základné znalosti o elektronickom podpise.

K použitiu zaručeného elektronického podpisu, t. j. podpisu ktorý podľa zákona o elektronickom podpise môže byť použitý v administratívnom styku so štátnou správou musí byť v prvom rade zabezpečená podmienka „podpisuj to čo vidíš“.

K tomu je potrebná úradom certifikovaná aplikácia (obdoba MS Outlook), ktorá umožňuje podpísanie dokumentu a aj overenie podpisu a úradom certifikované bezpečné zariadenie na vyhotovovanie elektronického podpisu.

Bezpečným zariadením môže byť napríklad certifikovaná kryptografická karta (obdoba platobnej karty) so zariadením, ktoré umožňuje komunikovať počítaču s touto kartou, tzv. čítačka kariet alebo USB token.

V takomto prípade bezpečné zariadenie pre vyhotovovanie elektronického podpisu plní aj funkciu bezpečného uchovávania tajného kľúča majiteľa.

Ďalšou dôležitou podmienkou je vystavenie kvalifikovaného certifikátu konkrétnej osobe, túto úlohu by mala zabezpečovať akreditovaná CA NBÚ alebo úradom akreditovaná CA.

Samotný proces elektronického podpisovania dokumentu je pre podpisovateľa obmedzený len na zasunutie kryptografickej karty do čítačky, zadanie PIN kódu a v aplikácií určenej na podpisovanie „odkliknutie“, že uvedený dokument sa má podpísať, takto upravený, podpísaný dokument je potom možné distribuovať.

Na strane overovateľa prebieha overenie podobným spôsobom, nie je potrebné vkladať kryptografickú kartu a zadávať PIN kód, stačí len v príslušnej aplikácií kliknúť na voľbu overiť elektronický podpis.

Bezpečné aplikácie by však aj pri overovaní ZEP mali vyžadovať vloženie tokenu, pretože certifikát ACA alebo NBÚ by sa mal načítať z tohto tokenu, čiže z bezpečného úložiska, kde nie je možné jednoduchým spôsobom tieto certifikáty zameniť za falošné.

Po overení sa na monitore objaví správa o úspešnom overení alebo správa o nemožnosti overenie a ak je to možné tak aj príslušný dôvod.

3.1 Praktická ukážka rôznych aplikácií pre EP a pre ZEP

Na Slovensku chýba „ťažná aplikácia“ technológie EP. Ak by bola aspoň jedna takáto aplikácia, potom by sa nabaľovali aj ďalšie. Otázkou zostáva: “Kto by takúto aplikáciu mal rozbehnúť verejný alebo súkromný sektor?“.

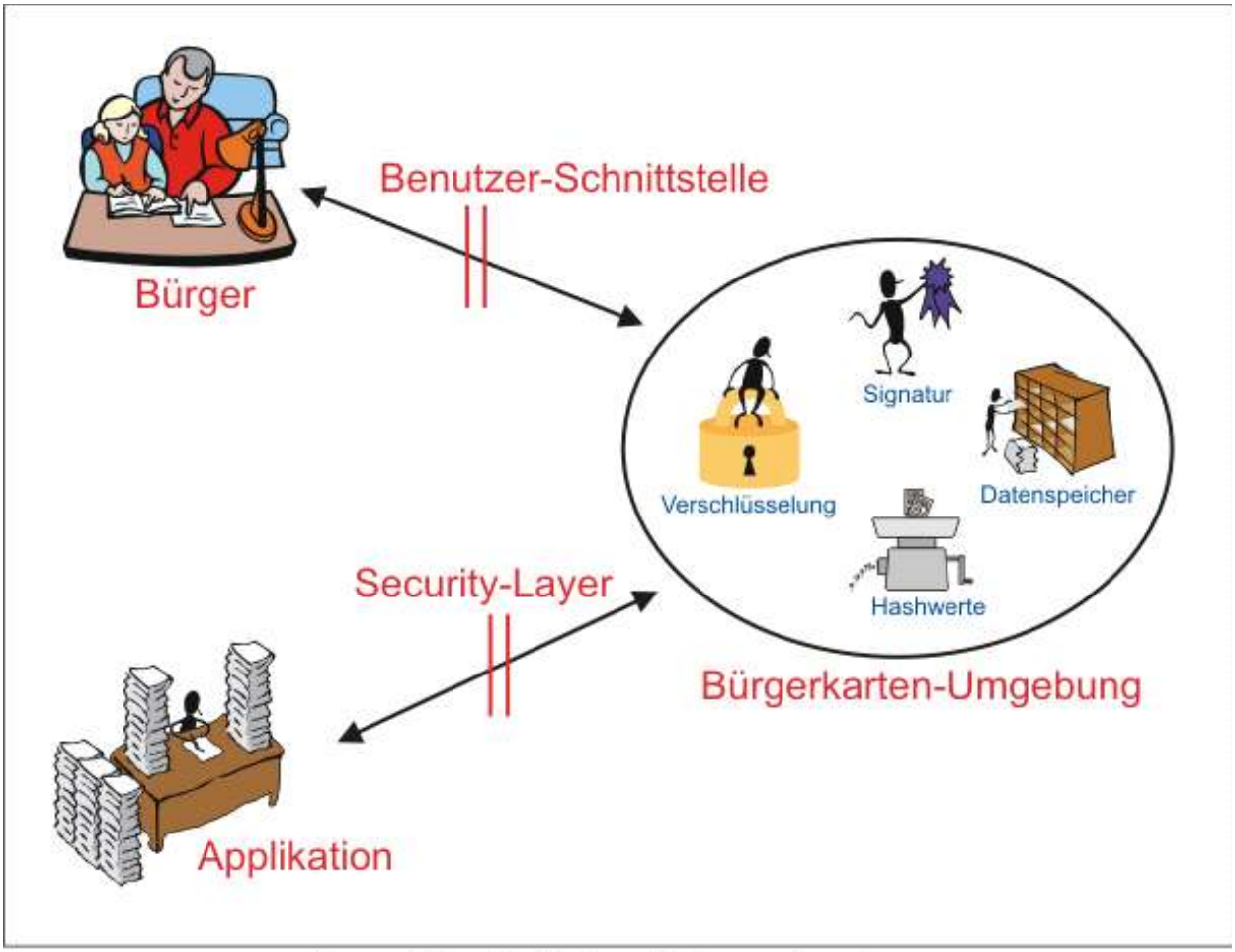
Príklady „ťažných aplikácií“:

- Verejný sektor – elektronické podateľne štátnych a verejnoprávnych inštitúcií (ministerstvá, sociálna poisťovňa, všeobecná zdravotná poisťovňa,...)
- Súkromný sektor – bankové a poisťovnícke domy (banky, sporiteľne, komerčné poisťovne) komunikácia s klientami.

Štát môže „zariadiť“ ťažnú aplikáciu zmenou legislatívy formuláciou „štátne a verejné inštitúcie musia umožniť administratívny styk s občanmi elektronickým spôsobom“. To znamená, že zmenou legislatívy by štátne a verejné inštitúcie boli povinné zriadiť elektronické podateľne. Treba však stanoviť dopad na štátny rozpočet.

3.2 Verejný sektor

Pre prípady rozvíjajúceho sa e-govermentu nemusíme ísť ďaleko, stačí ísť ku naším susedom do Rakúska. Výsledkom ich činnosti je zavedenie tzv. „Burger Karte“, alebo „Citizen Card“ – čo je elektronická podoba nášho občianskeho preukazu. Ten môže byť uchovaný buď na čipovej karte, alebo na mobilnom telefóne.



Das Modell der Bürgerkarte

Bürger - používateľ
Benutzer-Schnittstelle - rozhranie používateľa
Signatur - podpis
Verschlüssellung - kódovanie
Datenspeicher = vnútorná pamäť
Hashwerte - hodnota hash
Security-Layer - bezpečnostná vrstva
Bürgerkarten-Umgebung - okolie používateľskej karty
Applikation - aplikácia
Das Modell der Bürgerkarte - model používateľskej karty

Obr. 25: Model PKI v Rakúsku pre použite v eGoverment a eComerce aplikáciách

3.2.1 Model

Používateľská karta je model poskytujúci celý rad rozmanitých funkcií za účelom čo najrýchlejšieho výkonu E-Government a E-Commerce. V podstate možno pomocou používateľskej karty zhotovovať a kontrolovať elektronické podpisy prostredníctvom elektronických dokumentov, kódovať a dekódovať elektronické dokumenty, počítať a kontrolovať prostredníctvom elektronických dokumentov kontrolné informácie (hash) a ďalej zapisovať dáta do pamäti a potom ich z tejto pamäti vyberať.

Na schéme (Obr. 25)vidíme použitie používateľskej karty jej účastníkom. Okolie používateľskej karty „zabalí“ horeuvedené funkcie tak, aby používateľ používajúci tieto funkcie vrátane aplikácie riadil okolie používateľskej karty a mohol ho pohodlne používať.

Okrem toho grafická schéma uvádza dve rozhrania, ktorých podrobný popis je hlavným cieľom tejto špecifikácie: používateľské rozhranie reguluje komunikáciu medzi občanom a okolím používateľskej karty, kým rozhranie „security layer“ popisuje interakciu medzi aplikáciou a okolím používateľskej karty.

Na podrobný popis jednotlivých rozhraní a zainteresovaných strán sa používa nasledovná terminológia.

Používateľská karta

Podľa [E-GovG], §10 ZI 10 je používateľská karta "logická jednotka nezávislá od prevodu na odlišné technické komponenty a spája v sebe elektronický podpis s viazanosťou na jednu osobu (§ 4, odsek 2) s príslušnými bezpečnostnými údajmi a funkciami vrátane prípadných jestvujúcich plnomocenstiev". V zmysle terminológie používanej u špecifikácií pre rakúsku používateľskú kartu stáva sa okolie tejto karty implementáciou jej logickej jednotky.

Okolie používateľskej karty

Program či služba, ktorý umožňuje funkčnosť používateľskej karty karty. V podstate hovoríme o forme v podobe programu, ktorý prebieha lokálne na počítači používateľa (lokálne okolie používateľskej karty) alebo ako služba závislá od serveru, ktorá nabieha cez internet (okolie používateľskej karty závislé od serveru). Interakcia s týmto programom resp. službou prebieha cez dve rozhrania: cez používateľské rozhranie ako aj cez „security layer“.

Aplikácia

Tento program a dopyt na okolie používateľskej karty prechádza cez security layer, pričom prijíma a vyhodnocuje príslušné odpovede.

Používateľské rozhranie

Rozhranie, cez ktoré komunikuje užívateľ s okolím používateľskej karty. Cez toto rozhranie prebieha z jednej stránky používateľská interakcia, ktorá sa v prípade potreby vyžaduje pre výkon príkazu security layer (napr. indikácia signovaného dokladu, ak ide o príkaz na generovanie podpisu XML); z druhej stránky môže používateľ cez toto rozhranie konfigurovať samotné okolie používateľskej karty podľa vlastnej potreby (napr. môže meniť nastavenie pri ochrane prístupu ku svojim infoboxom). Predbežné nastavovanie hodnoty na používateľskom rozhraní sa riadi podľa požiadaviek na používateľské rozhranie.

Používateľ

Osoba, ktorá chce používať funkcie okolia používateľskej karty pri bezpečnom výkone E-Government alebo E-Commerce. Voľba okolia používateľskej karty prebieha spravidla nie prostredníctvom samotného používateľa, ale cez aplikáciu, ktorá sa rovná použitiu E-Government alebo E-Commerce.

Security layer

Rozhranie, cez ktoré komunikuje aplikácia s okolím používateľskej karty. Presný protokol, ktorý môže byť cez toto rozhranie vytvorený, sa špecifikuje v aplikačnom rozhraní security layer. Možné väzby protokolu na transportné vrstvy, ako je HTTP alebo TCP, sa reguluje transportným protokolom security layer.

3.2.2 Príkazy

Tento odsek nám poskytuje prehľad o funkciách, aké umožňuje okolie používateľskej karty. Funkcie možno v podstate rozdeliť na štyri rozsiahle oblasti:

- Vytváranie a skúšanie elektronických podpisov;
- Zakódovanie a odkódovanie elektronických dokumentov;
- Výpočet a kontrola hashových hodnôt cez elektronické dokumenty;
- Výber a záznam dát z dátovej alebo do dátovej pamäti.

3.2.2.1 Podpis

Užívateľ môže pomocou okolia používateľskej karty podpisovať elektronické dokumenty

ako aj preverovať jestvujúce podpisy cez elektronické dokumenty.

Podstatným znakom okolia používateľskej karty je v obidvoch prípadoch skutočnosť, že používateľ si môže predmetné elektronické dokumenty zobrazovať:

- pri tvorbe elektronického podpisu môže ešte pred ním presne skontrolovať údaje, ktoré skutočne podpisuje.
- Pri preverovaní jestvujúceho podpisu môže používateľ presne zistiť dáta chránené preverovaným podpisom..

Ak okolie používateľskej karty ponúka bezpečný podpis podľa [SigG] resp. cez [E-GovG] vymedzený rovnocenný podpis riadenia, zahrňuje doňho aj všetky právne zodpovednosti obidvoch spôsobilých druhov elektronického podpisu. Takto sa napríklad zlučuje pri tvorbe bezpečného elektronického popisu právne stanovená a certifikovateľná jednotka tvorby podpisu resp. tiež právne normovaná certifikačná jednotka zobrazenia v rámci jedného okolia používateľskej karty. To má pre vývoj aplikácií veľkú výhodu, ktorá spočíva v tom, že sa pri navrhovaní netreba starať o podobne zadávané právne údaje.

3.2.2.2 Kódovanie

Užívateľ môže pomocou okolia používateľskej karty kódovať nielen vlastné elektronické dokumenty pre akéhokoľvek adresáta, ale aj dekódovať jestvujúce kódované dokumenty pomocou dekódovacieho kľúča, ktorý je súčasťou okolia používateľskej karty.

3.2.2.3 Hash hodnoty

Užívateľ môže pomocou okolia používateľskej karty vypočítať hashovú hodnotu elektronického dokumentu a tiež overovať hashovú hodnotu v elektronickom dokumente.

3.2.2.4 Vnútorná pamäť

Okolie používateľskej karty poskytuje občanovi vnútornú pamäť pre čítanie a písanie akýchkoľvek dát požadovaných pre postupy u E-Government alebo E-Commerce.

V tejto špecifikácii sa člení vnútorná pamäť na logické jednotky označované ako infoboxy. Do vnútornej pamäte sa dajú ukladať nové infoboxy, môžu sa tam čítať, meniť alebo mazať. V okolí používateľskej karty sa nachádza celý rad štandardizovaných infoboxov. Tieto možno vyberať napríklad pre príslušné certifikáty priradené okolím používateľskej karty jednotlivým podpisovým resp. kódovacím kľúčom. Cez infoboxy si možno zaobstarať prístup k záznamom

normovaným v E-GovG ako je osobná väzba a plná moc. Táto špecifikácia zámerne neuvádza údaje ohľadne fyzického miesta, kde sa nachádzajú údaje vnútornej pamäti. Existuje celý rad možností, pričom tieto možnosti sa dajú pohodlne spolu kombinovať do jednej spoločnej a logickej vnútornej pamäte, napr.:

- Pamäť na bezpečnej jednotke tvorby podpisu (Smart-Card, USB-Token, ...), ak nám okolie používateľskej karty ponúkne vyhotovenie bezpečného podpisu;
- Pamäť na harddisku používateľa, ak ide v okolí používateľskej karty o lokálny program bežiaci na počítači používateľa;
- Pamäť adresovaná cez internet pod zvrchovaným prístupom providera, ak v okolí používateľskej karty ide o službu providera.

Nakoľko môžu infoboxy uložené v pamäti obsahovať chúlostivé informácie, kladú tieto špecifikácie príslušné požiadavky na uchovávanie a ochranu prístupu k nim.

3.2.3 Špecifikácie

V tomto odseku nájdeme prehľad jednotlivých špecifikačných dokumentov k rakúskej používateľskej karte. Všetky dokumenty majú informatívny charakter.

3.2.3.1 Aplikačné rozhranie security layer

Tento dokument popisuje rozhranie security layer, cez sa ktoré môže aplikácia dostať k funkciám poskytovaným okolím používateľskej karty. Rozhranie normuje celý rad príkazov; každý príkaz reaguje na jednoduchú schému dopyt/odpoveď, t.j. aplikácia položí okoliu karty otázku a toto okolie odpovie po spracovaní príkazu (prípadne po interakcii s užívateľom cez používateľské rozhranie. [ďalej ...]

3.2.3.2 Štandardizované kľúče a infoboxy

Tento dokument normuje identifikátory pre existujúce kľúčové boxy a infoboxy.

Kľúčový box označuje kľúč obsiahnutý v okolí karty, ktorý máme k dispozícii pre tvorbu elektronických podpisov resp. dekódovanie elektronických dát. Identifikátor pre kľúčový box príslušnými príkazmi security layer stanovuje, ktorý kľúč sa použije pre tvorbu podpisu resp. pre dekódovanie.

Infobox označuje zber dát uložený do okolia karty, ku ktorému umožňujú príkazy security layer prístup kvôli čítaniu či zmenám. V týchto príkazoch identifikátor infoboxu týmito príkazmi stanovuje, ktorý zber dát sa ukladá, číta, mení alebo vymazáva.

3.2.3.3 Minimálna konverzia u security layer

Tento dokument stanovuje, ktoré príkazy security layer musia byť implementované z okolia karty. V ďalšom obsahuje profily podpisových formátov používaných príkazmi na vytvorenie podpisu, jeho kontrolu, kódovanie a dekódovanie, úpravy pre zobrazovacie prvky okolia karty ako aj požiadavky na rozlišovanie URL vyskytujúce sa v jednotlivých príkazoch.

3.2.3.4 Transportné protokoly security layer

Rozhranie security layer možno aktivovať cez rôzne transportné protokoly. V tomto dokumente sa popisuje väzba security layer na transportné protokoly TCP, TLS, HTTP a HTTPS.

3.2.3.5 Požiadavky na používateľské rozhranie

Pre spracovanie celého radu príkazov security layer sa vyžaduje komunikácia okolia karty s používateľom prostredníctvom používateľského rozhrania, napríklad pri tvorbe podpisu ide o zobrazenie podpisových dát ako aj o rozlišovanie podpisovej funkcie zo strany používateľa. Dokument stanovuje požiadavky na takéto používateľské rozhranie u jednotlivých príkazov.

3.2.3.6 Ochrana prístupu

Vykonanie resp. výsledok väčšiny príkazov je u security layer pod ochranou. To znamená, že nie každá aplikácia môže vykonávať akýkoľvek príkaz security layer resp. môže mať prístup k výsledku vykonaného príkazu. Dokument špecifikuje ochranu prístupu, ktorú musí okolie karty rešpektovať. K tomu sa používa v prvom rade klasifikácia oprávnenia prístupu u aplikácie. Na základe klasifikácie sa stanovujú pravidlá, ktoré určujú, či príslušná aplikácia môže vykonať príkaz alebo nie.

3.2.3.7 Štandardný formát zobrazenia

Podstatné pre akceptovanie karty je, aby okolie karty a jeho komponenty boli dostupné na trhu a schopné spracovávať aspoň spoločný formát dokumentu (napríklad taký, aké sa používajú na zobrazovanie podpisových dát pri tvorbe podpisu). Tento formát by mal mať príslušné predpoklady pre layout ako aj pre viazanie obrazov, pritom však by mal byť vhodný ako zobrazovací formát pre bezpečný podpis. Dokument špecifikuje takýto dokumentačný formát spočívajúci na XHTML a CSS2.

3.2.3.8 Chybový kód u security layer

Ak nemožno z nejakého dôvodu spracovať príkaz z okolia karty, odpovie okolie aplikácii nie odpoveďou prislúchajúcou k dopytu, ale pomocou zvlášť vyšpecifikovanej chybovej odpovede. Dokument špecifikuje chybové kódy obsiahnuté v chybovej odpovedi

Aplikácie E-Government na základe používateľskej karty nájdeme na webovej stránke www.help.gv.at. Vzorovou aplikáciou pre obyvateľov Viedne je elektronické potvrdenie signalizácie. Pomocou karty sa však môžu vykonávať aj iné úradné postupy.

Pre elektronické doručovanie súdnych a úradných listín podľa zákona o E-Government možno nahlasovať pomocou používateľskej karty aj iné vzorové doručovacie služby.

U rakúskeho sociálneho poistenia sa môžu pomocou elektronického podpisu vyžadovať poistné termíny ako aj základné údaje k nemocenskému poisteniu. Pre zmluvných partnerov (napr. lekárov) existuje navyše tiež možnosť vyžiadania čísiel poistenia.

BAWAG je prvá rakúska banka, kde možno použiť pomocou TAN pri e-bankingu namiesto „podpisu“ bezpečný elektronický podpis.

ARA Altstoff Recycling Austria AG, a.s. pre zber a zhodnotenie odpadu podľa § 11 VerpackVO, preberá od zmluvných partnerov (výrobcov, dovozcov, baličov a distributérov) elektronicky podpísané hlásenia o objeme baliaceho materiálu, ktorý sa nachádza v obehu.

Neoverené certifikáty možno používať aj pre overovanie jednotlivým zákazníkom, napr. zo zasadaní HTTP (SSL resp. TLS). Príklad nájdeme na webovej stránke A-Trust. Telekom Austria umožňuje posielať pomocou takéhoto overovania dopyty, o.i. na pozemkovú databázu, zoznam firiem, centrálny ohlasovací register a na centrálny živnostenský register.

S/MIME je veľmi rozšírený štandard podporovaný väčšinou mailových klientov. Tento

štandard sa používa na kódovanie a podpisovanie e-mailov. Spoločnosti RTR-GmbH nie je známy žiaden Secure Viewer pre S/MIME (existencia Secure Viewer by bola dôležitým predpokladom pre vyhotovovanie bezpečných elektronických podpisov).

3.3 Súkromný sektor

Nekvalifikované certifikáty môžu slúžiť na autentifikáciu klientov, napr. http session, SSL, alebo TSL. S/MIME je široko rozšírený a väčšinou mail-klientov podporovaný štandard na kryptovanie a podpisovanie e-mailov.

3.3.1 S/MIME – Bezpečná pošta

Štandard pre zabezpečenie elektronickej pošty S/MIME bol navrhnutý organizáciou RSA Labs. a prijatý množstvom výrobcov. Špecifikáciu S/MIME vo verzii 2 pôvodne vydala firma RSA Data Security, ale kvôli dosiahnutiu vyššej akceptácie odovzdali špecifikáciu združeniu IETF, ktoré S/MIME vylepšilo a vyvinulo verziu 3, ktorá sa používa v súčasnosti. Dnes je S/MIME považovaný za priemyselný štandard a je podporovaný veľkou väčšinou komerčných softvérových produktov. Systém S/MIME počíta s hierarchickou infraštruktúrou certifikačných autorít a na svoju správnu činnosť potrebuje osobný certifikát vydané certifikačnou autoritou pre koncového používateľa.

Certifikačná autorita vydáva certifikáty pre koncových požívateľov automaticky. Certifikát je možné získať v priebehu niekoľkých minút. Na získanie osobného certifikátu postačuje prejsť niekoľko jednoduchých krokov, sumarizovaných v tabuľke č.2.

Krok 1	Otvorenie prehliadača na stránke http://identity.bgs.sk/
Krok 2	Vyplnenie žiadosti o osobný certifikát
Krok 3	Automatické overenie totožnosti žiadateľa certifikačnou autoritou
Krok 4	Nainštalovanie hotového certifikátu do prehliadača

Tab. 2: Procedúra vydania osobného certifikátu od CA

V prvom kroku si otvoríte svoj prehliadač na stránke certifikačnej autority Identity. Ak ste tu prvý krát, veľmi jednoduchou procedúrou si nainštalujete koreňový certifikát certifikačnej autority Identity.

Keď na stránkach certifikačnej autority prejdete na podstránku s osobnými certifikátmi, vyplníte svoje základné osobné údaje do formulára žiadosti o osobný certifikát (krok 2). Najdôležitejší údaj v tomto formulári je vaša e-mail adresa. Vaša adresa slúži ako váš jednoznačný identifikátor a pomocou tejto adresy sa bude overovať vaša identita. Po vyplnení formulára začne váš prehliadač automaticky generovať kľúčový pár a žiadosť o certifikát. Váš práve vygenerovaný súkromný kľúč sa bezpečne uloží na disku vašej pracovnej stanice a žiadosť o certifikát sa automaticky odošle certifikačnej autorite.

Po prijatí platnej žiadosti o certifikát certifikačnou autoritou nasleduje overenie vašej identity (krok 3). Certifikačná autorita pošle na vami uvedenú e-mail adresu správu, ktorá obsahuje špeciálne URL, na ktorom si môžete prevziať váš certifikát. Ak ste zadali skutočne vašu adresu, za niekoľko minút po vyplnení žiadosti vám bude doručená výzva k prevzatiu certifikátu.

Ak otvoríte váš prehliadač na URL uvedené v e-mailovej správe od certifikačnej autority, ukáže sa vám stránka so základnými údajmi o vašom certifikáte. Máte hneď možnosť certifikát si nainštalovať do prehliadača kliknutím na príslušný odkaz na stránke (krok 4). Po takomto nainštalovaní je osobný certifikát pripravený na používanie. Ak používate poštový systém, ktorý je priamo integrovaný s prehliadačom alebo operačným systémom, nie je potrebná už žiadna ďalšia činnosť a môžete plne využívať bezpečnostné vlastnosti vášho poštového systému.

S/MIMEv3 definuje dve MIME obálky, jednu pre digitálny podpis a druhú pre šifrovanie. Ak sa použije digitálny podpis aj šifrovanie, použijú sa obe obálky a email sa najprv podpíše a potom zašifruje. Syntax oboch obálok sa riadi štandardom PKCS 7. Digitálny podpis používa štruktúru „signed-data“, šifrovanie používa štruktúru „enveloped-data“.

S/MIMEv3 obsahuje nové rozšírenia oproti S/MIMEv2:

- **Digitálne podpísané potvrdenia o doručení** – umožňujú odosielateľovi zistiť, či bola správa doručená príjemcovi bez modifikácie. Príjemca dokáže vygenerovať platné potvrdenie o doručení iba v prípade, ak bola správa podpísaná odosielateľom a príjemca overil platnosť podpisu. Keď Alica pošle Bobovi emailom objednávku a dostane od Boba potvrdenie o doručení, získa Alica dôkaz, že objednávka bola doručená a že nebola cestou zmenená.
- **Bezpečnostné návestia** – umožňujú odosielateľovi určiť podmienky zaobchádzania s obsahom správy. Najčastejšie sa používa na vyjadrenie proprietárnosti alebo vyhradenosti

obsahu správy, napr. v prípade vládnych organizácií.

- **Podpora diskusných skupín** – ak chce odosielateľ poslať šifrovaný e-mail väčšiemu zoznamu príjemcov, bežný postup je nasledovný: odosielateľ zašifruje e-mail pomocou symetrického kľúča a následne tento kľúč doručí každému príjemcovi zašifrovaný jeho verejným kľúčom. Tento postup je však časovo veľmi náročný a s výhodou ho možno nahradiť použitím špeciálneho servera, ktorý sa nazýva Mail List Agent (MLA). V takom prípade odosielateľ zašle šifrovanú správu iba jedinému príjemcovi – na MLA a ďalšie operácie odosielania správy príjemcom sa vykonávajú už na tomto serveri. MLA nemusí dešifrovať správu, ale má prístup ku kľúču, ktorý bol použitý na šifrovanie správy. Odosielateľ musí používať MLA, ktorý je označený ako dôveryhodný (trusted) a ktorý odošle e-mail iba členom diskusnej skupiny.

Všetky služby S/MIME používajú certifikáty a v nich zviazanosť verejného kľúča a emailovej adresy používateľa. Emailová adresa by sa mala nachádzať v rozšírení certifikátu. V prípade, že nie je uvedená email adresa v certifikáte môže dôjsť k problémom pri spájaní s identitou. Pri šifrovaní musí mať odosielateľ istotu, že verejný kľúč použitý na distribúciu kľúča na šifrovanie obsahu patrí správnemu príjemcovi. Použitím nesprávneho verejného kľúča sa odosielateľ vystavuje riziku, že sa k obsahu správy dostane nepovolaná osoba. Rovnako sa aj MLA spolieha na správne zviazanie identity príjemcu a jeho verejného kľúča a na distribúciu symetrického kľúča iba pre účastníkov diskusnej skupiny.

Pri digitálnom podpisovaní musí mať príjemca istotu, že verejný podpisovací kľúč určený na overenie digitálneho podpisu patrí odosielateľovi. Príjemca musí porovnať emailovú adresu z hlavičky „Sender“ alebo „From“ s emailovou adresou uvedenou v certifikáte.

Pri potvrdeniach o doručení musí mať overovateľ potvrdenia istotu, že verejný podpisovací kľúč určený na overenie podpisu potvrdenia patrí odosielateľovi potvrdenia. Overovateľ potvrdenia o doručení musí porovnať emailovú adresu zo žiadosti o potvrdenie s emailovou adresou v certifikáte.

3.3.2 SSL – Bezpečné servery

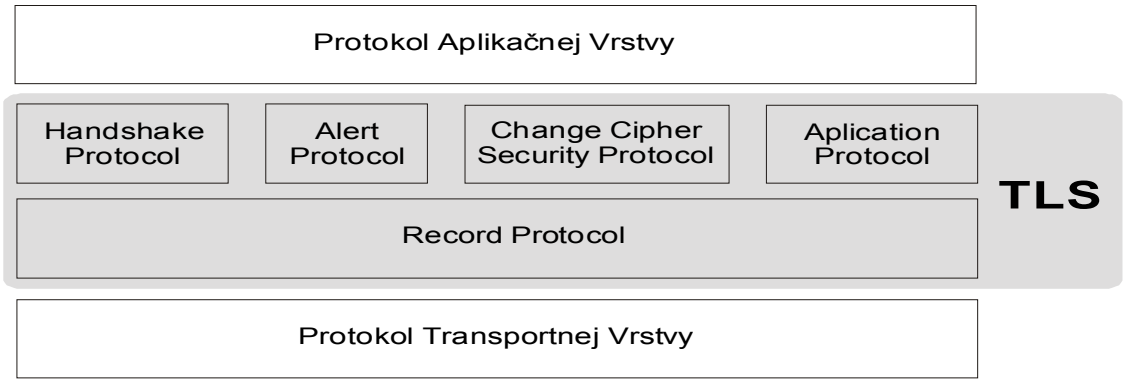
Systém „Secure Socket Layer“, alebo skrátene SSL, je nadstavba protokolu TCP, ktorá ho obohacuje o bezpečnostné prvky. SSL prináša šifrovanie spojenia, kryptografické zabezpečenie

integrity spojenia (MAC) a vzájomnú autentifikáciu komunikujúcich strán. Použitie SSL je pre aplikácie prakticky transparentné, do vývojárov aplikácie vyžaduje len minimálnu modifikáciu systému. Pomocou SSL je štandardne riešené zabezpečenie bežných služieb Internetu, ako napríklad HTTP, POP3, IMAP, atď. Najčastejšie sa SSL používa na zabezpečenie WWW serverov. Rozšírenie štandardného protokolu HTTP o bezpečnostné služby SSL sa nazýva HTTPS. Tento protokol umožňuje dramaticky zvýšiť bezpečnosť vášho servera s minimálnou námahou. Pre WWW aplikácie je tento protokol absolútne transparentný, nevyžaduje si žiadnu zmenu aplikácie. Ochrana údajov (šifrovanie, MAC) prebieha medzi prehliadačom koncového používateľa a procesmi WWW servera. WWW server predkladá používateľovi svoj certifikát, vylučujúc tak možnosť zámeny IP adresy servera. Samotný koncový používateľ nepotrebuje osobný certifikát, ak ho však má, môže ho použiť na autentifikáciu. Takáto silná autentifikácia je oveľa bezpečnejšia ako autentifikácia heslami.

Certifikačná autorita vydáva certifikáty pre zabezpečené servery, použiteľné pre komunikáciu protokolom SSL. Správca servera si vygeneruje na svojom systému kľúčový pár a žiadosť o certifikát spôsobom vhodným pre jeho server. Privátny kľúč sa bezpečne uloží v systéme servera, žiadosť o certifikát správca odošle pomocou WWW formulára certifikačnej autorite. Pracovník certifikačnej autority manuálne overí identitu servera jednak kontrolou DNS záznamov a ostatných záznamov vzťahujúcich sa na vlastníctvo doménového mena, ako aj kontrolou autenticity mena organizácie uvedenej v žiadosti. Po úspešnom overení žiadosti nasleduje manuálne podpísanie žiadosti Certifikačnou autoritou a doručenie podpísaného certifikátu žiadateľovi elektronickou cestou. Celá procedúra by nemala trvať dlhšie ako niekoľko dní.

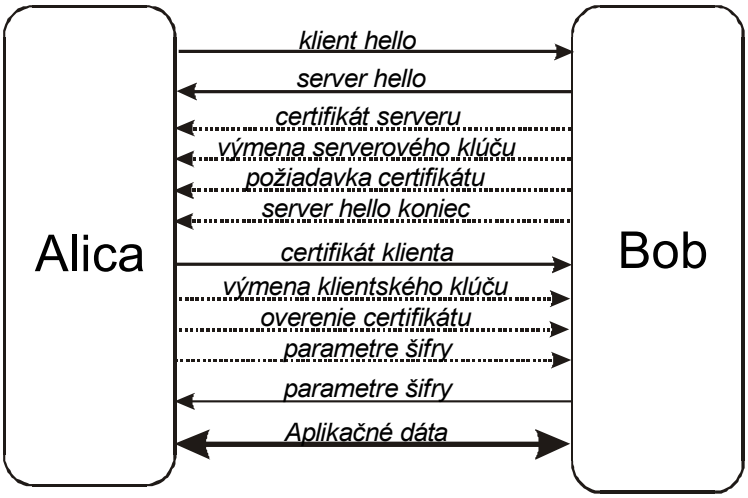
3.3.3 Transport Layer Security protokol

Špecifikácia Transport Layer Security (TLS) je odvodená od špecifikácie Secure Socket Layer verzia 3 (SSLv3) spoločnosti Netscape. Slúži na zabezpečenie ľubovolného TCP spojenia medzi uzlami siete.



Obr. 26: Vrstvy protokolu TLS

Protokol TLS je tvorený dvoma vnútornými vrstvami a niekoľkými pomocnými subprotokolmi. Nižšia vrstva (Record Protokol) je určená na transport správ komunikačnými kanálmi. Vyššia vrstva nastavuje parametre zriadenej relácie (session), jej manažment a signalizáciu. Aplikačný subprotokol je zodpovedný za prenos dát poskytovaných aplikačnou vrstvou. TLS nevyžaduje žiaden konkrétny šifrovací algoritmus. Komunikujúce strany sa sami dohodnú na najvhodnejšom spoločnom algoritme pre zabezpečenie komunikácie. Protokol je asymetrický, čo znamená, že klient iniciuje spojenie na pasívne čakajúci server. TLS poskytuje rôzny stupeň autentifikácie komunikujúcich uzlov od úplnej anonymity, kedy neprebieha autentifikácia medzi uzlami, cez čiastočnú autentifikáciu, kedy jeden z uzlov dokazuje svoju totožnosť pomocou certifikátu X.509, po úplnú autentifikáciu, kedy sa navzájom autentifikujú oba uzly certifikátmi X.509. Najbežnejším dnešným spôsobom je čiastočná autentifikácia, moderné systémy ale plne podporujú úplnú autentifikáciu.



Obr. 27: Komunikácia pomocou TLS

Vzhľadom na to, že celá výmena kľúča pre symetrický komunikačný kryptografický algoritmus sa deje pomocou asymetrického šifrovania, nie je možné odpočuť a tak zistiť aký bol zvolený komunikačný kľúč. Tým pádom je spojenie bezpečné a celá ďalšia výmena dát je zabezpečená.

TLS sa v dnešnej dobe bežne používa na zabezpečenie prístupu k službám ako HTTP, IMAP, POP, LDAP atď.

Na komunikáciu medzi uzlami sa môže používať aj asymetrická šifra, ktorá je ale v porovnaní so symetrickou veľmi náročná na matematické operácie a prostriedky výpočtového systému, a teda v konečnom dôsledku pomalá.

3.3.4 IPsec

IPsec poskytuje ochranu na tretej (sieťovej) vrstve referenčného modelu OSI, ochraňuje teda IP datagramy. Pomocou IPsec možno chrániť buď komunikáciu medzi dvoma zariadeniami, alebo komunikáciu medzi bránami dvoch organizácií. Protokol IPsec sa používa pri vytváraní virtuálnych privátnych sietí (Virtual Private Networks – VPNs). IPsec vyvinulo združenie IETF ako hybrid existujúcich proprietárnych riešení a predstavuje teda komplexnú bezpečnostnú architektúru IP.

Pri komunikácii pomocou IPsec sa vytvárajú bezpečnostné asociácie. Bezpečnostná asociácia pomocou atribútov určuje bezpečnostný protokol AH alebo ESP, algoritmus na symetrické

šifrovanie, obsahuje autentifikačné a šifrovacie kľúče, definuje platnosť kľúčov a identifikuje IP adresy oboch účastníkov.

Bezpečnostnú asociáciu jednoznačne identifikujú tri položky:

- security parameter index (SPI). SPI identifikuje každú bezpečnostnú asociáciu
- cieľová IP adresa. Principiálne môže byť unicastová, broadcastová alebo multicastová, ale IKE je v súčasnosti definované len pre unicastové adresy.
- identifikátor bezpečnostného protokolu (AH alebo ESP)

Obr. 28: IPsec tunelovací režim

Existujú dva druhy bezpečnostných asociácií pre oba protokoly AH aj ESP:

- **Transportný režim** – umožňuje ochranu spojenia medzi dvoma zariadeniami. Hlavička protokolu AH alebo ESP sa nachádza medzi IP hlavičkou a protokolom vyššej vrstvy (TCP, UDP). Protokol ESP v transportnom režime ochraňuje iba vyššie vrstvy, pri použití AH možno okrem protokolu vyššej vrstvy ochrániť aj vybrané časti IP hlavičky.

Tunelovací režim – umožňuje ochrániť IP tunel. V prípade, že niektorý koniec bezpečnostnej asociácie je smerovač alebo firewall, treba použiť tunelovací režim. V tomto režime sa hlavička protokolu AH alebo ESP nachádza medzi dvomi IP hlavičkami. Vonkajšia IP hlavička určuje adresu zariadenia, ktoré spracuje IPsec, vnútorná IP hlavička určuje skutočnú IP adresu pre doručenie datagramu. ESP v tunelovacom režime ochraňuje IP hlavičku a protokol vyššej vrstvy, AH ochraňuje vnútornú IP hlavičku, protokol vyššej vrstvy a vybrané časti vonkajšej IP hlavičky.

Authentication Header (AH) – Bezpečnostný protokol AH zabezpečuje integritu pre IP datagram a autentifikuje zdroj datagramu buď podľa zdrojovej IP adresy alebo mena koncového

používateľa. AH poskytuje integritu pre protokol vyššej vrstvy a vybrané časti IP hlavičky a navyše aj ochranu pred „replay“ útokom, čo zvyšuje zabezpečenie proti DOS útokom. Na zabezpečenie integrity sa používa hashovacia funkcia MD5 alebo SHA-1. Protokol AH neposkytuje šifrovanie.

Encapsulating Security Payload (ESP) – Bezpečnostný protokol ESP umožňuje zabezpečiť utajenie (šifrovanie), autentifikáciu a integritu. Utajenie sa zabezpečuje šifrovaním obsahu. Autentifikácia a integrita sa zabezpečuje rovnakým spôsobom ako v prípade protokolu AH. V bezpečnostnej asociácii treba použiť buď utajenie alebo autentifikáciu, prípadne nepovinne aj obe súčasne. Ak sa použije autentifikácia, poskytuje protokol rovnaké zabezpečenie proti „replay“ útokom ako protokol AH.

V tunelovacom režime sa používa šifrovanie medzi dvoma bránami, čo poskytuje čiastočné utajenie dátového toku. Identity zdroja a cieľa sú totiž utajené. Na šifrovanie sa využívajú algoritmy DES, 3DES, prípadne ďalšie algoritmy. Na zabezpečenie integrity sa používajú hashovacie funkcie MD5 alebo SHA-1.

Výmena kľúčov (Internet Key Exchange – IKE) – Výmena kľúčov sa uskutočňuje v dvoch fázach. Prvej fáze sa vytvorí autentifikovaný a šifrovaný kanál. Na zviazanie identity vzdialenej implementácie IPsec s verejným kľúčom sa používajú certifikáty. V druhej fáze sa vytvorí jedna alebo viacero bezpečnostných asociácií pre protokoly AH a ESP.

4 Elektronický podpis – legislatíva

V nasledujúcej kapitole v krátkosti sumarizujeme zo zákona NR SR č. 215/2002 Z.z. o elektronickom podpise vyhlášok NBÚ k zákonu 215/2002 Z.z., robíme to z dôvodu jednoznačnosti názvoslovia a poukázania na niektoré administratívne problémy v problematike PKI na Slovensku.

4.1 Zákon NR SR č. 215/2002 Z.z. o elektronickom podpise

Tento zákon upravuje vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním elektronického podpisu, práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom. Tento zákon sa nevzťahuje na vyhotovenie a používanie elektronického podpisu pre utajované skutočnosti podľa osobitného zákona. Na vyhotovenie a používanie elektronického podpisu v uzavretých systémoch sa tento zákon použije, ak sa účastníci uzavretého systému nedohodnú inak. Zákon nadobudol účinnosť v plnom rozsahu dňa 1. septembra 2002. Zákon vychádza zo Smernice Európskej únie č. 1999/93/EC z decembra 1999.

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

- nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu,
- na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.

(§ 3 ods. 1 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise)

§4 – Zaručený elektronický podpis - spĺňa požiadavky uvedené v §3 a naviac:

- je vyhotovený pomocou súkromného kľúča, ktorý je určený na vyhotovenie zaručeného EP
- možno ho vyhotoviť len s použitím bezpečného zariadenia na vyhotovovanie zaručeného EP
- na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie zaručeného EP je vydaný kvalifikovaný certifikát

§6 - Certifikát verejného kľúča - je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný (§ 6 zákona NR SR č. 215/2002 Z.z. o elektronickom podpise). Skladá sa z tela certifikátu a z elektronického podpisu tela certifikátu.

- telo certifikátu obsahuje najmä:
- identifikačné údaje držiteľa certifikátu
- verejný kľúč držiteľa certifikátu
- identifikačné údaje vydavateľa certifikátu
- identifikačné číslo certifikátu
- dátum a čas začiatku a konca platnosti certifikátu
- identifikáciu algoritmov, pre ktoré je uvedený verejný kľúč určený
- identifikáciu algoritmov použitých pri vyhotovení elektronického podpisu tela certifikátu

§7 - Kvalifikovaný certifikát - je certifikát verejného kľúča podľa predchádzajúcej definície a naviac:

- je v ňom uvedené, že je kvalifikovaný
- má v sebe uvedené obmedzenia na jeho použitie, ak tretia strana takéto obmedzenia rozlišuje
- je v ňom uvedený účel, na ktorý je určený
- má telo certifikátu podpísané zaručeným EP
- vydala ho akreditovaná CA alebo NBÚ

Typy kvalifikovaných certifikátov (KC):

- KC fyzickej osoby – vydáva ho akreditovaná CA fyzickej osobe
- KC akreditovanej CA – vydáva ho NBÚ akreditovanej certifikačnej autorite
- kvalifikovaný krížový certifikát – vydáva ho akreditovaná CA akreditovanej CA-te
- kvalifikovaný certifikát NBÚ – vydáva ho NBÚ na vlastný verejný kľúč (tzv. self signed certificate)

§9 - Časová pečiatka - je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

a) vyhotovila ju akreditovaná CA použitím súkromného kľúča určeného na tento účel
b) na verejný kľúč patriaci k uvedenému súkromnému kľúču bol vydaný kvalifikovaný certifikát
c) bola vyhotovená len použitím bezpečného zariadenia na vyhotovovanie časovej pečiatky
d) umožňuje jednoznačne identifikovať dátum a čas kedy bola vyhotovená

§12 - Certifikačná autorita - je poskytovateľ certifikačných služieb, ktorý spravuje certifikáty a vykonáva certifikačnú činnosti

a) poskytovanie certifikačných služieb je podnikaním
b) na vykonávanie certifikačných činností a poskytovanie certifikačných služieb sa povolenie nevyžaduje

Povinnosti CA pred začatím poskytovania služieb je CA povinná zverejniť:

a) certifikačný poriadok
b) používané technické špecifikácie, formáty, normy a štandardy
c) cenník platených služieb a zoznam bezplatne poskytovaných služieb
d) obmedzenia pri poskytovaní služieb, ak existujú
e) informácie o svojej akreditácii
   - zverejňovať svoje identifikačné údaje a informácie o svojich certifikátoch
   - oznámiť NBÚ začiatok svojej činnosti min. 30 dní vopred

CA je ďalej povinná:

a) mať vypracované bezpečnostné pravidlá a pravidlá na výkon certifikačných činností

b) dodržiavať uvedené pravidlá počas celej doby poskytovania certifikačných služieb
c) vykonávať certifikačné činnosti tak, aby nebolo možné vytvárať kópie súkromných kľúčov
d) certifikáty vydávať na základe zmluvy
e) pred uzavretím zmluvy informovať žiadateľa o svojej bezpečnostnej politike a pravidlách poskytovania certifikačných služieb
f) poskytnúť žiadateľom informácie o produktoch pre EP
g) informovať žiadateľa o možných právnych dôsledkoch
h) zabezpečovať vydávanie certifikátov
i) zabezpečovať službu zrušenia certifikátov
j) zverejňovať zoznam zrušených certifikátov
k) viesť prevádzkovú dokumentáciu
l) archivovať súvisiacu dokumentáciu

§13 – Akreditácia - Certifikačná autorita môže NBÚ požiadať o akreditáciu:

- Akreditovanou CA môže byť právnická alebo fyzická osoba, ktorá má vytvorené materiálne, priestorové, technické, personálne, organizačné a právne podmienky na poskytovanie akreditovaných certifikačných služieb
- podrobnosti o podmienkach na poskytovanie akreditovaných certifikačných služieb stanovuje vyhláška NBÚ č. 540/2002 Z.z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov
- ak žiadateľ o akreditáciu splnil podmienky na udelenie akreditácie, NBÚ do 90 dní od prijatia žiadosti rozhodne o akreditácii a certifikačnej autorite vystaví certifikát

Povinnosti akreditovanej CA

- všetky povinnosti CA sa vzťahujú aj na akreditovanú CA
- bezpečnostné pravidlá a pravidlá na výkon certifikačných činností musia byť v súlade s vyhláškou NBÚ č. 541/2002 Z.z ., o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností
- akreditovaná CA je povinná preukázať spoľahlivosť nevyhnutnú na poskytovanie

certifikačných služieb

§21 Registračná autorita - RA koná v mene certifikačnej autority alebo na základe zmluvy uzatvorenej s certifikačnou autoritou. RA je vo svojej činnosti viazaná certifikačným poriadkom CA, v ktorej mene koná alebo s ktorou má uzatvorenú zmluvu RA najmä:

- prijíma žiadosti o vydanie certifikátu
- kontroluje súlad údajov v žiadosti o certifikát s údajmi v predloženom preukaze totožnosti žiadateľa o vydanie certifikátu
- odosiela žiadosti o vydanie certifikátu certifikačnej autorite
- odovzdáva certifikáty žiadateľom o vydanie certifikátu

§15 - Zrušovanie certifikátov - CA je povinná zrušiť certifikát, ktorý spravuje, ak:

- zistí, že pri vydaní certifikátu neboli splnené podmienky podľa zákona
- zistí, že certifikát bol vydaný na základe nepravdivých údajov
- o zrušenie certifikátu požiada držiteľ
- to nariadi súd
- zistí, že držiteľ zomrel alebo právnická osoba zanikla
- zistí, že súkromný kľúč patriaci k verejnému kľúču uvedenému v certifikáte pozná iná osoba

Certifikát sa považuje za zrušený od okamihu vydania prvého zoznamu zrušených certifikátov, ktorý tento certifikát obsahuje. Platnosť zrušeného certifikátu nemožno obnoviť.

§8 - Zoznam zrušených certifikátov - elektronický dokument, ktorým vydavateľ certifikátov oznamuje predčasné ukončenie ich platnosti. Skladá sa z tela zoznamu zrušených certifikátov a elektronického podpisu tela zoznamu zrušených certifikátov.

Telo zoznamu zrušených certifikátov obsahuje najmä:

- identifikačné údaje vydavateľa certifikátov
- dátum a čas vydania zoznamu zrušených certifikátov
- dátum a čas vydania ďalšieho zoznamu zrušených certifikátov
- zoznam identifikačných čísiel certifikátov, ktoré boli zrušené spolu s dátumom a časom ich

zrušenia

§10 – Úrad (NBÚ) - Ústredným orgánom štátnej správy pre EP je NBÚ. Požiadavky na správu kvalifikovaných certifikátov akreditovanou CA sa vzťahujú aj na NBÚ.

NBÚ plní tieto úlohy:

- vykonáva kontrolu dodržiavania zákona
- posudzuje žiadosti CA-ít pôsobiacich v SR o akreditáciu, udeľuje a odníma akreditáciu
- vydáva kvalifikované certifikáty verejných kľúčov akreditovaným certifikačným autoritám
- zverejňuje vlastný verejný kľúč
- vydáva kvalifikované certifikáty verejných kľúčov zahraničným certifikačným autoritám
- eviduje CA pôsobiace v SR
- vedie a zverejňuje zoznam akreditovaných CA a CA s odňatou akreditáciou
- zrušuje vydané kvalifikované certifikáty
- vedie register zahraničných CA, ktorých certifikáty boli uznané na použitie v SR
- certifikuje produkty pre elektronický podpis
- plní ďalšie úlohy vyplývajúce zo zákona

§11 – Kontrola - NBÚ môže kontrolovať CA odo dňa oznámenia začiatku svojej činnosti.

CA je povinná umožniť výkon kontroly. Ak CA porušuje povinnosti vyplývajúce zo zákona (napr. nie je dostatočne bezpečnostne spoľahlivá) môže NBÚ najmä:

- obmedziť (max. na 3 mesiace) alebo zakázať poskytovanie certifikačných činností
- nariadiť zrušenie kvalifikovaných certifikátov

§15 - Používanie elektronického podpisu - Ak možno v styku s verejnou mocou používať elektronický podpis, tento EP musí byť zaručeným elektronickým podpisom, Pri overovaní zaručeného EP overovateľ na základe kvalifikovaného certifikátu verejného kľúča overí, či verejný kľúč na overenie zaručeného EP patrí podpisovateľovi.

§22 - Povinnosti držiteľa certifikátu - Držiteľ certifikátu je povinný:

a) zaobchádzať so svojím súkromným kľúčom s náležitou starostlivosťou, tak aby nedošlo k

zneužitiu súkromného kľúča

b) uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča
c) neodkladne požiadať CA, ktorá spravuje jeho certifikát o zrušenie certifikátu, ak zistí, že došlo alebo hrozí zneužitie jeho súkromného kľúča.

Za škodu spôsobenú porušením povinností zodpovedá držiteľ.

§24 – Požiadavky na produkty pre elektronický podpis - Na uchovávanie súkromných kľúčov a na vyhotovovanie zaručených elektronických podpisov sa musia používať bezpečné zariadenia, ktoré spoľahlivo chránia v nich uložený súkromný kľúč. Súlad bezpečných zariadení s bezpečnostnými požiadavkami overuje a potvrdzuje NBÚ.

Bezpečné zariadenia musia najmä:

a) zabezpečiť, že podpisovaný elektronický dokument sa pri podpise nezmení
b) umožniť zobrazenie podpisovaného dokumentu ešte pred podpísaním

§17 – Uznávanie zahraničných certifikátov - Certifikát alebo kvalifikovaný certifikát, ktorý vydala CA so sídlom v zahraničí možno uznať v SR ak: Medzinárodná dohoda podpísaná Slovenskou republikou ustanovuje, že zahraničný kvalifikovaný certifikát je uznávaný ako kvalifikovaný certifikát alebo zahraničná CA je uznaná za akreditovanú CA v SR.

§25 – Audit - Akreditovaná CA je povinná opakovane sa podrobiť externému auditu bezpečnosti poskytovania certifikačných činností (raz za 12 mesiacov). Záverečná správa o výsledkoch auditu sa musí predložiť NBÚ do 30 dní od ukončenia auditu. Podrobnosti a audite sú vo vyhláške NBÚ č.540/2002 Z.z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov.

§33 – Ochrana osobných údajov - Na informačný systém poskytovateľa certifikačných služieb sa vzťahuje zákon NR SR č. 428/2002 Z.z. o ochrane osobných údajov v informačných systémoch

4.2 Vyhláška NBÚ č. 537/2002 Z. z.

O formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky).

Táto vyhláška upravuje:

a) formát a spôsob vyhotovenia zaručeného elektronického podpisu,
b) podrobnosti o podmienkach platnosti pre zaručený elektronický podpis, postup pri overovaní zaručeného elektronického podpisu a podmienky overenia platnosti zaručeného elektronického podpisu,
c) spôsob zverejňovania verejného kľúča úradu,
d) podpisové schémy, algoritmy a parametre týchto algoritmov na vyhotovovanie zaručeného elektronického podpisu,
e) formát a spôsob vyhotovovania časovej pečiatky,
f) požiadavky na vedenie dokumentácie časových pečiatok.

4.3 Vyhláška NBÚ č. 538/2002 Z. z.

O formáte a obsahu kvalifikovaného certifikátu, o správe kvalifikovaných certifikátov a o formáte, periodicite a spôsobe vydávania zoznamu zrušených kvalifikovaných certifikátov (o kvalifikovaných certifikátoch).

Táto vyhláška upravuje:

a) formát a obsah kvalifikovaného certifikátu,
b) podrobnosti o správe kvalifikovaných certifikátov,
c) formát zoznamu zrušených kvalifikovaných certifikátov,
d) periodicitu vydávania zoznamu zrušených kvalifikovaných certifikátov,
e) spôsob vydávania zoznamu zrušených kvalifikovaných certifikátov.

4.4 Vyhláška NBÚ č. 539/2002 Z. z.

‚ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (o produktoch elektronického podpisu).

Táto vyhláška upravuje:

a) podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky,
b) požiadavky na produkty pre elektronický podpis.

4.5 Vyhláška NBÚ č. 540/2002 Z. z.

O podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov.

Táto vyhláška upravuje podrobnosti o:

a) formát materiálnych, priestorových, technických, organizačných a právnych podmienkach na poskytovanie akreditovaných certifikačných služieb,
b) požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov a o výkone auditu akreditovanej certifikačnej autority.

4.6 Vyhláška NBÚ č. 541/2002 Z. z.

O obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností.

Táto vyhláška upravuje:

a) obsah a rozsah prevádzkovej dokumentácie certifikačnej autority,
b) bezpečnostné pravidlá a pravidlá na výkon certifikačných činností akreditovanej certifikačnej autority.

4.7 Vyhláška NBÚ č. 542/2002 Z. z.

o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku. Vyhláška upravuje podrobnosti o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku.

5 Analýza Certifikačných autorít

V tejto časti sa budeme venovať analýze možnosti využitia práce našich predchodcov, ktorí sa zaoberali rovnakou, prípadne podobnou tématikou. Z nášho pohľadu je efektívne, keby sme využili výsledky ich práce.

5.1 Požiadavky na CA

Funkčné moduly – tato požiadavka definuje, že systém Certifikačnej Autority (ďalej iba CA) musí implementovať moduly, ktoré jej zabezpečia dostatočnú použiteľnosť a funkčnosť v našom projekte. Identifikovali sme nasledovne potrebne funkčné moduly/časti:

- implementuje hlavne schémy PKI
- verejne rozhranie, ktoré umožní interakciu používateľov zo systémom CA
- rozhranie, ktoré umožní manažovanie CA
- generovanie self-signed CA certifikátov a CRL
- generovanie certifikačných požiadaviek s bežne prístupným webovým prehliadačmi
- poskytovanie klientských certifikátov/CRL
- on-line validácia certifikátov
- uloženie certifikátov v LDAP

Verejná dostupnosť (Open Source Licencia) – táto požiadavka vyplýva z toho že, pre takýto projekt nie je potrebné vynaložiť finančné prostriedky na niektorú z komerčných CA a preto sa orientujeme na voľne dostupné CA. Toto neznamená, že verejne dostupné CA sú menej kvalitne ako komerčné, často je to býva naopak. Kvalitu ktorú verejná CA musí poskytovať je na rovnakej úrovni ako komerčná.

Podpora lokalizácie – jednou z požiadaviek na CA ktorá sa bude implementovať v tomto projekte je možnosť lokalizácie do slovenského jazyka.

Pri hľadaní vhodnej CA sme identifikovali tri produkty:

1. OpenCA
2. PyCA
3. XCA

5.2 OpenCA

OpenCA Project je snaha vytvoriť robustný, široko použiteľný a verejne dostupný CA systém implementujúci najpoužívanejšie protokoly s plnohodnotnou kryptografickou podporou. OpenCA je založený na mnohých verejne dostupných (ďalej Open Source) projektoch. (OpenLDAP, OpenSSL, Apache Project, Apache mod_ssl)

Vývoj projektu je rozdelený do dvoch hlavných úloh:

- študovanie a zlepšovanie bezpečnostných schém garantujúcich najlepší model použiteľný v CA
- vo vývoji softvéru na jednoduché postavenie a manažovanie CA.

PKI je jedna zo najširšie akceptovaných potrieb budúcnosti. Problém sa objavuje v tom že, čoraz viacej aplikácií môže byt zabezpečených s použitím veci ako sú certifikáty a kľúče, ale je naozaj ťažko postaviť tieto infraštruktúry, ktoré sú okrem toho aj často finančne náročné. Toto bol bod začiatku projektu OpenCA. Cieľ OpenCA je vytvorenie open source dôveryhodného systému, ktorý podporuje širokú verejnosť s dobrým, nie drahým a budúcnosti istým riešeniam pre ich základnú infraštruktúru PK.

5.2.1 Popis CA

OpenCA sa začal v roku 1999. Základná myšlienka pozostávala z troch hlavných častí – PERLovské WWW rozhranie, OpenSSL na podporu šifrovania a databáza. Tento jednoduchý koncept sa zachoval aj v dnešnej podobe projektu. Skoro všetky operácie sa môžu vykonať cez WWW rozhranie. Jediný rozdiel je v tom že, existuje šesť prednastavených WWW rozhraní a ich kombináciou môžeme skutočne vytvoriť ľubovoľné rozhranie aké len chceme. Podpora šifrovania je pomocou kryptografických knižníc z projektu OpenSSL. V databáze sa uchovávajú všetky používateľské objekty ako sú žiadosti na podpísanie certifikátu (CSR – certificate signing request), žiadosti o zrušenie certifikátu (CRR - Certificate Rrevocation Request) a zoznam zrušených certifikátov (CRL – Certificate Rrevocation List).

5.2.2 Poskytované funkcie

V aktuálnom štádiu vývoja, tento projekt poskytuje nasledovne funkcie:

- Verejne rozhranie

- LDAP rozhranie
- RA rozhranie
- CA rozhranie
- SCEP
- OCSP
- IP filtre pre rozhrania
- Prihlásenie do systému na základe hesla
- Prihlásenie do systému na základe certifikátu (vrátené smartcards)
- Prístupové pravá na základe úloh
- Rôzne typy certifikátov
- Zrušenie certifikátu na základe osobného identifikátora
- Zrušenie certifikátu na základe digitálneho podpisu
- Vydávanie zoznamu zrušených certifikátov
- Upozornenie o vypršaniu certifikátu
- Podpora pre väčšinu WWW prehliadačov

OpenCA je navrhnutá ako distribuované rozhranie ktoré umožňuje maximálnu flexibilitu ako pre veľké organizácie tak aj pre malé. OpenCA nie je monoliticky systém ale využíva niekoľko softvérových produktov z open source komunity. Využíva nasledovne produkty:

- Apache
- Mod_ssl
- OpenSSL
- OpenLDAP
- Perl

5.2.3 Požiadavky CA

OpenCA bola testovaná na niekoľkých softvérových architektúrach ale veľkom množstve hardvérových. Zoznam testovaných hardvérových architektúr je zverejnený na webovej stránke projetu. Autori pripomínajú, že OpenCA je možne použiť na ľubovolnom systémektorý

podporuje Apache, mod_ssl, OpenSSL a Perl. Z tohoto vyplýva obmedzenie že OpenCA nemôžeme používať bez istých úprav na systémoch založených na operačnom systéme Windows. Vo všeobecnosti je možné bez problémov spustiť OpenCA na týchto systémoch:

- i386 s Linux, FreeBSD, OpenBSD a NetBSD
- UltraSparc s Solaris 8 a Linux
- PowerPC s AIX

Pri testovaní OpenCA sme zaznamenali ,že používateľské rozhranie je veľmi intuitívne a poskytuje všetky možnosti potrebné na manažovanie CA, vydávanie, podpisovanie certifikátov, generovanie a exportovanie zoznamov zrušených certifikátov, generovanie žiadosti o vydanie alebo podpísanie certifikátu a ďalšie funkcie.

5.3 PyCA

Tento nastroj (pyCA) sa snaží uľahčiť ľuďom postaviť a postaviť vlastnú CA ktorá by spĺňala požiadavky na dostatočne bezpečný proces vydávanie certifikátov. Programový balík pyCA sa tiež snaží znížiť potrebu administratívnych úloh a frustráciu používateľov, poskytovaním pohodlného webového rozhrania používateľom kontaktujúcich certifikačnú autoritu.

5.3.1 Popis CA

Nasledovne systémy sú časťou PKI:

- Klientsky systém - cez ,ktorý používateľ pristupuje službám PKI (mailový klient alebo WWW rozhranie). Používateľ si vytvorí dvojicu kľúčov sám a sám sa o ne aj stará.
- Verejný systém CA (RA) - obsahuje (ukladá) iba verejne certifikačné dáta ako vydané klientske/serverovske certifikáty, CRL a na nim bežia služby ako mail, WWW a/alebo LDAP. Tieto služby umožňujú používateľom prístup k certifikačným dátam. Žiadny privátny kľuč nie je uložený na serveri. Je úlohou zodpovednej osoby (administrátora) je aby zabezpečil systém bežnými prostriedkami (firewally atd.). Služby ktoré poskytuje systém by tiež mali byt zabezpečené napríklad protokolom SSL aby bola zaistená integrita systému.

- Privátny systém CA - kľuč CA by mal byt uložený na izolovanom systéme (nie sieťovom), ktorý je iba prístupný osobám zodpovedným za vydávanie certifikátov. Transport údajov medzi týmto systémom a verejným systémom sa vykonáva za pomoci vymeniteľného úložiska dát. V prípade, že je v SSL podpora pre šifrovacie média je odporúčané aby sa privátny kľuč nachádzal na takomto médiu (média ako napríklad smartcards).

5.3.2 Poskytované funkcie CA

V aktuálnom štádiu vývoja tohto programového balíka sú implementovane nasledovné funkcie:

- Generovanie CA hierarchie certifikátov a CRLs
- Generovanie požiadaviek na certifikát s široko dostupnými webovými prehliadačmi
- Nastroj na vyhľadávanie klientskych certifikátov uložených v OpenSSL databáze
- Stiahnutie klientskych certifikátov/ CRLs s príslušnými MIME typmi
- On-line validácia certifikátov
- Uloženie všetkých certifikátov v LDAP
- Skripty umožňujúce vykonanie procesu certifikácie v izolovanom prostredí (nie sieťovom) s pomocou privátneho kľúča (kľúčov) CA.
- Jednoduchá konfigurácia na základe OpenSSL konfiguračného súbora

5.3.3 Požiadavky

Na spustenie tohoto programového balíka potrebujeme:

- Systém s operačným systémom Unix resp. Linux
- OpenSSL 0.9.4 alebo novšie

Na spustenie CGI-BIN programov potrebujeme

- WWW server s podporou CGI-BIN ako napríklad Apache. Lepšie by bolo použiť webovy server s podporou SSL ako napríklad ApacheSSL alebo Apache mod_ssl
- WWW prehliadač (Netscape Navigator, Mozilla,Opera Microsoft Internet Explorer 4 alebo novší

- Na využitie LDAP na uloženie certifikátov (napríklad OpenLDAP) konfigurovany na uloženie certifikačných atribútov

V čase analýzy aplikácia nebola otestovaná tak že nemožno detailnejšie hovoriť o jej výhodách resp. nevýhodách viazaných konkrétne pre náš projekt. Z informácií ktoré sme získali z dokumentácie. ktorú poskytuje autor tejto aplikácie sme usúdili, že tato aplikácia je vhodným kandidátom pre náš projekt keďže implementuje hlavne požiadavky uvedené v našom projekte.

5.4 XCA

Tato aplikácia je grafické používateľské rozhranie pre OpenSSL, RSA verejne kľúče, certifikáty, podpisovanie certifikátov a zrušenie certifikátov. Kľúče sú zašifrované v databáze.

XCA podporuje okrem štandardných PEM a DER formátov, importovanie a exportovanie PKCS#12 formátov a importovanie PKCS#7 formátov žiadosti o podpísanie certifikátu.

Certifikáty môžu byt vytvorene samopodpisovaním, podpisovaním zo druhej strane (iné CA) alebo podpisovaním PKCS#10 žiadosti. Platnosť certifikátov a X509.v3 extenzii môže byt upravená aby vyhovovala požiadavkám. Implementovaná je stromová štruktúra ktorá zobrazuje vzťahy medzi certifikátmi. Aplikácia sa stará aby sa nevytvorili duplicitne certifikáty overením sériových čísiel pri importovaní alebo vytváraní certifikátov.

Certifikačné šablóny môžu byt použité na uľahčenie procesu vytvárania a podpísania certifikátov a žiadosti. Vydane certifikáty môžu byt zrušené a zoznam zrušených certifikátov môže byt vygenerovaný a exportovaný. Externe zoznamy zrušených certifikátov môžu byt importovane a preskúmané.

Funkcie

Databáza

- Používa sa jeden databázový súbor pre uchovanie všetkých objektov: kľúčov, žiadosti a certifikátov.
- transakcie, obnova a databázové extenzie sú použité na zachovanie konzistentnosti db.

Kľúče

- importovanie a exportovanie PEM, DER, PKCS#8 privátnych a verejných RSA kľúčov

- generovanie kľúčov variabilnej dĺžky.
- Kľúče sú v db zašifrované 3-DES algoritmom.

PKCS#10 Žiadosti

- Importovanie a exportovanie žiadosti.
- Generovanie žiadosti.

X509 Certifikáty

- Generovanie certifikátov samopodpisaných a podpísaných druhou osobou.
- Stromové zobrazenie certifikátov.
- Všetky X509 extenzie sú implementovane.
- Sériové čísla certifikátov sú automaticky inkrementuju.
- Prednastavenie sériového čísla certifikátu
- Exportovanie CRL pre CA certifikáty
- Generovanie žiadosti z certifikátu.
- Importovanie DER, PEM and PKCS#12 formátov.
- Podpisovanie a šifrovanie súborov v PEM PKCS#7 formáte
- Možnosť zvoliť si algoritmus na podpisovanie

Šablóny

- Generovanie prednastavených CA certifikátov, šablóny klientskych a serverovských certifikátov
- Certifikáty a žiadosti môžu používať šablóny

Zoznam zrušených certifikátov

- Importovanie, exportovanie a detailne zobrazenie týchto zoznamov

Existuje okrem verzie pre Unix-Linux aj verzia pre Windows operačné systémy. Výhodou tejto aplikácie je že pri použití na izolovanom systéme predstavuje veľmi bezpečné riešenie na implementáciu CA. Prenos dát medzi takto izolovanom systéme a verejným serverom by sa

uskutočňoval pomocou prenosného uložiska dát. Nevýhodou tohto systému je že neumožňuje interakciu používateľa zo systémom čo znamená že by sa muselo implementovať ďalšie rozhranie ktoré by umožnilo používateľom vytvárať žiadosti o certifikát alebo podpísanie certifikátu, poskytnúť zoznam zrušených certifikátov ako aj žiadosť o zrušenie certifikátu. Okrem toho nevýhoda tohto systému je že ukladá privátne kľúče do databázového súboru čo znamená že pri kompromitácii takéhoto systému sú kompromitovane aj privátne kľúče CA. Lepšie riešenie by bolo keby systém používal privátny kľuč napríklad z pamäťovej karty (smarcard). Ďalšia nevýhoda je nemožnosť lokalizácie aplikácie do slovenského jazyka.

5.5 Zhodnotenie

Nakoniec sme sa rozhodli, že vo fáze implementácie využijeme certifikačnú autoritu na báze projektu OpenCA. Táto certifikačná autorita je vo svete najviac používanou a najrozšírenejšou a spĺňala všetky požiadavky, ktoré sme si na začiatku stanovili. Je podporovaná na cieľovej platforme implementácie a to server v softvérovom štúdiu.

6 Analýza Softvéru na podpisovanie

Našim prvotným cieľom je vytvoriť softvérový produkt, ktorý by bol bezpečný v takej úrovni aby sa na ňom dali vyhotovovať zaručené elektronické podpisy. K tomuto účelu potrebujeme softvér, ktorý by vedel sám sebe z kontrolovať integritu a zaručenosť funkčnosti.

6.1 Samooverovanie integrity aplikácie

Požiadavky na program používaný na podpisovanie (a overenie podpisu) obsahujú aj overenie pravosti programu. Toto overenie je dôležité pre zaistenie dôveryhodnosti programu aj podpísaných dokumentov.

V súčasnosti sa integrita a pravosť programov overuje niekoľkými spôsobmi:

- statická kontrola
- kontrolné súčty (CRC, MD5, SHA,...)
- dynamická kontrola
  - rôzne systémy agentov - kontrolných rutín
  - overovanie alebo oprava kritických častí kódu
  - oblivious hashing

Medzi pomocné techniky zabezpečenia patrí zaznamenávanie pokusov o prienik a zneprehľadnenie kódu (code obfuscation), najmä pre programy písané v interpretovaných jazykoch, Jave, alebo v jazyku symbolických inštrukcií.

6.1.1 Statická kontrola

Statická kontrola sa vyznačuje jednoduchšou implementáciou, ale vo všeobecnosti je najľahšie odstrániteľná - útočník po zmene kódu jednoducho prepočíta kontrolný súčet a zapíše ho na určené miesto. Taktiež sa často dá eliminovať celá kontrola prepísaním alebo odstránením jej kódu z programu. Preto táto kontrola by mala kontrolovať aj samú seba a byť podľa možnosti redundantná. Môže sa kombinovať s proti debugovacími technikami.

6.1.2 Dynamická kontrola

Dynamická kontrola je vykonávaná za behu rôznymi rutinami kontrolujúcich zmeny

programu alebo jeho častí. Oblivious hashing kontroluje dynamické kontexty bežiacej aplikácie a vyznačuje sa tým, že nečíta segment kódu programu. Programy s dynamickou kontrolou sú zložitejšie, pre úspešný útok vyžadujú viacero zmien v kóde.

Z hľadiska vyváženosti zabezpečenia a náročnosti implementácie sú možné nasledovné varianty zabezpečenia:

1. Ak bude bezpečné úložisko údajov poskytovať API, ktoré umožní kontrolu podpisu programu:
   a) Dĺžka a kontrolný súčet programovej časti sa podpíše programom s využitím privátneho kľúča certifikačnej autority. Tieto údaje a podpis budú pripojené k programu.
   b) Kontrolný súčet bude overovaný v bezpečnom úložisku údajov a autenticitu podpisu kontrolovať pomocou verejného kľúča CA, dostupného z úložiska.
   c) Podmienky pre aplikáciu:
      - dôveryhodný (trusted) počítač na vytvorenie kontrolného súčtu programu a jeho podpis,
      - verejný kľúč CA dostupný na bezpečnom úložisku údajov,
      - používateľsky nemodifikovateľné kľúče na úložisku (pre každú zmenu kľúča bude vydané nové úložisko).
2. Ak úložisko údajov nebude poskytovať vyššieuvedenú funkcionalitu:
   a) Dĺžka a kontrolný súčet programovej časti sa podpíše programom s využitím privátneho kľúča certifikačnej autority. Tieto údaje a podpis budú pripojené k programu.
   b) Kontrolný súčet bude program overovať a autenticitu podpisu kontrolovať pomocou verejného kľúča CA, ktorý program získa zo siete alebo bude priložený.
   c) Podmienky pre aplikáciu:
      - dôveryhodný (trusted) počítač na vytvorenie kontrolného súčtu a jeho podpis,
      - dôveryhodný počítač pre beh programu (napr. bez vírusov alebo iného škodlivého kódu),
      - kontrolný súčet aj dĺžka programu budú verejne dostupné, aby si ich používateľ mohol overiť aj externe (mimo programu).
3. Použitie bootovateľnej "živej" distribúcie operačného systému Linux na CD médiu s funkcionalitou obmedzenou na jediný účel - podporu programu. Alternatíva je podobná alternatíve A, s výhodou ochrany programu pred modifikáciou disku (vlastný operačný

systém, read-only médium).

a) Podmienky pre aplikáciu:

- možnosť vyhradiť samostatný počítač len na podpisovanie dokumentov.

Ďalšie možnosti zabezpečenia boli vylúčené z dôvodu vysokej implementačnej náročnosti (systémy agentov) alebo triviálnosti zabezpečenia (nechránený kontrolný súčet).

6.2 Záver analýzy možností pre samooverovací program

Ochrana softvéru pred modifikáciou má vo všetkých troch prípadoch niekoľko slabín, vyplývajúcich z použitia programovateľného počítača na účely spojené s zabezpečením. V programovateľnom počítači sa nedá s absolútnou istotou vylúčiť modifikácia programu ani dát, či už cielená (útok crackera) alebo náhodná (chyba počítačového alebo programového vybavenia, zlomyseľný kód) okrem systémov, kde je zaručená informačná bezpečnosť a táto bezpečnosť je matematicky dokázaná. To, či došlo k modifikácii, môže dôveryhodne overiť len zariadenie, ktoré nie je používateľsky programovateľné, používateľ (útočník) nemá žiadnu možnosť modifikovať alebo inak upravovať programové vybavenie. Ani v jednom vybranom prípade zabezpečenia nie je možné túto podmienku splniť -

- v bode 1 úložisko spolupracuje s externým programom vytvárajúcim kontrolný súčet,
- v bode 2 je celé overenie len softvérové,
- v bode C je možné nahradiť médium za iné (podvrhnuté).

Pri možnostiach daných projektom problém nie je riešiteľný softvérovými prostriedkami s relevantným stupňom ochrany. Preto v ďalšej fáze projektu sme upustili od implementácie takejto ochrany. Implementácia aj tej najjednoduchšej ochrany, o ktorej vieme, že je neúčinná, vyvoláva len falošný pocit bezpečnosti. A práve tento falošný pocit bezpečnosti je nemysliteľný v prípade, že sa pracuje z citlivými informáciami a právnymi záväzkami dokumentov, ktoré sú elektronicky podpísané.

7 Špecifikácia

V nasledujúcich podkapitolách sú v krátkosti opísané požadované vlastnosti na jednotlivé moduly

8 Návrh

8.1 Program na podpisovanie

Účelom navrhovaného programu je zobraziť zadaný textový dokument, vytvoriť jeho kontrolný súčet a podpísať ho s použitím certifikovaného kľúča. Je vyvíjaný ako súčasť infraštruktúry verejného kľúča (public key infrastructure - PKI) pre tímový projekt.

8.1.1 Požiadavky na program:

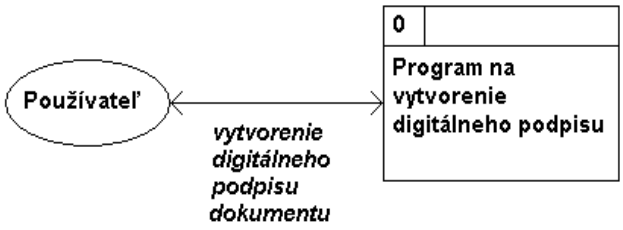
1. načítanie súboru dokumentu (TXT, XML, HTML, RTF) - Táto funkčná požiadavka vyplýva z účelu programu (elektronický podpis) a z platnej legislatívy.Súbor sa načíta z lokálneho disku alebo vymeniteľného média. Po načítaní sa súbor zobrazí v textovej podobe, aby si ho mohol používateľ prezrieť.
2. načítanie privátneho kľúča a certifikátu - Funkčná požiadavka vyplývajúca z účelu programu. Kľúč sa načíta z úložiska.
3. podpísanie súboru - Funkčná požiadavka, ktorá vyplýva z účelu programu. Zo súboru sa vygeneruje kontrolný súčet a ten sa podpíše kľúčom, ktorý je na úložisku.
4. ovládanie len z lokálneho počítača (jednpoužívateľské) - Požiadavka na prevádzku, vyplýva z funkcionality. Podpisovanie by nemalo byť možné ovládať zo vzdialeného počítača využitím akejkoľvek siete.
5. grafické používateľské rozhranie - Požiadavka na výsledok; funkcionalita je dostatočne úzka aj pre program spúšťaný z príkazového riadku, je však vhodné, aby bol program ľahko a intuitívne ovládateľný.
6. multiplatformnosť zdrojového kódu alebo aj samotného programu - Požiadavka na výsledok, nepovinná. Testy funkcionality v laboratóriu prebiehajú pod OS Windows, ale vhodnou voľbou implementačného prostredia je možné docieliť kompilovateľnosť alebo spustiteľnost programu na rôznych platformách.
7. legislatívne požiadavky - zákon 251/2002 Z.z. a iné, viď kapitola č.4, strana 72.

8.1.2 Roly používateľov:

Existuje jediná rola, ktorá je v dokumente označovaná "používateľ".

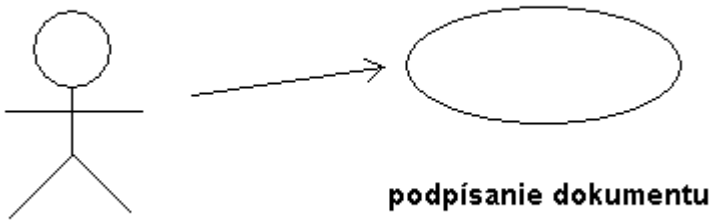
8.1.3 Prípady použitia:

Program je jednoúčelový, t.j. poskytuje funkciu elektronického podpisu pre vybraný dokument. Tento prípad použitia obsahuje postupnosť krokov: načítanie a zobrazenie dokumentu, podpísanie dokumentu, uloženie podpísaného dokumentu.



Obr. 29: Kontextový diagram toku údajov

8.1.4 Funkcie programu

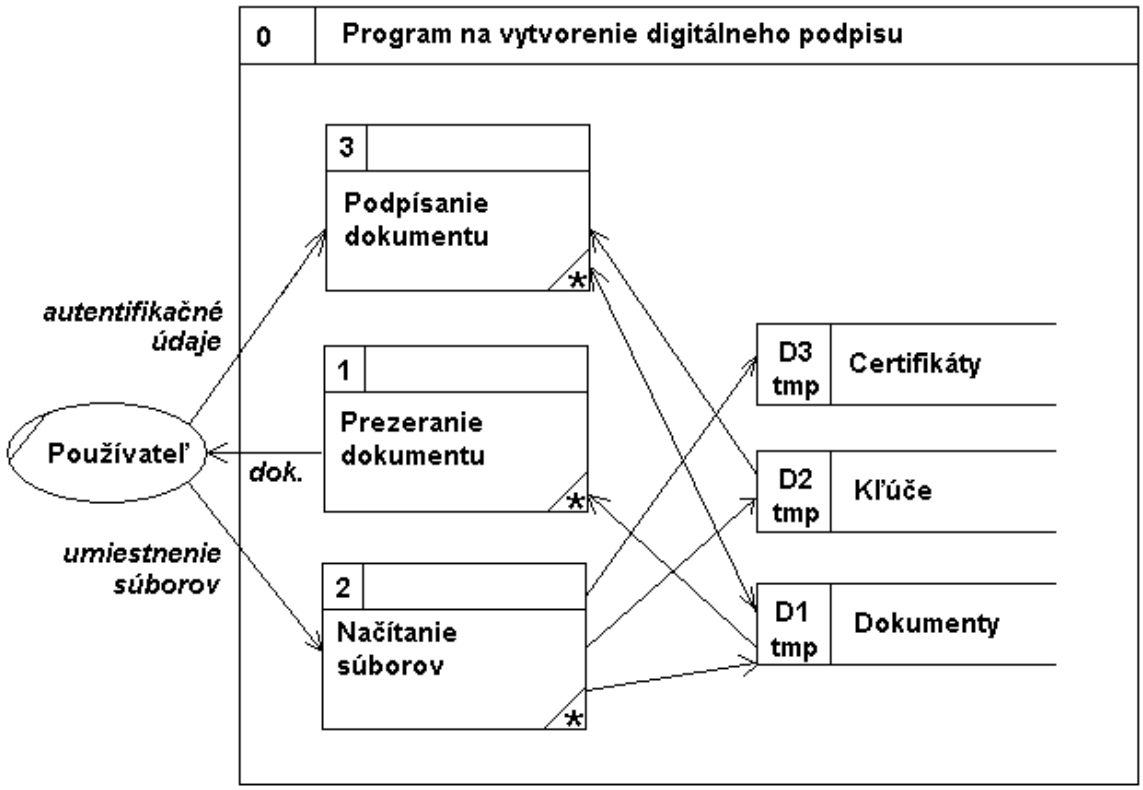


Obr. 30: Use case diagram

Zoznam akcií (funkcií) programu:

- START - spustenie programu.
- MENU - zobrazenie menu.
- READ_DOCUMENT - načítanie dokumentu z média (lokálneho disku alebo výmenného média).
- DISPLAY - zobrazenie načítaného dokumentu v textovej podobe.
- READ_KEY - načítanie súboru privátneho kľúča z média.
- READ_CERTIFICATE - načítanie súboru certifikátu z média.
- SIGN - podpísanie dokumentu privátnym kľúčom.

- WRITE_DOCUMENT - zapísanie dokumentu na médium.
- EXIT - ukončenie programu.



Obr. 31: Diagram toku údajov 1. úrovne

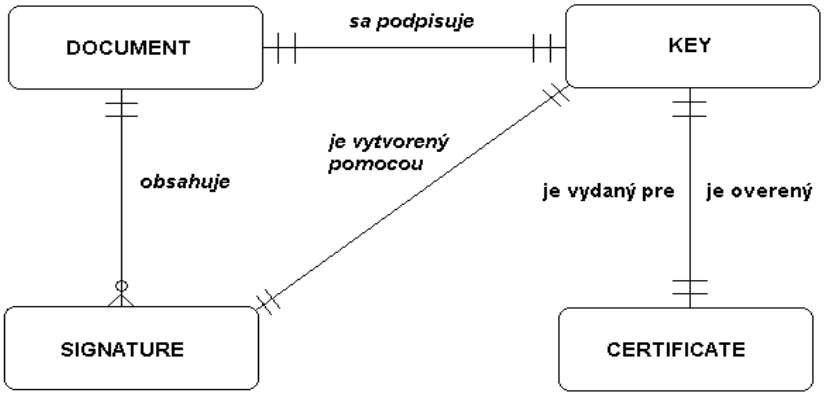
8.1.5 Model údajov

Zoznam objektov programu a ich atribútov:

- DOCUMENT - objekt dokumentu, ktorý sa podpisuje
  - PATH - string, atribút cesty v súborovom systéme, z ktorej sa dokument načíta
  - EMPTY - boolean, určuje, či je dokument prázdny alebo nebol ešte načítaný
  - WRITE_PATH - string, atribút cesty v súborovom systéme, kam sa dokument zapíše
  - CONTENT - obsah dokumentu
  - HASH - kontrolný súčet dokumentu, ktorý sa podpisuje

- SIGNATURE - vytvorený podpis

- KEY - objekt privátneho kľúča, s ktorým sa podpisuje
  - PATH - string, atribút cesty v súborovom systéme, z ktorej sa kľúč načíta
  - EMPTY - boolean, určuje, či je kľúč prázdny alebo nebol ešte načítaný
- CERTIFICATE - objekt certifikátu
  - PATH - string, atribút cesty v súborovom systéme, z ktorej sa certifikát načíta
  - EMPTY - boolean, určuje, či je kľúč prázdny alebo nebol ešte načítaný



Obr. 32: Diagram Modelu Dát

8.1.6 Opis funkcii v pseudokóde

Popis akcií v pseudokóde:

```
MENU =        {
      READ_DOCUMENT.ENABLE(); READ_KEY.ENABLE()
READ_CERTIFICATE.ENABLE(); EXIT.ENABLE();
      IF (!DOCUMENT.IS_EMPTY()
            && !KEY.IS_EMPTY()
            && !CERTIFICATE.IS_EMPTY()) { SIGN.ENABLE(); }
      IF (DOCUMENT.IS_SIGNED() { WRITE.ENABLE(); }
      }
/* ENABLE() je povolenie spustenia danej akcie z menu */

READ_DOCUMENT =    {
            OS.GET_PATH(DOCUMENT);
            OS.READ(DOCUMENT.PATH);
            DISPLAY(DOCUMENT.CONTENT);
            }

READ_KEY =        {
            OS.GET_PATH(KEY);
```

```
            OS.READ(KEY.PATH);
            }

READ_CERTIFICATE =       {
                  OS.GET_PATH(CERTIFICATE);
                  OS.READ(CERTIFICATE.PATH);
                  }

SIGN =       {
      CALCULATE_HASH(DOCUMENT.CONTENT);
      CREATE_SIGNATURE(DOCUMENT.HASH);
      APPEND(DOCUMENT.CONTENT, DOCUMENT.SIGNATURE);
      APPEND(DOCUMENT.CONTENT, DOCUMENT.CERTIFICATE);
      DISPLAY(DOCUMENT.CONTENT);
      WRITE_DOCUMENT;
      }

WRITE_DOCUMENT = {
                  OS.GET_WRITE_PATH(DOCUMENT);
                  OS.WRITE(DOCUMENT.WRITE_PATH);
                  }
```

Pseudoobjekt OS označuje funkcie poskytované operačným systémom

Zoznam použitých skratiek

1. Dostálek, L. a kol.: Velký pruvodce protokoly TCP/IP Bezpecnost, ISBN 80-7226-849-X, Computer Press Praha, 2003
2. NÁRODNÝ BEZPECNOSTNÝ ÚRAD SEKCIA ELEKTRONICKÉHO PODPISU: http://www.nbu.gov.sk/NBU_SEP/default.php
3. Die österreichische Bürgerkarte: http://www.buergerkarte.at/
4. Public-Key Infrastructure (X.509) (pkix): http://www.ietf.org/html.charters/pkix-charter.html
5. The RFC Archive: http://www.rfc-archive.org/getrfc.php?rfc=3280
6. Wikipedia, the free encyclopedia: http://en.wikipedia.org/
7. Fülöp, L.:Bezpecnost výpoctových systémov,Funkcie PKI pre elektronickú podateľnu,
8. Šk.r.: 2003/2004
9. BAUER, H.:CERTIFIKACNÁ AUTORITA,Záverecný projekt,FIIT STU,2004

Zoznam použitých skratiek

Skratka	Význam
CRL	Certificate Revocation Lis – Zoznam zrušených certifikátov
CRR	Certificate Revocation Request – Žiadosť o zrušenie certifikátu
CSR	Certificate Signing Request – Žiadosť o podpísanie certifikátu
LDAP	Lightweight Directory Access Protocol – skupina protokolov na pristupovanie k informačným adresárom.
PKCS	Public Key Cryptography Standards – šifrovacie štandardy verejného kľúča, ktoré boli vytvorene organizáciou RSA Security a sú široko používané v PKI
PKCS#10	Definuje ASN.1 štruktúru žiadosti o podpísanie certifikátu
RA	Registration Authority – autorita zodpovedná na registrovanie a manažovanie žiadostí o vydanie certifikátu
SCEP	Simple Certificate Enrollment Protocol – je protokol vytvorený spoločnosťou Cisco a používa sa na riadenie komunikácie medzi PKI a sieťovými komponentmi ako smerovače a ďalšími VPN komponentmi.
SPKAC	Signed Public Key And Challenge – je štandard na žiadosť o podpísanie
certifikátov	ktorý používa Netscape.
DER	Distinguished Encoding Rules - je binárny ASN.1 štandard na kódovanie dát.
PEM	Privacy-Enhanced Mail - je base64 kódovaná verzia DER formátovaných dát s pridanou hlavičkou a zapätím na prenášanie pomocou emailu.

Príloha A. WSDL špecifikácia SAML rozhrania

```
<?xml version="1.0"?>
```