Slovenská technická univerzita
Fakulta informatiky a informačných technológií
Ilkovičova 3, 812 19 Bratislava

Infraštruktúra PKI a vybavenie pre koncových používateľov

Tímový Projekt

Tím číslo 4 PSS:
Bc. Peter Mulinka
Bc. Radovan Škríb
Bc. Martin Mačica
Bc. Jozef Hamar
Bc. Tomáš Smolek

Rok: 2004 / 2005
Vedúci projektu: Doc. Ing. Ladislav Hudec, Csc.

1. Predslov

Náš život je obklopený informáciami na papieri. A ani si neuvedomujeme ako často tieto informácie potvrdzujeme svojim podpisom. Intuitívne podpíšeme list priateľovi, podpisom potvrdíme doručenie poštovej zásielky, čas príchodu do práce či účasť na seminári. Podpis je našim identifikátorom rovnako ako odtlačok prsta. Vyjadruje súhlas s obsahom dokumentu a je zárukou jeho autenticity. V súčasnom „papierovom svete“ má vlastnoručný podpis zároveň právnu účinnosť. Osoba, ktorá dokument vytvorila a podpísala, je zodpovedná za jeho obsah. Podpisy takýchto osôb nájdeme na všetkých úradných dokumentoch, či už je to rodný list, vysvedčenie alebo lekársky recept. Bez podpisu zodpovednej osoby nie je platná vystavená faktúra v obchodnom svete, nie je platný rozsudok vo svete súdnictva a nie je platná medzinárodná zmluva vo svete politiky. A keďže sa náš „papierový svet“ čoraz viac stáva svetom elektronickým a informácie na papieri sú čoraz častejšie nahrádzané informáciami v elektronickej forme, bolo nevyhnutnosťou vytvoriť i elektronickú podobu podpisu na papieri – elektronický podpis.

Mnohí z nás už dnes využívajú výhody elektronizácie. Napísať list v teple svojej obývačky a ihneď ho aj odoslať prostredníctvom internetu je iste pohodlnejšie a rýchlejšie ako ísť na poštu a postaviť sa do radu pred okienko. Nehovoriac o tom, že osoba, pre ktorú je elektronická informácia určená, ju obdrží takmer v tom istom okamihu ako bola odoslaná. Rovnako aj služby ako Home banking, Internet banking a ďalšie nám umožňujú získavať informácie o účte a vykonávať aktívne bankové transakcie z nášho domova, zrýchľujú prístup k informáciám a k realizácii aktívnych bankových transakcií a šetria naše peniaze, keďže poplatky za elektronicky vykonávané transakcie sú podstatne nižšie než za klasické príkazy na papieri. Rozširovanie podobných služieb iba zvýšuje naše pohodlie, šetrí náš čas a náklady spojené s osobnou návštevou úradov a inštitúcií, znižuje prácnosť a chybovosť pri manipulácii s údajmi, a čo je rovnako dôležité, prispieva i k ochrane našich lesov. Predstavme si, že všetky úradné veci by sme mohli vybavovať prostredníctvom internetu. Žiadne stránkové hodiny, preplnené čakacie haly a pomalé vybavovanie agendy. Nebolo by praktickejšie doma vyplnené daňové priznanie ihneď odoslať internetom ako vyzdvihnúť si formulár na daňovom úrade, doma ho vyplniť a opätovne ho odniesť na úrad? Iste bolo. Má to však jeden háčik. Formulár daňového priznania, rovnako ako všetky úradné dokumenty, vyžaduje náš podpis.

Elektronický podpis je nielen jednou z kľúčových podmienok plnohodnotnej komunikácie prostredníctvom počítačovej siete, najčastejšie prostredníctvom internetu, ale predovšetkým prvoradou podmienkou rozvoja elektronického obchodu a podnikania. Dnes už nie je ničím nezvyčajným objednať si súkromne želaný tovar za pomoci internetu. Obchodná korešpondencia firiem sa však väčšinou nezaobíde bez podpisu zodpovednej osoby a pečiatky firmy. Bolo teda nevyhnutnosťou vytvoriť elektronickú alternatívu podpisu, ktorá nahradí klasický podpis i pečiatku, aby sa už obchodná korešpondencia nemusela pohybovať „fyzicky“, na papieri.

Mnohé firmy nekomunikujú prostredníctvom internetu iba s obchodnými partnermi, ale i so svojimi zamestnancami vykonávajúcimi prácu doma. Aj keď to v našom prostredí znie ešte futuristicky, teleworking – metóda práce z prostredia domova za pomoci dnes už bežne dostupných komunikačných prostriedkov, vo svete nie je ničím nezvyčajným. Firmy nemusia vynakladať veľké sumy na zriaďovanie svojich pobočiek, nemajú náklady za prenájom kancelárií, spotrebovanú energiu, stravovanie zamestnancov. A zamestnanec je ušetrený skorého vstávania a stresu spojeného s odchodom do práce. Teleworking sa samozrejme nehodí pre množstvo povolaní, je zrejmé, že budova sa nepostaví, ak bude stavbár sedieť doma, ale architekt tú budovu navrhnúť doma môže. Vo všeobecnosti, akákoľvek práca, pri ktorej sa pracuje s počítačom, telefónom či internetom, je dnes už vhodná na prevedenie do domáceho prostredia. Najlepším príkladom sú programátori či iní tvoriví pracovníci firiem, od ktorých sa nevyžaduje osobná účasť v kancelárii. India, štát s druhým najväčším počtom programátorov na svete, poskytuje služby tejto kvalifikovanej pracovnej sily americkým softvérovým spoločnostiam. Tým je jedno, že ich pracovníci sú vzdialení niekoľko tisíc kilomentrov, podstatný je výsledok, ktorým je kvalitný kód. Príkladov, samozrejme, existuje viac – administrátori webových serverov, výskumní pracovníci či telefonickí konzultanti, to všetko sú povolania, ktoré je možné vykonávať v rámci domácej kancelárie. Dôkazom, že teleworking môže úspešne fungovať, sú i Nemecko a Veľká Británia, kde takouto formou pracuje dnes už 6 percent ľudí v produktívnom veku. Rozvoj elektronického podpisu a jeho legislatívna úprava umožňujú zamestnávateľovi a zamestnancovi nielen bezpečnú a autentifikovanú komunikáciu chrániacu záujmy firmy a výsledky zamestnancovej práce, ale zároveň i rozšírenie možností zamestnania pracovníkov ďalších odborov touto progresívnou pracovnou metódou.

Elektronický podpis je teda technika, spôsob, ktorým sa podpisujú elektronické dokumenty. Jeho vývoj pramení z potreby podpisovať najrôznejšie počítačové dokumenty a elektronické poštové správy priamo v ich elektronickej forme, čo eliminuje potrebu dať dokument na papier kvôli ručnému podpisu. Potrebám spoločnosti, čoraz viac závislej na elektronickej informácii, sa prispôsobila i legislatíva, ktorá stanovuje, za akých podmienok je elektronický podpis právnym aktom.

Právnu formu elektronického podpisu v SR ustanovuje zákon o elektronickom podpise a o zmene a doplnení niektorých zákonov č. 215/2002 Zb. schválený NR SR 15. marca 2002. Prijatím zákona o EP a nadväzujúcich vyhlášok bol v podstate elektronický dokument uznaný za rovnocenný s papierovým. Legislatívna úprava elektronického podpisu sa opiera o Smernicu EÚ č. 1999/93/EC z decembra roku 1999. Na to, aby bolo možné používať elektronický podpis v každom obchodnom či neobchodnom styku, je potrebné vydanie tzv. zaručeného elektronického podpisu, ktorý musí spĺňať kritériá dané v § 4 zákona č. 215/2002 Zb. Takýto elektronický podpis musí zaručovať:

- **Autentifikáciu.** Ide tu o rozpoznanie a jednoznačnú identifikáciu osoby podpisujúcej určitý dokument. To znamená, že vďaka elektronickému podpisu má osoba, ktorej je dokument určený, istotu, že odosielateľ je skutočne tá osoba, za ktorú sa vydáva. Ak má podpis mať nejakú váhu, musí byť vytvorený takým spôsobom, ktorý nie je možné zmeniť. A hoci je ručný podpis jedinečným pre každého z nás, predsa sa vyskytujú prípady, keď dochádza k jeho zneužitiu. V prípade sporných situácií overuje pravdivosť klasického podpisu znalec – grafológ, ale i on je len človek, ktorý sa môže mýliť. Napodobiť alebo falšovať elektronický podpis je oveľa ťažšie ako ručne písaný podpis, ak dokonca nie nemožné. Je totiž chránený veľmi zložitým šifrovaním - jedinečnou kombináciou znakov – jednotiek a núl. Vďaka tomu výsledkom overovania elektronického podpisu je vždy výrok „áno“ alebo „nie“ so 100 % istotou.
- **Integritu.** Integrita správy zaručuje to, že poslaný dokument sa dostal k adresátovi v nepozmenenej podobe, t.j. že to, čo odosielateľ odoslal, je skutočne to, čo prijímateľ dostal. Prednosťou elektronického podpisu v porovnaní s klasickým je i to, že elektronický podpis je závislý od obsahu dokumentu, ktorý podpisujeme, je teda zakaždým inou kombináciou jednotiek a núl. To znamená, že ak by došlo k zmene obsahu podpísaného dokumentu nejakou treťou osobou alebo poruchou pri prenose podpísaného dokumentu po internete, pri overení elektronického podpisu, sa to hneď

prejaví. Elektronický podpis teda zaručuje, že pri prenose nedošlo k zmene obsahu správy. Okrem toho elektronickým podpisom nie je možné podpísať prázdny dokument („prázdny papier“) a keďže závisí od obsahu podpísaného dokumentu, je neprenosný na iný dokument.

- **Nepopierateľnosť.** Nepopierateľnosť znemožňuje podpisujúcemu tvrdiť, že podpis nie je jeho a že to nebol on, kto daný dokument podpísal a odoslal. To znamená, že odosielateľ svojím podpisom súhlasí s obsahom dokumentu, berie na seba právnu zodpovednosť za obsah zaslaného dokumentu a neskôr nemôže poprieť, že daný dokument poslal on (napr. objednávku na nejaký tovar).

Pre bežného používateľa je vytvorenie elektronického podpisu veľmi jednoduché. Jeho podstata vychádza z existencie dvojice kľúčov – súkromného a verejného. Súkromný kľúč je iba jeden a je našim výlučným vlastníctvom, kým verejný kľúč môžeme poskytnúť viacerým osobám, s ktorými sme v elektronickom styku (priateľovi, banke, účtovníkovi, obchodnému partnerovi). Svojim súkromným kľúčom správu podpíšeme, t.j. pretransformujeme do nečitateľnej podoby jednotiek a núl. Vďaka verejnému kľúču, ktorý je akýmsi dvojčaťom súkromného kľúča na rozšifrovanie správy, si adresovaná osoba môže správu prečítať a zároveň sa uistiť, že podpísaný dokument sme naozaj poslali my a obsah dokumentu počas jeho prenosu nebol pozmenený.

Jediným rizikom, ktoré v prípade elektronického podpisu môže hroziť, je odcudzenie a zneužitie súkromného kľúča. Nebezpečenstvo však nie je také veľké akoby sa mohlo zdať, ako potvrdzujú i skúsenosti s elektronickým bankovníctvom od jeho počiatkov u nás v roku 1995. Po takmer desiatich rokoch Home bankingu nebolo zaznamenané ani jedno zneužitie konta klientov využívajúcich túto službu.

Výber úrovne bezpečnosti si klient volí sám na základe náležitej osvety a zváženia miery rizika. Starostlivosť o súkromný kľúč je hlavnou povinnosťou majiteľa takéhoto kľúča, rovnako ako zodpovednosť za škodu spôsobenú porušením tejto povinnosti. Nebezpečenstvo jeho odcudzenia je rozhodne oveľa menšie ako nebezpečenstvo odcudzenia našej peňaženky či osobných dokladov pri nákupoch na preplnenom trhovisku.

Elektronizácia a spolu s ňou aj elektronický podpis sa budú rýchle rozvíjať. V rámci medzinárodného spoločenstva budú rásť tlaky na normalizáciu a štandardizáciu v snahe

zabezpečiť kompatibilitu použitia elektronického podpisu v čo najväčšom rozsahu. Je iba otázkou času, kedy bude vybudovaná infraštruktúra verejného kľúča a elektronický podpis sa stane súčasťou našej doby podobne ako platobné karty a mobilné telefóny. A hoci sme zvyknutí akosi viac dôverovať informácii na papieri než informácii v elektronickej forme, čoskoro prídeme nato, že podobne, ako je mobilný telefón výhodnou alternatívou pevnej linky a platobná karta akceptovanou variantou platby v hotovosti, i elektronický podpis je rovnako dobrý ako jeho zaužívaný starší brat vytvorený perom a atramentom. Vlastne ešte lepší.

2. Úvod

2.1. Slovník pojmov

Rozumný čas

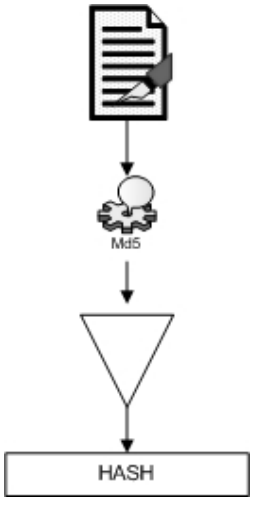
Bežný počítač

Dostupná architektúra

Útok hrubou silou (Brutal Force Attack - BFA)

2.2. Elektronický odtlačok dokumentu - Hash

V roku 1976 vyvolali u odbornej verejnosti mierny rozruch páni Diffie a Hellman svojim tvrdením, že „ak vieme šifrovať, nemusíme nutne vedieť aj dešifrovať“. V tej dobe bol hlavný smer vývoja v zdokonaľovaní klasických šifier a táto myšlienka bola niečím novým. O niečo neskôr začali vznikať prvé šifry založené na tomto princípe.



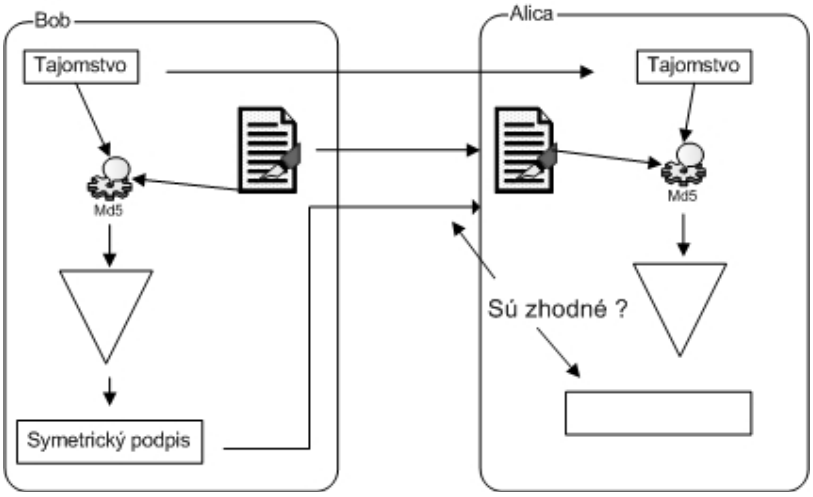
Obr. 2.1
princíp kontrolného súčtu

Elektronický odtlačok dokumentu je voľný preklad názvu „Message digest“, alebo Hash[heš]. V ďalšom texte bude pre tento mechanizmus jednotne používaný spisovne správny názov kontrolný súčet, aj keď by používanie hovorového hash bolo možno technicky vhodnejšie.

Kontrolný súčet je vlastne jednosmerná funkcia, ktorá zo správy ľubovoľnej dĺžky vygeneruje konštantne dlhý reťazec bitov. Najpoužívanejšie dva algoritmy vytvárajú kontrolné súčty o dĺžke 128 a 160 bitov. To však znamená že musí existovať viac dokumentov, ktoré budú mať rovnaký kontrolný súčet. Počet dokumentov s rôznym kontrolným súčtom je však pri 128 bitovej dĺžke 38 miestne číslo v dekadickej sústave, pri 160 bitovom je to 48 miestne číslo. To naznačuje, že ide o dostatočnú rezervu. Existuje názor, že za celú históriu ľudstva nevzniknú normálnou cestou dva dokumenty s rovnakým kontrolným súčtom. Keďže ide o jednosmernú funkciu, neexistuje inverzná funkcia. Je veľmi náročné nájsť ku kontrolnému súčtu originálny text. Podľa niekoho dokonca úplne nemožné.

My však budeme opatrnejší, pretože história nás už dostatočne poučila a to, čo je dnes nemožné dešifrovať na dostupných architektúrach, môže o rok zvládnuť bežný počítač za využitia najnovších matematických poznatkov behom krátkeho času.

Je viacero požiadaviek na kontrolný súčet. Ako na matematickú podstatu, tak na algoritmus výpočtu. Kontrolný súčet by mal byť dostatočne rýchli, aby ho bolo možné počítať aj na bežnom počítači v rozumnom čase, na druhej strane však nie moc, aby útočníkovi sťažil útok hrubou silou. Ďalšou dôležitou požiadavkou je, aby sa všeobecne pri malej zmene vstupu dosiahla veľká zmena na výstupe. To znamená, že ak napríklad v jednostranovom dokumente zmeníme len meno nejakej osoby, prípadne čo i len jednu cifru v určitom čísle(môže ísť o peňažnú sumu), potrebujeme, aby sa výsledný kontrolný súčet oproti pôvodnému dostatočne zmenil. Dostatočne je relatívny pojem. Keď kontrolný súčet kontroluje program, stačí, aby sa zmenil jediný bit a tento program okamžite zmenu zistí. Keby sme ho však kontrolovali sami, mohli by sme jednoducho prehliadnuť zmenu jedného znaku(prípadne šikovne zamenené dva opticky sa podobajúce znaky: B-8, 1-l, atď.). Preto by sa mal kontrolný súčet pri malej zmene dokumentu zmeniť dostatočne veľa.



Obr. 2.2 Kontrola integrity prijatej správy

Mohlo by sa zdať, že využitie kontrolných súčtov je malé. Nemá veľký význam šifrovať niečo, keď nevieme získať späť pôvodný text. Avšak práve na tomto princípe sú postavené všetky použitia kontrolného súčtu. Typickým príkladom je ukladanie hesiel používateľov v systéme. V skutočnosti v systéme nie sú uložené heslá používateľov, ale len ich kontrolné súčty. Používateľ najskôr zadá svoje meno, potom heslo. Z hesla sa vypočíta

kontrolný súčet, ktorý sa potom porovná s kontrolným súčtom uloženým v systéme. Toto zabraňuje zneužitiu hesla. Samotné kontrolné súčty hesiel sú samozrejme starostlivo chránené. Ich prípadné odcudzenie útočníkovi však aj tak veľa neprezradí, pretože z nich nevie získať pôvodné heslá. Ďalšie využitie nájde kontrolný súčet pri prenášaní správ, keď potrebujeme zaručiť, že správa nebola cestou modifikovaná. Odosielateľ - nazvime ho Alica - vypočíta zo správy kontrolný súčet a priloží ho k správe. Prijímateľ - pre zmenu Bob - zo správy vypočíta znova kontrolný súčet a navzájom ich porovná. Ak sú rovnaké, má záruku, že správu od odoslania nikto nemodifikoval. Nemá však záruku, že správu odoslala Alica, ktorá je pod ňou podpísaná, alebo niekto iný. Alica s Bobom majú však ešte ďalšiu možnosť: dohodnúť sa na nejakom spoločnom tajomstve (ľubovoľný text) a pri odosielaní správy vypočítať kontrolný súčet zo správy s priloženým tajomstvom. Bob teda priloží tajomstvo k správe, vypočíta kontrolný súčet, a Alici pošle správu spolu s kontrolným súčtom. Alica opäť priloží ku správe tajomstvo, vypočíta kontrolný súčet porovná ho s prijatým kontrolným súčtom od Boba. Správu teda mohol poslať len Bob. Tento mechanizmus sa zvykne nazývať aj symetrický podpis. Keby však Alica chcela, mohla by napísať falošnú správu, priložiť k nej tajomstvo a tvrdiť, že ju dostala od Boba. Neexistoval by spôsob ako dokázať, že správu poslal Bob, alebo Alica. Posledné dva problémy budú riešené v niektorej z nasledujúcich kapitol, kde budú rozoberané mechanizmy autentifikácie.

Dnes sa používajú v praxi najčastejšie dva algoritmy: MD5 a SHA-1. MD5 je skratka z Message Digest 5 a jeho výsledkom je kontrolný súčet o dĺžke 128 bitov. Výstupom Secure Hash Algorithm – 1 je 160 bitov a je mierne pomalší od MD5. Táto vlastnosť ho robí relatívne odolnejším voči útoku hrubou silou.

Kontrolný súčet je teda jednosmerná funkcia, ktorá sa vypočíta z ľubovoľne dlhej správy. Jeho vlastnosti sú konštantná dĺžka, rýchly výpočet, dostatočná zmena výstupu pri zmene vstupu a vysoká výpočtová zložitosť pri hľadaní pôvodného textu. Kontrolný súčet nám zaručuje integritu správy, t.j. že správa nebola modifikovaná.

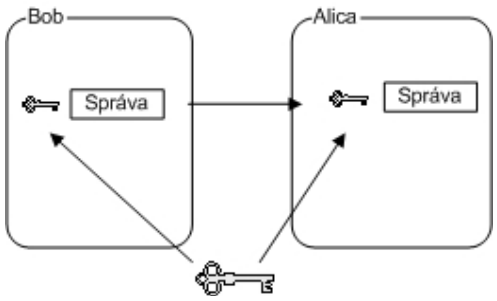
2.3. Symetrické šifrovanie

Keď sa spomenie slovo šifrovanie, ľudia si najčastejšie vybavia symetrické šifrovanie. Symetrická šifra je asi najreprezetnatívnejšia šifra spomedzi známych metód šifrovania.

Správa sa zašifruje šifrovacím algoritmom za pomoci tajného kľúča. Zašifrovaný text sa prenesie k adresátovi, ktorý ho za pomoci dešifrovacieho algoritmu a toho istého tajného

kľúča dešifruje. Na šifrovanie aj dešifrovanie sa teda používa ten istý kľúč. V ideálnom prípade nám tento spôsob čiastočne zabezpečuje aj to, čo chýbalo kontrolnému súčtu – autenticitu. Keďže kľúč je tajný, správu mohla odoslať iba Alica s Bobom. Ak teda Alica obdrží zašifrovanú správu, má istotu, že ju odoslal Bob.

Vzniká tu však problém: Alica aj Bob musia poznať tajný kľúč. Akékoľvek zaslanie skrýva riziko odchytenia a podvrhnutia. Keby napríklad chcela Alica poslať tajný kľúč Bobovi normálnymi prenosovými cestami, mohla by tento kľúč odchytiť tretia osoba - Oskar. Alica s Bobom by si mysleli, že je všetko v poriadku a začali by si posielať zašifrované správy. Oskar by však vedel tieto správy nielen čítať, ale vedel by dokonca aj generovať falošné správy a tým pádom aj modifikovať posielané. Mohol by poslať Bobovi správu, podpísať sa pod ňu ako Alica a Bob by nemal žiadny mechanizmus, ako si overiť, že správu poslala naozaj Alica. Takže opäť nie je autenticita dokonale zabezpečená.



Obr. 2-3 Symetrické šifrovanie

Jediný možný spôsob ako zabrániť tomu, aby sa kľúč dostal do nepovolaných rúk bez znalosti iných mechanizmov, je osobná výmena kľúča. Ani to však nerieši problém, keď Alica zašifruje správu a bude Bobovi tvrdiť, že ju dostala od neho.

Symetrické šifrovanie sa môže výhodne použiť pri zabránení nepovolaným osobám prístupu k údajom. Typický príklad je ukladanie súkromných dát na disku počítača. Keďže jediný, kto musí poznať kľúč je majiteľ dát, nehrozí odcudzenie kľúča z dôvodu jeho zasielania poštou, či inými komunikačnými kanálmi.

Medzi najznámejšie symetrické šifry patria DES, 3DES, IDEA, GHOST, BLOWFISH, AES a niektoré ďalšie. Vo všeobecnosti je najrozšírenejším algoritmus DES (Data Encryption Standard), ktorý používa 56 bitový kľúč. Všetky uvedené šifry sú tzv. blokové šifry. To znamená, že vstupný text je rozdelený na bloky, tie sa zašifrujú a výsledok sa poskladá z jednotlivých zašifrovaných blokov. Najčastejšia dĺžka bloku je 64 bitov, teda 8

bajtov. Algoritmus DES je však veľmi starý a je viac známych spôsobov, ako zmenšiť bezpečnosť ním šifrovaného textu. Jeho nástupcom je štandard AES (Advanced Encryption Standard) s dĺžkami kľúčov 128, 192 a 256 bitov.

Jeden zo známych útokov na blokové šifry spočíva v poprehadzovaní zašifrovaných blokov tak, aby výsledok vyhovoval útočníkovi. Zámenou dvoch blokov obsahujúcich napríklad peňažnú čiastku v zašifrovanom platobnom príkaze by bolo možné dostať inú sumu. A to všetko bez nutnosti dešifrovanie správy. Aby sa predišlo tomuto typu útokov, je možné pri šifrovaní vziať do úvahy poradie vstupných blokov. Vtedy hovoríme o móde blokovej šifry. Pri šifrovaní bloku sa použije aj predchádzajúci blok, čím dosiahneme vzájomnú závislosť po sebe idúcich blokov.

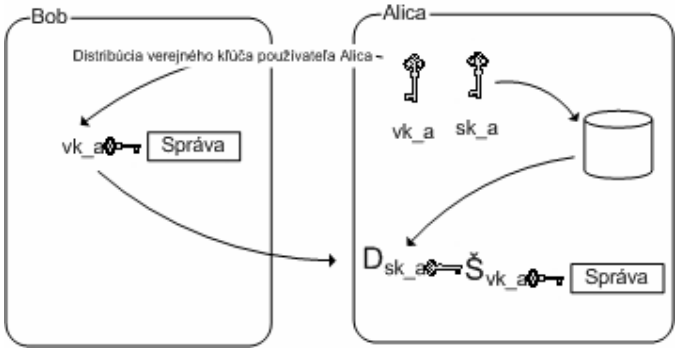
Symetrické šifrovanie je rýchle, na šifrovanie aj dešifrovanie sa používa ten istý kľúč. Za istých okolností je možné dosiahnuť autentifikáciu, t.j. jednoznačne identifikovať odosielateľa správy. Problémom pri symetrickom šifrovaní použitom na výmenu informácii je distribúcia kľúča.

2.4. Asymetrické šifrovanie

Na rozdiel od symetrického šifrovania s jedným kľúčom pri asymetrickom existuje kľúčový pár súkromného a verejného kľúča. Kým pri symetrickom šifrovaní slúžil tajný kľúč aj na šifrovanie, aj na dešifrovanie, pri asymetrickom šifrovaní sú tieto dva kľúče navzájom inverzné. Ak správu zašifrujeme verejným kľúčom, dešifrovať ju je možné len za pomoci znalosti súkromného kľúča. A naopak, správu zašifrovanú súkromným kľúčom je možné dešifrovať len kľúčom verejným. Súkromný kľúč je výhradným majetkom dotyčnej osoby, verejný kľúč je k dispozícii každému, kto o neho prejaví záujem. Z matematického hľadiska sú súkromný a verejný kľúč zameniteľné. Zo znalosti jedného je veľmi náročné vygenerovať druhý.

Keďže po zašifrovaní správy súkromným kľúčom Alice nie je inak ako jej verejným kľúčom možné správu dešifrovať a za podmienky, že Alicin súkromný kľúč vlastní len Alica, je možné jednoznačne identifikovať odosielateľa, ktorým je Alica. Z toho vyplýva, že Alica si musí dávať o to väčší pozor na svoj súkromný kľúč, pretože po jeho odcudzení by sa mohol niekto vydávať za ňu, a Alica by nemala možnosť dokázať opak.

Alica s Bobom si teda každý vygenerujú dvojicu kľúčov. Súkromný si starostlivo odložia, a verejný si dajú navzájom k dispozícii. Keď bude chcieť Alica poslať správu Bobovi, zašifruje ju jeho verejným kľúčom a pošle mu ju. Nikto iný okrem Boba nebude schopný ju rozlúštiť. Bob svoju odpoveď zašifruje verejným kľúčom Alice.



Obr. 2.4 asymetrické šifrovanie

Opäť je tu však problém s distribúciou verejného kľúča. Počas posielania verejných kľúčov ich môže podobne ako pri symetrickom šifrovaní odchytiť Oskar. Teraz však neostane len pri odpočúvaní, ale vygeneruje si dvojicu kľúčov: súkromný a verejný. Verejný pošle Alici pod hlavičkou Bobovho verejného kľúča, a Bobovi pod hlavičkou Alicinho verejného kľúča. Ak bude teda Alica posielať správu Bobovi, zašifruje ju nevedomky verejným kľúčom Oskara. Ten ju cestou odchytí a dešifruje svojim súkromným kľúčom. Principiálne mu nič nebráni túto správu modifikovať. Výsledok potom zašifruje Bobovým pravým verejným kľúčom a pošle mu ju. Bob samozrejme nemusí veriť, že správa pochádza skutočne od Alice, hlavne keď ju mohol zašifrovať jeho verejným kľúčom hocikto. Keď však vedie dialóg s Alicou, je veľmi pravdepodobné, že to bude ona.

Celý problém teda spočíva v identifikovaní skutočného vlastníka verejného kľúča, teda v odhalení podvrhnutého verejného kľúča. Toto možno riešiť uverejňovaním verejného kľúča na rôznych verejných miestach, kde je málo pravdepodobné jeho podvrhnutie. Príkladom môžu byť tlačené periodiká, zabezpečené webové stránky atď. Stále však ostáva najbezpečnejšou cestou osobné predanie verejného kľúča.

V praxi sa však málokedy používa asymetrické šifrovanie na šifrovanú komunikáciu. Oveľa bežnejšie je, že si Alica s Bobom pomocou asymetrického šifrovania len vymenia tajný kľúč pre symetrické šifrovanie a všetka komunikácia už prebieha šifrovaná symetricky,

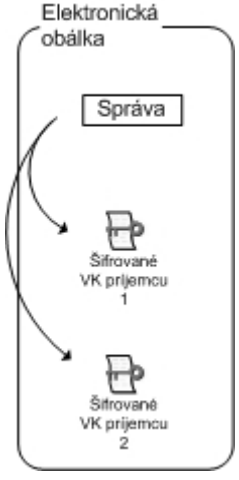
pretože symetrické šifrovanie je oveľa rýchlejšie ako asymetrické. Tento postup sa tiež nazýva Diffie-Hellmanov algoritmus.

Najčastejšie používanými asymetrickými algoritmami sú RSA (Riven, Shamir, Adelman) DSA a ECC. Algoritmus RSA používa dĺžky kľúčov 512, 1024, 2048 a 4096 bitov. Dĺžka kľúča 512 sa považuje za dostatočnú, preto sa častejšie používa 1024 bitov. Ako je vidno, dĺžka kľúča je o jeden rád vyššia ako pri symetrických šifrách, čo je aj dôvodom prečo je RSA pomalší ako symetrické algoritmy. Počítanie s tak veľkými číslami vyžaduje vlastnú množinu algoritmov, keďže sa nedajú použiť štandardné funkcie vyšších programovacích jazykov. V poslednom čase sa presadzuje algoritmus ECC, ktorý je založený na princípe eliptických kriviek a je zaujímavý predovšetkým z pohľadu rýchlosti. Z hľadiska bezpečnosti sa dĺžka kľúča 1024 bitov u RSA približne rovná 160 bitom pri ECC. Avšak kvôli rozšírenosti RSA je jeho prípadné vytlačenie algoritmom ECC ešte v nedohľadne, ak vôbec.

Asymetrické šifry používajú dva kľúče. Verejný a súkromný. Z hľadiska šifrovania sú spolu zviazané: čo sa zašifruje jedným, dá sa dešifrovať len druhým. Zo znalosti jedného kľúča nemožno odvodiť druhý kľúč. Asymetrické šifrovanie zabezpečuje autenticitu, t.j. ak niečo dokážeme dešifrovať verejným kľúčom nejakej osoby, máme záruku, že to šifrovala ona a dokument nie je podvrhnutý.

2.5. Elektronická obálka

Elektronická obálka rieši podobne ako Diffie-Hellmanov algoritmus problém pomalého asymetrického šifrovania. Správa je šifrovaná symetrickým algoritmom za pomoci náhodného tajného kľúča. K takto zašifrovanej správe sa pribalia dodatočné dáta zašifrované verejným kľúčom prijímateľa. Tieto dodatočné dáta obsahujú okrem iného použitý symetrický algoritmus a náhodný tajný kľúč potrebný na rozšifrovanie správy. Výhoda spočíva v rýchlosti, a tiež v tom, že dáta stačí v prípade viacnásobných prijímateľov šifrovať len jeden krát. Stačí pre každého prijímateľa zašifrovať dodatočné informácie prislúchajúcim verejným kľúčom.



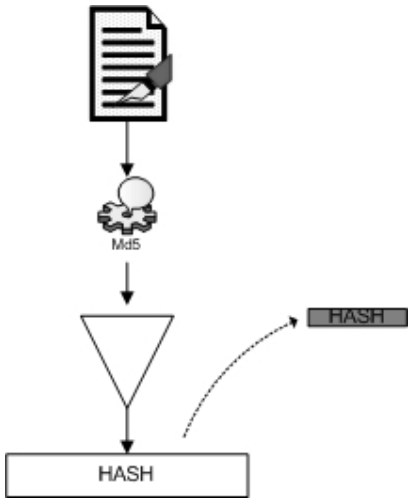
Obr. 2-5 Elektronická obálka

2.6. Elektronický podpis

Elektronický podpis slúži v prvom rade ako mechanizmus kontroly autenticity a integrity dokumentu. Pri rôznych činnostiach a komunikácií je nutné zabezpečiť tieto dve veci skôr ako samotné utajenie.

Na zabezpečenie integrity sa využíva kontrolný súčet. Tento sa vypočíta z dokumentu, ktorý chceme elektronicky podpísať. Keďže však nechceme, aby niekto cestou zmenil dokument a vypočítal z neho nový kontrolný súčet, tak nami vypočítaný kontrolný súčet zašifrujeme našim privátnym kľúčom. Tým dosiahneme autenticitu. Takto zašifrovaný kontrolný súčet sa priloží k dokumentu a nazýva sa elektronický podpis. Teraz si môže ktokoľvek prečítať dokument, vypočítať si z neho vlastný kontrolný súčet a porovnať ho s tým, ktorý dostane rozšifrovaním nášho – keďže náš verejný kľúč mu je k dispozícií. Keby porovnanie vrátilo negatívny výsledok, máme istotu, že niekto cestou zmenil dokument. V opačnom prípade je dokument zaručene pravý (nepozmenený) a zaručene od nás.

Teraz je ešte dôležitejšie, aby bol súkromný kľúč dobre strážený. Jeho zneužitie môže mať vážne následky. V krajinách kde je elektronický podpis rovný normálnemu podpisu môže prípadný útočník s ukradnutým súkromným kľúčom dotyčnej osoby podpísať prakticky akýkoľvek dokument.



Obr. 2-6 Elektronický podpis

2.7. Certifikát

Pri elektronickom podpise je však rovnaký problém s distribúciou verejného kľúča, ako pri asymetrickom šifrovaní. Bob nemusí mať istotu, že verejný kľúč, ktorý obdržal od Alice, a ktorým bude dešifrovať kontrolný súčet dokumentu, patrí naozaj Alici. Tento problém už definitívne riešia certifikáty.

Alica si vygeneruje asymetrickú dvojicu kľúčov a navštívi tzv. certifikačnú autoritu. Vyplní „žiadosť o certifikát“, kde vypíše svoje identifikačné údaje, a túto žiadosť digitálne podpíše svojim súkromným kľúčom. Tým súčastne dokáže existenciu a hlavne vlastníctvo súkromného kľúča. Certifikačná autorita následne vydá Alici certifikát verejného kľúča. Certifikát obsahuje údaje o Alici, údaje o certifikačnej autorite, ktorá certifikát vystavila a Alicin verejný kľúč. Táto štruktúra je elektronicky podpísaná súkromným kľúčom certifikačnej autority. Ešte treba pripomenúť, že vzhľadom na to, že certifikačná autorita svojim podpisom potvrdzuje pravosť všetkých sebou vydaných certifikátov, je treba jej súkromný kľúč chrániť s najväčšou zodpovednosťou. Alica potom Bobovi nepošle svoj verejný kľúč, ale certifikát verejného kľúča. Bob si môže overiť verejný kľúč certifikačnej autority u nej samotnej. Verejný kľúč certifikačnej autority bude Bobovi určite viac k dispozícií ako Alicin. Certifikačná autorita sa aj sama stará o to, aby jej verejný kľúč bol verejne dostupný. Môže byť vydaný v tlačených periodikách, kde sa výrazne znižuje možnosť falzifikácie, alebo podvrhnutia.

3. Autentifikácia

3.1. Identifikačné technológie

V tejto kapitole opíšeme primárne technológie na zistenie totožnosti užívateľa, koncového používateľa alebo obidvoch.

Autentifikácia je mimoriadne kritická časť, pretože všetko je založené na otázke „kto si?“. V množstve hromadných sietí by sme neudelili oprávnený prístup k špeciálnym častiam siete skôr, než zriadime službu na zistenie (totožnosti) osoby, ktorá skúša získať prístup k súkromným prostriedkom. Spoľahlivá autentifikačná metóda je závislá na použitej technológii.

Autentifikačné metódy môžeme voľne kategorizovať na tie, kde je miestne riadenie, alebo kde sa obstaráva autentifikačné overenie cez dôvernú tretiu stranu.

Potenciálna slabosť niektorých autentifikačných metód je dôvera (komu dôverujeme). Mnoho autentifikačných metód sa spolieha na tretiu stranu k overeniu niekoho totožnosti. Sila overenia ja závislá na sile autentifikácie. Keď použijeme tretiu stranu k autentifikácii koncového užívateľa alebo zariadenia, opýtame sa sami seba: „Aká je pravdepodobnosť, že tretia strana, s ktorou počítame na poskytnutie autentifikačného overenia je kompromisom?“.

3.2. Ochrana heslom

Hoci sú heslá často používané ako kontrola pre autentifikáciu užívateľa alebo zariadení, môžu byť odhalené, ak sú ľahko uhádnuteľné, ak nie sú dostatočne často menené a ak sú prenášané nezabezpečené. Na vytvorenie bezpečnejšieho hesla sú možnosti zakódovania hesla, alebo modifikovaním zakódovania tak, že zakódované hodnoty sa zakaždým menia.

Prístupové heslo na strane servera nie je uchovávané v čistej textovej podobe, ale je znehodnotené jednocestným algoritmom proti zneužitiu správcom siete.

Keď používateľ zadá heslo, aby sa autentifikoval, systém zavolá na zadané heslo jednocestnú funkciu. Výsledok sa porovná s údajom uloženým v systéme. Napríklad v systéme UNIX sa ukladajú jednocestne znehodnotené heslá, kde jednocestný algoritmus je založený na symetrickej šifre. Šifruje sa stále rovnaký text, ale ako šifrovací kľúč slúži práve

heslo. Ak by si dvaja užívatelia zadali rovnaké heslo, tak by mali i rovnaký údaj uložený v systéme.

Táto chyba sa odstraňuje tým, že do jednocestnej funkcie vstupuje ďalšie číslo – tzv. soľ. Toto číslo pri generovaní hesla automaticky generuje systém. Soľ sa ukladá spoločne s heslom znehodnoteným jednocestnou funkciou. Pri overení hesla tak do výpočtu vstupuje heslo a soľ, výsledok sa potom porovná s údajom uloženým v systéme.

3.3. Jednorazové heslá

Jednorazové heslá riešia problém odposluchu hesla počas jeho prenosu sieťou a následným použitím. Jednorazové heslá sa nepoužívajú len v aplikáciách prevádzkovaných v počítačových sieťach, ale aj v aplikáciách, kedy je nutné autentifikovať užívateľa, ktorý požaduje službu bežným telefónom.

Ako najčastejšie jednorazové heslá sa používa zoznam jednorazových hesiel, kde po zadaní jedného hesla zo zoznamu si toto heslo užívateľ vyčiarkne zo zoznamu. Jednorazové heslá môžu byť aj očíslované. Systém potom môže povedať používateľovi aké heslo má použiť.

Nevýhoda zoznamu môže byť aj problém pamätania si celého zoznamu hesiel a taktiež možná vyčerpanosť hesiel.

Veľmi zaujímaným a v poslednej dobe často využívaným spôsobom je používanie očíslovaných hesiel, kde sa hesla nevyžadujú jedno po druhom, ale náhodne. Následne môže byť používanie jednotlivých hesiel aj opakované. Následne to už nie sú "jednorazové heslá", ale pre potenciálneho útočníka je použitie dvoch rovnakých hesiel v istom čase málo pravdepodobné. Pre niektoré aplikácie je dostatočná aj autentizačná karta vo forme plastikovej kartičky s predtlačenými sadami čísiel. Tento systém je často využívaný v internetbankingu ako tzv. "Gridcard".

Obr. 3-1 Autentizačná karta so sériou čísiel

Rekurentný algoritmus

Rekurentný algoritmus používa niektorý z algoritmov pre výpočet kontrolného súčtu. Užívateľ si musí sám zvoliť nejaký reťazec – násadu, ktorý nikomu neoznamuje. Ako algoritmus F sa zvolí jeden z jednocestných algoritmov. Kontrolný súčet z reťazca násada vyjadríme ako

F(násada).

Ak použijeme algoritmus F dvakrát na tú istú správu, tj. F(F(násada)), potom budeme písať:

F_2(násada)

a podobne F_n(násada) bude znamenať, že sme použili algoritmus F na reťazec násada celkom n-krát.

V inicializačnom kroku sa užívateľ a správca aplikácie dohodnú na čísle, napr. 1000. Užívateľ vyrobí F_{1000}(násada) a pošle ju správcovi. Správca aplikácie si do databázy k užívateľovi poznamená názov algoritmu pre výpočet kontrolného súčtu (tj. F), číslo 1000 a F_{1000}(násada). Správca teda nepozná text násada (je to užívateľovo tajomstvo).

Pri autentifikácii pošle užívateľ na server meno, server vo svojej databáze zistí, akú užívateľ používa autentifikačnú metódu. Pošle užívateľovi správu obsahujúcu číslo (n-1), tj. 999. Užívateľ vygeneruje odpoveď F_{999}(násada) a odošle ju ako jednorazové heslo serveru. Server preverí totožnosť užívateľa tak, že prevedie porovnanie

F(F_{999}(násada))=F_{1000}(násada).

Algoritmus F je mu známy, F_{1000}(násada) má uložené v konfiguračnom súbore a F_{999}(násada) dostane v odpovedi od užívateľa.

Po úspešnom preverení užívateľa uloží server do konfiguračného súboru namiesto hodnoty F_{1000}(násada) hodnotu F_{999}(násada) a namiesto čísla 1000 číslo 999. Pri ďalšej autentifikácii sa všetko opakuje s číslom o jednotku menším, tj. prevádza sa autentifikácia

F(F_{998}(násada))=F_{999}(násada)

Užívateľ môže teda vygenerovať celkom 999 hesiel na jedno použitie, potom musí zmeniť hodnotu reťazca násada a správcovi servera zaslať novú hodnotu F_{1000}(násada).

S/Key Password Protocol

S/Key One-Time Password System (S/Key systém jednorazového hesla), uvoľnený Bellcorom a definovaný v RFC 1760, je schéma generovania jednorazových hesiel založená

na MD4 a MD5. *S/Key Password Protocol* je implementáciou **rekurentného algoritmu**. Jadrom protokolu je použitie algoritmu pre výpočet kontrolného súčtu MD 4.

Násadu si klient volí sám, aby bola dlhá minimálne 8 bajtov. Algoritmus MD4 produkuje 16 bajtov dlhý kontrolný súčet, ktorý sa v tomto prípade delí na dve polovice po 8 bajtov. Tie sa spoja operáciou XOR do výsledných 8 bajtov. Ak použijeme predchádzajúcu terminológiu, tak algoritmom F je algoritmus MD 4, ktorého výsledok sa delí na dve polovice. Tie sú operáciou XOR zlúčené do výsledných 8 bajtov.

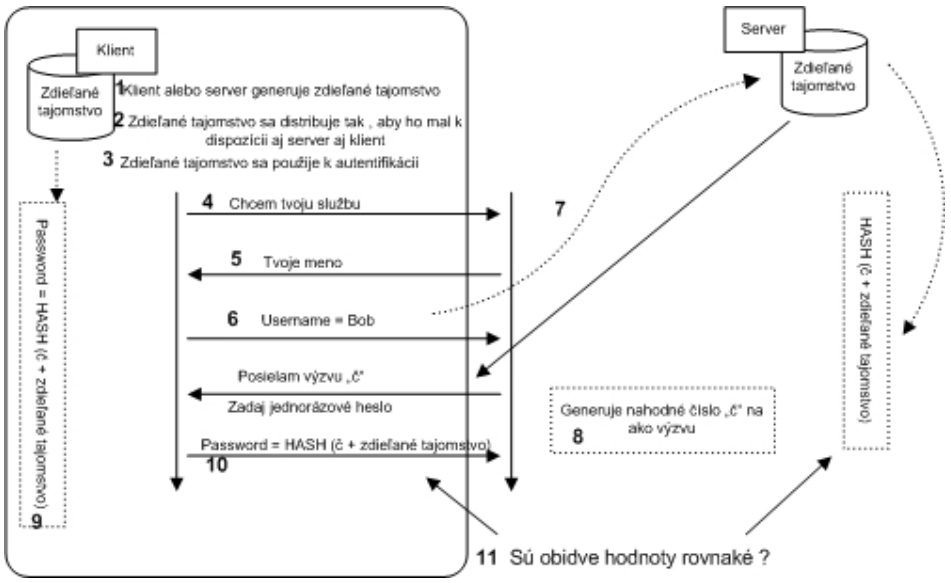
S/Key má rozšírenie umožňujúce použiť rovnaký algoritmus (vrátane rovnakej násady) pre viac aplikácií (napr. pre viac serverov). Princíp spočíva v tom, že aplikácia (server) využívajúca užívateľa k preukázaniu svojej totožnosti (autentifikácii) klientovi zobrazí tri údaje:

1. informáciu, že sa používa S/Key protokol;
2. číslo n, koľkokrát má používateľ aplikovať algoritmus F;
3. soľ (salt), čo je reťazec vygenerovaný serverom a zasielaný používateľovi nezabezpečene ako súčasť výzvy. Práve týmto údajom sa budú výzvy jednotlivých aplikácií líšiť.

Užívateľ najskôr spojí násadu so soľou a výsledný reťazec potom použije ako násadu pre algoritmus F.

3.4. Autentizácia používateľa a autorizácia dát za využitia zdieľaného tajomstva

Autentizácia sa prevádza pomocou jednocestného hesla. Jednorazové heslo vytvorené za využitia zdieľaného tajomstva využíva jednocestnú funkciu akou je napríklad kontrolný súčet. Z bezpečnostného hľadiska má tento typ autentizácie jednu nepríjemnú vlastnosť. Obidve strany poznajú zdieľané tajomstvo a môžu sa navzájom upodozrievať, že toto tajomstvo zneužili. Napríklad klient môže tvrdiť, že to nebol on pri dokazovaní totožnosti ale správca serveru. Toto sa dá riešiť rekurentným algoritmom alebo asymetrickým kryptovaním.



Obr. 3-2 Autentifikácia za využitia zdieľaného tajomstva

Pred tým ako budeme môcť využívať mechanizmus autentizácie jedna strana vygeneruje reťazec, nazývaný zdieľaným tajomstvom, ktorý predá druhej strane.
Obidve strany vlastnia spoločné tajomstvo a môže sa začať autentizácia.
Klient vytvára komunikáciu zo serverom.
Server sa klienta spýta na jeho meno.
Klient odošle serveru svoje prihlasovacie meno.
Server nájde v databáze meno daného používateľa.
Server zašle klientovi náhodné číslo “č”.
Klient dané číslo zreťazí so zdieľaným tajomstvom vypočíta hash, ktorý pošle serveru.
Server urobí rovnaký výpočet a porovná s prijatým hashom.
Pokiaľ sú rovnaké klient preukázal svoju totožnosť.

Podobný mechanizmus je použitý napríklad aj pri bankových platobných príkazoch.

Na začiatku sa vytvorí zdieľané tajomstvo
Klient zreťazí dôležité dáta platobného príkazu zo zdieľaným tajomstvom a vypočíta hash pomocou autentizačného kalkulátoru.
Odošle formulár aj s vypočítaným hashom

Server si pomocou zdieľaného tajomstva s daným klientom vytvorí rovnaký hash, ktorý porovná s prijatým od klienta.
Ak sa rovnajú, tak prevedie platobný príkaz.

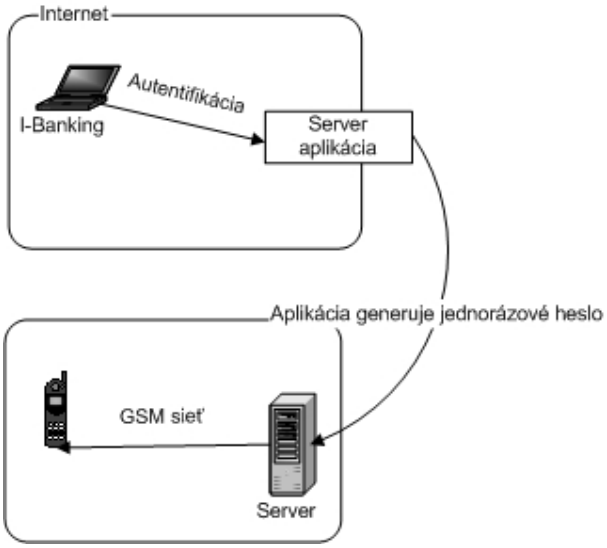
Autentizačné kalkulátory

Sú to elektronické pomôcky na autentifikáciu klienta. Autentizačné kalkulátory(AK) používajú niektorý s algoritmov na výpočet kontrolného súčtu(MD5,SHA-1 a pod.).

Používateľ obdrží od správcu aplikácie AK, ale najprv doň vloží tajomstvo "násadu". Tajomstvo je reťazec, ktorý bude uložený v kalkulátory a na serveri aplikácie. Výrobcovia AK detailný popis algoritmu nezverejňujú a považujú ho za svoje vlastníctvo.

Nevýhodou AK je ich samotné zakúpenie, ktoré nie je najlacnejšie a taktiež potreba nosiť zo sebou samotný AK.

Možným riešením je nahradiť AK mobilným telefónom. Tento spôsob využíva dva nezávislé kanály, čím klesá možnosť útoku. Ďalšou výhodou sú lacné zriaďovacie náklady, lebo v dnešnej dobe vlastní mobilný telefón väčšina ľudí.



Obr. 3-3 Jednorazové heslo zaslané pomocou GSM

Asymetrické kryptovanie

Princíp preukázania totožnosti na základe asymetrického kryptovania je jednoduchý. Občanovi bude predané náhodne vygenerované číslo “č”, ktorý ho podpíše pomocou svojho súkromného digitálneho kľúča. Digitálne podpísané číslo občan vráti inštitúcií a tá ho verifikuje. Celý podrobný postup bude popísaný v neskorších kapitolách. Dôležité bude teda udržanie si svojho súkromného kľúča. Autorizácia dát na základe asymetrického kryptovania sa nazýva **elektronický podpis dát**.

Uloženie súkromného kľúča

- Na disku:Je to veľmi praktické, ale zároveň veľmi nebezpečné, lebo môže pomerne ľahko dôjsť k odcudzeniu. Aj keď budú daného kľúče chránené šifrovaním, stále je to možnosť získať súkromný kľúč
- Hardwarový kľuč: je to technické zariadenie, ktoré poskytuje bezpečnejšie uloženie. Na rozdieľ od autentizačných kalkulátorov je hardwarový kľúč nutné pripojiť k počítaču.

Hardwarové kľúče bývajú vyhotovené ako čipové karty, čierne skrinky (Host security modul - HSM) alebo mini kľúče pripojiteľné cez USB port. Dnešné kľúče sa uchovávajú tak, že nikdy neopustia kľúč. Kľúč:

- Generuje dvojicu verejného/súkromného kľúčov
- Generuje podklady pre žiadosť o certifikát
- Vydaný certifikát je možné uložiť do kľúča
- V prípade použitia súkromného kľúča aplikácia vyšle dáta do hardvérového kľúča a kľúč prevedie šifrovanie súkromným kľúčom uloženom v hardwarovom kľúči.

4. Certifikačná autorita

Keď chceme dôverovať určitému subjektu musíme mať certifikát podpísaný daným subjektom. Medzi danými subjektmi vznikol priamy vzťah dôvery. Bolo by veľmi nepraktické vlastniť všetky certifikáty k všetkým subjektom, ktorým chceme dôverovať. Daný problém sa dá realizovať pomocou tretej osoby, ktorej dôverujeme a tá nám bude zaručovať dôveru ostatných subjektov. Ale je potrebné zaručenie dôvery v tretiu osobu. Za týmto účel vzniká reťazenie certifikátov a tým pádom aj nepriamy vzťah dôvery medzi rôznymi subjektmi.

Ak by mohol vydávať certifikáty, ktokoľvek vznikla by štruktúra bez žiadnych pravidiel. Ak však certifikáty vydávajú len niektoré subjekty (certifikačné autority - CA), môže vzniknúť prísna hierarchia alebo niekoľko oddelených stromov (hierarchická štruktúra).

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. Certifikáty možno vydať takmer pre čokoľvek.

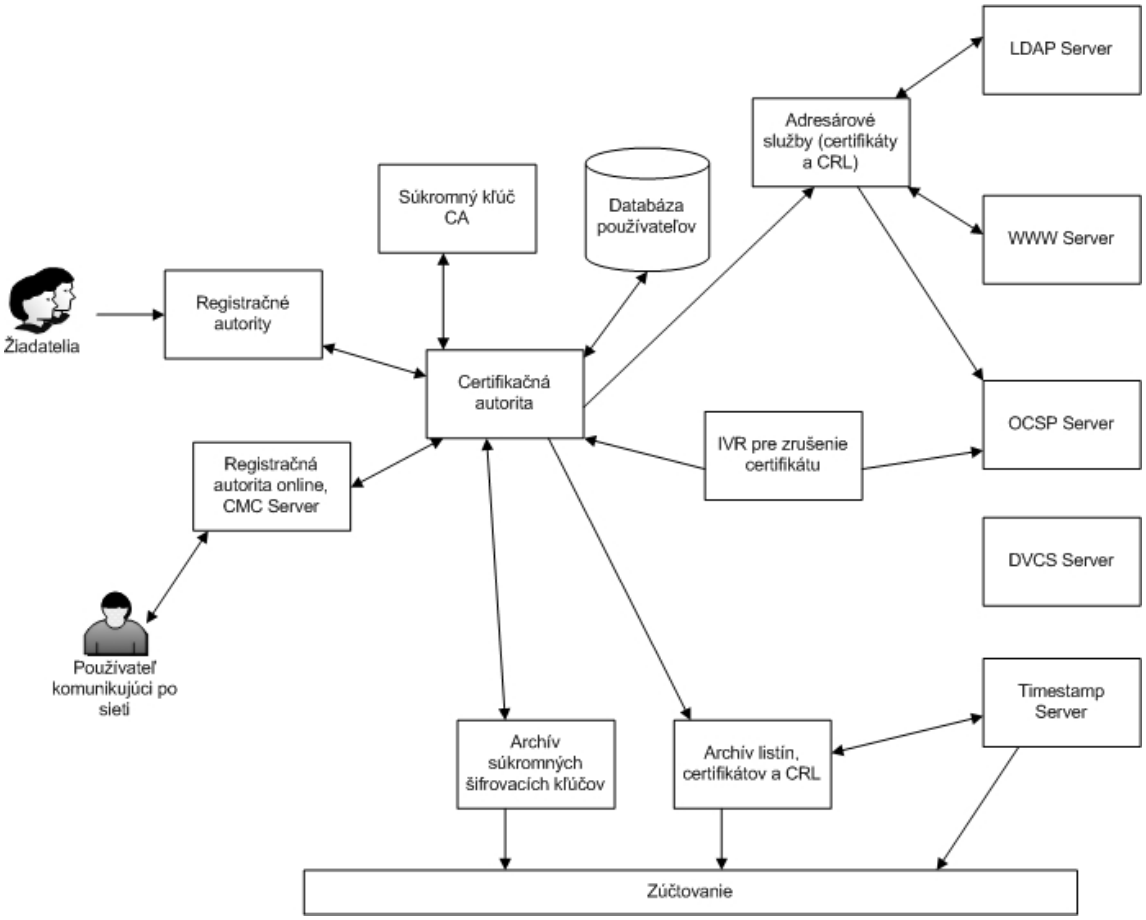
4.1. Hierarchická štruktúra

Štruktúra, ktorú vytvárajú certifikačné autority sa nazýva hierarchická štruktúra. 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 podriadenú certifikačnú autoritu fakulty. Certifikačná autorita regiónu bude certifikovať certifikačné autority obcí. Hierarchická štruktúra je najbežnejšie používaná štruktúra PKI, pretože dobre modeluje existujúce štruktúry reálneho sveta. Táto štruktúra je podporovaná štandardmi X.509 mnohými ďalšími.

4.2. Význam certifikačnej autority

Certifikačná autorita vystupuje pri vzájomnej komunikácii dvoch subjektov ako tretí nezávislý dôveryhodný subjekt, ktorý prostredníctvom ním vydaného certifikátu jednoznačne identifikuje subjekt s jeho digitálnym podpisom. Certifikát je teda akýmsi elektronickým preukazom totožnosti.

4.3. Štruktúra CA



Obr. 4-1 Základné schéma CA

Certifikačné autority majú časti, ktoré odpovedajú jej ponúkaným službám a jej bezpečnostnej politike. CA musí chrániť aktíva:

- Súkromný kľúč CA je tým najväčším aktívom CA. Odcudzenie kľúča certifikačnej autority sa stáva katastrofou pre samotnú existenciu CA.
- Sekvencia vydaných čísiel certifikátov. Vydanie dvoch rovnakých čísiel sa taktiež stáva katastrofou pre CA
- Databáza používateľov, ktorú musí chrániť z dvoch dôvodov
- CA nesmie vydať dvom rôznym osobám certifikát s rovnakým predmetom.
- Ochrana osobných údajov jednotlivých používateľov
- Archív súkromných šifrovacích kľúčov používateľov
- Archív listín uložených na CA a archív vydaných certifikátov a CRL. Ich strata by znamenala, že nie je možné daní podpisy verifikovať.

CA môže mať tiež:

- Registračné autority, kam prichádzajú žiadatelia o certifikáty. Žiadatelia môžu na registračnú autoritu (RA) priniesť žiadosť o certifikát, tá overí ich totožnosť a verifikuje žiadosť o certifikát a následne ho predá CA. Je tu aj možnosť, že RA vydá iba jednorazové heslo pre vydanie certifikátu a používateľ pošle žiadosť elektronicky cez OnLine RA.

  Používateľ môže cez OnLine RA žiadať o:

  - obnovenie certifikátu v dobe platnosti starého certifikátu
  - vydanie nového certifikátu na základe jednorazového hesla od RA
  - Ak vlastní certifikát, môže žiadať o vydanie ďalších certifikátov. Žiadosti podpisuje vlastným certifikátom.
  - Zálohovanie/obnovenie svojho šifrovacieho kľúča na CA
  - Obnovenie certifikátu
  - CRL alebo iný certifikát vydaný CA
- správna autorita
- Telefónny záznamník, slúžiaci k odvolaniu certifikátu
- Adresárové služby, kde je možne publikovať informácie o používateľoch (tie, ktoré povolia používatelia, aby sa mohli zverejňovať) a hlavne informácie týkajúce sa CRL.

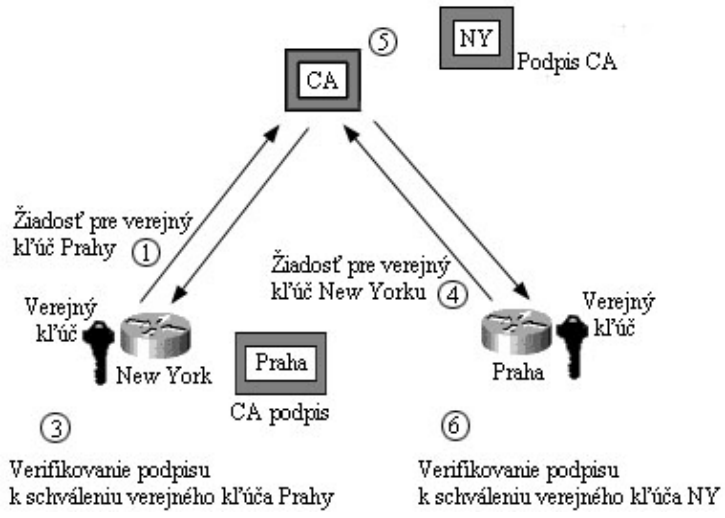
Testovacie certifikačné autority

Na testovacie účely boli vytvorené TCA, ktoré nepožadujú žiadnu totožnosť žiadateľa o certifikát. Stačí iba zaslať žiadosť CA a ona Vám automatický vystaví certifikát. TCA garantuje iba to, že nevydá certifikát z rovnakým sériovým číslom. Keby sme chceli používať danú CA musíme si zvlášť overiť totožnosť žiadateľa.

4.4. Certifikácia

Popis komunikácie medzi digitálnymi certifikátmi

Princíp si vysvetlíme na jednoduchom prípade:



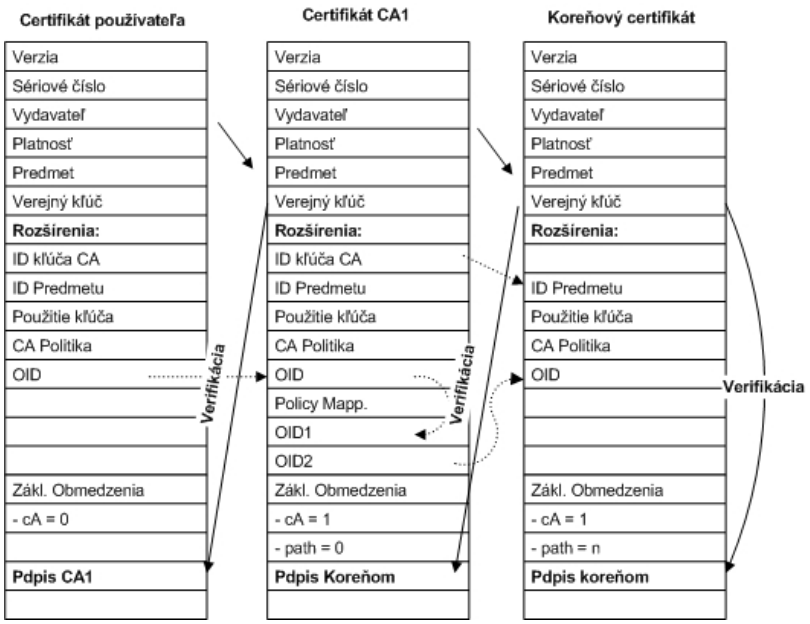
Obr. 0.1 Popis komunikácie medzi digitálnymi certifikátmi

1. New Yorkský smerovač pošle žiadosť certifikačnej autorite (CA) k obržaniu verejného kľúča Pražského smerovača.
2. Cerifikačné autorita pošle Pražskému smerovaču certifikát podpísaný jej súkromným kľúčom.

3. New Yorkský smerovač si overí podpis verejným kľúčom certifikačnej autority k tomu, aby mohol schváliť verejný kľúč Pražského smerovača.
4. Pražský smerovč pošle žiadosť certifikačnej autorite k získaniu verejného kľúča New Yorkského smerovača.
5. Certifikačná autorita pošle New Yorkskému smerovaču certifikát podpísaný s jej súkromným kľúčom.
6. Pražský smerovač si overí podpis verejným kľúčom certifikačnej autority k tomu, aby mohol schváliť verejný kľúč New Yorkského smerovača.

4.5. Reťazec certifikátov

Pokiaľ verifikujeme certifikát, musíme mať k dispozícií množinu certifikátov, z ktorej je možne vybrať reťazec ku koreňovému certifikátu. Koreňové certifikáty majú rovnaké pole „vydavateľ“ a „predmet“. Reťazec certifikátov môže získať z rôznych zdrojov, ale koreňový certifikát musí byť získaný z bezpečných zdrojov, lebo ten je podpísaný sám sebou.



Obr. 4-2 Reťazenie certifikátov

Pokiaľ by niekto poslal množinu certifikátov aj z koreňovým certifikátom, je možné tieto certifikáty použiť iba pre ľahšie vyhľadávanie reťazca. Vždy musí byť koreňový certifikát získaný pomocou bezpečnej cesty.

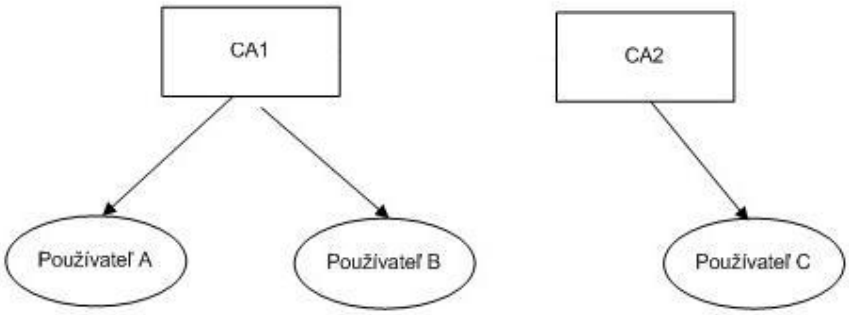
Taktiež je potrebné pri jednotlivých certifikátoch kontrolovať, či nie sú odvolané (nie sú v CRL).

Na zabezpečenie počítača je veľmi dôležitý zoznam dôveryhodných certifikátov, ktorý je inštalovaný na počítači. Musíme si dávať pozor, aby nami používaný internetový prehliadač obsahoval iba dôveryhodné certifikáty. Windows 2000 zaviedol tzv. CTL (Certificate Trusted List). Je to zoznam dôveryhodných certifikátov.

Potrebná vec, ktorú treba overiť je, či je daný certifikát možné k danému účelu použiť. Znamená to, či certifikačná politika uvedená v certifikáte odpovedá zamýšľanému využitiu certifikátu.

Krížová certifikácia

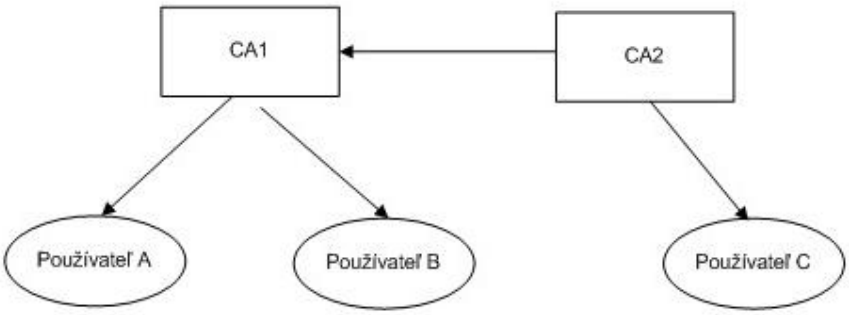
Musíme brať do úvahy, že certifikačné autority nemusia medzi sebou vytvárať striktne stromovú štruktúru. Môže nastať prípad, kedy koreňové certifikačné autority sú na rovnakej úrovni. V takomto prípade musíme vytvoriť krížovú certifikáciu.
Zoberme si prípad z obr. 4.5.1.2



Obr. 4-3 stromová štruktúra CA, nie je CA1 certifikované CA2

Používateľ A dôveruje používateľovi B. Je to preto, že majú spoločnú CA1 a používateľ A je schopný zostaviť reťazec certifikátov z certifikátov CA1 a certifikátu B. Taktiež funguje aj prípad, keď potrebuje používateľ B overiť dôveryhodnosť A. Problém nastáva, keď

používateľ A chce komunikovať s používateľom C. Nie je to možne lebo CA1 nepozná používateľa C.
Riešenie ponúka použitie krížového certifikátu.



Obr. 4-4 CA2 je krížovao certifikované CA1

Ide v podstate o to, že CA1 si okrem svojho koreňového certifikátu nechá vydať certifikát podpísaný CA2. Je vhodné aby si takto podpísali certifikáty CA navzájom. Potom výsledkom je že máme 4 certifikáty:

- CA1 podpísaný CA1
- CA2 podpísaný CA2
- CA1 podpísaný CA2
- CA2 podpísaný CA1

Obnovenie certifikátov CA

Nový certifikát je potrebné vydať s takým predstihom, aby súkromným kľúčom patriacemu k starému certifikátu neboli vydané certifikáty, ktorých platnosť skonči neskôr ako platnosť kľúča, ktorým boli podpísané.
V dobe, keď platia obidva certifikáty CA, majú niektorí používatelia podpísané svoje certifikáty starým a niektorý novým súkromným kľúčom CA.
Aby používatelia s certifikátom podpísaným starým kľúčom dôverovali certifikátom podpísaným novým kľúčom je ideálne vytvoriť krížový odkaz na certifikáty. Vzniknú

certifikáty „nový podpísaný starým“ a „starý podpísaný novým“, ktoré majú obmedzenú platnosť na dobu, kedy sa prekrýva platnosť certifikátov.

4.6. Certifikačná politika

Pri verifikácií certifikátov sa neuverejňuje iba elektronický podpis, ale aj certifikačná politika. Certifikačná politika je dokument (text), z ktorého by malo byť jasné, pre aké účel je certifikát vydaný. V certifikačne politike by malo byť uvedené aký je vzťah medzi používateľom a údajmi uvedenými v certifikáte. To je, akým spôsobom si CA overuje totožnosť žiadateľa o certifikát.

4.7. Bezpečnosť CA

Samotná CA tiež vlastní certifikát podpísaný nadradenou CA alebo v prípade koreňovej certifikačnej autority samotnou CA. Na ochranu privátneho kľúča CA triedy 2 a 3 sú však kladené mimoriadne bezpečnostné požiadavky, nakoľko sa používa na podpisovanie vydávaných certifikátov. Túto ochranu môžeme zabezpečiť s jedným z uvedených možností:

- privátny kľúč je symetricky šifrovaný a je uložený na smart karte, ktorú možno z počítača vybrať a uložiť do trezoru;
- privátny kľúč je symetricky šifrovaný a uložený na čipovej karte s procesorom. Nakoľko procesor robí sám všetky operácie s kľúčmi, privátny kľúč nikdy neopustí kartu;
- privátny kľúč a celé programové vybavenie CA pre prácu s kľúčmi je uložený na notebooku, ktorý sa zatvára do trezoru. Tento notebook môže byť vybavený deštrukčným systémom, ktorý sa aktivuje pri neodbornej manipulácii.

Bezpečný hardware sa často umiestňuje do miestnosti s riadeným prístupom tj. prístup do miestnosti je povolený len osobám s určitým odtlačkom prstov alebo čipovou kartou, atď. Prístup k privátnemu kľúču môže byť podmienený prítomnosťou aspoň dvoch operátorov CA. Všetky bezpečnostné opatrenia sú obsiahnuté v Bezpečnostnej politike CA. Bezpečnostný poriadok nezahrňuje len ochranu privátneho kľúča, ale celkovú bezpečnosť celého systému ako celku. Úrovňou Bezpečnostnej politiky CA je daná jej dôveryhodnosť.

5. PKI

Táto kapitola sa zaoberá infraštruktúrou verejného kľúča, známej skôr ako PKI – „Public Key Infrastructure“.

Budeme sa tu venovať certifikátom, ich obsahu, typom a verziám, norme X.509. Bližšie si rozoberieme žiadosť o certifikát, v prípade diskreditácie súkromného kľúča odvolanie certifikátu. S tým súvisí problematika odvolaných certifikátov a ich zoznam CRL – „Certificate Revocation List“. Z pohľadu elektronického podpisu je dôležité aj overovanie certifikátov.

PKI ako také je v porovnaní s inými internetovými normami relatívne mladé. Ako to už pri vzniku nových technických štandardov býva, spočiatku neexistovali žiadne pravidlá, podľa ktorých sa mohli výrobcovia softvéru riadiť. Vznikali preto rôzne implementácie, ktoré spolu nie vždy komunikovali tak, ako by si to používateľ želal. Aj dnes sa problematikou komunikácie založenej na asymetrickom šifrovaní a certifikátmi zaoberá viacero noriem. Najznámejšie sú systém SET (elektronické bankovníctvo) a RFC-3280. Hlavne RFC-3280 (spolu so svojim predchodcom RFC-2459) priniesla do tejto oblasti viac jednoznačnosti.

5.1. Certifikáty

Princíp a stručná charakteristika certifikátov boli popísané v úvodnej kapitole. Na tomto mieste sa budeme venovať detailnejším informáciám.

Tu popisované certifikáty popisujú certifikát podľa normy X.509 verzie 3 kódovaný ASN.1. Verzia 2 rozširuje verziu 1 len o polia `issuerUniqueID` a `subjectUniqueID`. Verzia 3 pridáva extensions, alebo rozšírenia certifikátu, čím podstatne rozširuje možnosti certifikátov. Samotný certifikát je potom kódovaný v DER. Všetky definície použité v tejto kapitole sú presne prebraté z RFC-3280.

Certifikát má tvar nasledujúcej štruktúry:

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

`tbsCertificate` je pole s údajmi, ktoré vyplní certifikačná autorita (CA).

Formát `tbsCertificate` definujeme nasledovne:

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

Podrobne sa mu budeme venovať v kapitole 4.1.1

`signatureAlgorithm` je CA-ou použitý algoritmus na elektronické podpísanie certifikátu a je definovaný nasledovne:

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

Algoritmus identifikuje použitú funkciu kontrolného súčtu spolu so šifrovacím algoritmom (napr. rsa with sha-1).

`signatureValue` je samotný podpis certifikačnej autority.

Základné položky certifikátu

Štruktúra `tbsCertificate` popisuje položky zviazané s vlastníkom certifikátu, CA-ou, ktorá certifikát vydala a so samotným certifikátom. Popisuje aj tzv. rozšírenia certifikátu (`extensions`), ktorým sa venuje nasledujúca podkapitola.

version

Verzia certifikátu.

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

Identifikuje, či je certifikát typu X.509 verzie 1, 2, alebo 3. V prípade, že ide o verziu 1 je uvedená hodnota „0“, pri verzii 2 hodnota „1“, pri verzii 3 „2“.

V prípade, že verzia nie je uvedená použije sa implicitná hodnota „0“, čiže verzia 1.

Každá implementácia by mala rozoznať akúkoľvek verziu certifikátu. Implementácie odvolávajúce sa na RFC-3280 musia rozoznať aspoň verziu 3.

serialNumber

Sériové číslo certifikátu.

```
CertificateSerialNumber  ::=  INTEGER
```

Každé sériové číslo musí byť nezáporné celé číslo jednoznačne identifikujúce certifikát v rámci CA-y, ktorá tento certifikát vydala. V kombinácií s identifikátorom CA-y jednoznačne identifikuje certifikát na celom svete.

signature

CA-ou použitý algoritmus na elektronické podpísanie certifikátu. Musí byť zhodný s poľom `AlgorithmIdentifier` zo štruktúry `Certificate`. Algoritmus identifikuje použitú funkciu kontrolného súčtu spolu so šifrovacím algoritmom (napr. rsa with sha-1).

issuer

Identifikátor CA-y, ktorá vydala a podpísala certifikát.

```
Name ::= CHOICE {
  RDNSequence }
```

`Name` je relatívne zložitá štruktúra, ktorá je detailne popísana v RFC-3280 v kap. 4.1.2.4. Nám bude stačiť vedieť, že obsahuje o.i. polia

```
* country,
* organization,
* organizational-unit,
```

```
* distinguished name qualifier,
* state or province name,
* common name
* serial number.
```

validity

Platnosť certifikátu.

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

Time ::= CHOICE {
     utcTime        UTCTime,
     generalTime    GeneralizedTime }
```

Platnosť certifikátu je vymedzená spodnou a hornou hranicou platnosti vrátane. Tieto dve hranice musia byť kódovane kódovaním `UTCTime` v prípade, že ide o dátum do roku 2049 (`UTCTime` používa pre rok dvojciferné číslo), `GeneralizedTime` v prípade, že ide o dátum v roku 2050 a neskôr. CA sa zaručuje, že počas tohto intervalu bude udržiavať informácie o stave certifikátu.

Sú dva dôvody pre obmedzovanie platnosti certifikátu:

- bezpečnostný
- organizačný

Bezpečnostný dôvod je podobný ako je dôvod pre častú zmenu hesla v systéme. S narastajúcim časom rastie riziko zneužitia súkromného kľúča. Taktiež sa časom môžu objaviť nové metódy umožňujúce prelomenie použitej šifry. Tu vzniká problém s dobou platnosti certifikátu CA-y. Na jednej strane je tento certifikát dôležitejší ako používateľské, takže by mal mať kratšiu dobu platnosti. Na strane druhej však na overenie certifikátu potrebujeme platný certifikát CA-y. Certifikát CA-y teda môže vypršať najskôr po vypršaní platnosti posledného platného certifikátu podpísaného súkromným kľúčom CA-y, ku ktorému sa vzťahuje daný certifikát.

Organizačný dôvod hovorí o životnosti aplikácie, pre ktorú je certifikát vydaný.

Ďalším dôvodom by mohli byť obchodné praktiky CA-ít. Vydávanie certifikátov je v dobrom zázemí mimoriadne výnosná činnosť so stálym príjmom.

subject

Jedinečný identifikátor subjektu, ktorému je certifikát vydávaný., tzv. predmet certifikátu. Tento predmet môže byť nielen osoba, ale aj napr. server.

`subject` je tiež typu `Name`, ako tomu bolo pri poli `issuer` a platia pre neho rovnaké pravidlá. Avšak pole `subject` nesmie byť rovnaké u viacerých certifikátov vydaných jednou CA-tou. Keďže však jeden objekt môže mať viacero certifikátov je treba jednotlivé `subject`-y rozlíšiť. Slúžia na to polia `serialNumber` a `dnQualifier` v štruktúre `Name`. `serialName` si netreba zamieňať so `serialNumber` v štruktúre `TBSCertificate`.

subjectPublicKeyInfo

Informácie o verejnom kľúči subjektu a samotný kľúč.

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

Položka `algorithm` identifikuje, pre aký algoritmus je certifikovaný verejný kľúč určený. `subjectPublicKey` je samotný kľúč.

issuerUniqueID a subjectUniqueID

Slúžia na rozlíšenie certifikátov s rovnakými poliami `issuer` a `subject`. Objavili sa v X.509 v2 a implementácie CA odvolávajúce sa na RFC-3280 ich nesmú používať. Veľmi pravdepodobne budú v nasledujúcej verzií vypustené.

extensions

Rozšírenia certifikátu. Objavili sa v X.509 v3. obsahujú jedno alebo viac rozšírení. Podrobnejšie im budú venovaná nasledujúca časť.

Rozšírenia certifikátu

Rozšírenia certifikátu slúžia na umiestnenie dodatočných informácii o subjekte, CA, certifikovanom verejnom kľúči, alebo o certifikáte.

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

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

`extnID` rozlišuje názov rozšírenia.

`critical` určuje, či ide o tzv. kritické rozšírenie. Rozdiel medzi kritickými a nekritickými rozšíreniami je v tom, že aplikácie pracujúce s certifikátmi musia certifikát odmietnuť v prípade, že pri jeho spracovávaní narazia na kritické rozšírenie, ktorému nerozumejú. Nekritické rozšírenie môže byť jednoducho ignorované.

`extnValue` samotné dáta rozšírenia.

Certifikát môže obsahovať len jedno rozšírenie určitého typu.

Podľa RFC-3280 musia aplikácie rozoznávať nasledovné rozšírenia:

- key usage
- certificate policies
- subject alternative name
- basic constraints
- name constraints
- policy constraints
- extended key usage
- inhibit any-policy

mali by rozoznávať aj nasledujúce rozšírenia:

- authority key identifier
- subject key identifier
- policy mapping

Rozšírenia sú podrobne popísané v RFC-3280 a taktiež v [DOSTALEK1], preto sa im tu ďalej nebudeme venovať. Len spomenieme, že za pomoci rozšírení je možné vydať napr. certifikát, ktorý bude slúžiť len na určitú činnosť, prípadne na istú činnosť nebude použiteľný.

5.2. Žiadosť o certifikát

Existujú 3 typy žiadostí o certifikát:

- RFC-1424, žiadosť protokolu PEM
- RFC-2314, žiadosť v tvare PKCS#10
- RFC-2411, žiadosť v tvare CRMF

Prvý typ sa v praxi nepoužíva. Druhému a tretiemu sú venované samostatné časti.

Žiadosť o certifikát v tvare PKCS#10

Pri tomto tvare žiadosti žiadateľ vlastní kľúčový pár, ktorý si chce nechať podpísať. Vyplní štruktúru žiadosti elektronicky ju podpíše a pošle Registračnej Autorite (RA). RA overí, či údaje neboli cestou modifikované a tým rovno overí aj existenciu súkromného kľúča. V prípade, že je všetko v poriadku predá žiadosť CA-e. CA zo žiadosti vyčíta predmet certifikátu a verejný kľúč. Zvyšok doplní podľa seba a vydá certifikát.

Žiadosť o certifikát v tvare CRMF

Táto žiadosť o.i. rieši problémy súvisiace s dokazovaním existencie súkromného kľúča.

V prípade, že si žiadateľ chce nechať vydať certifikát na šifrovanie a nie na elektronický podpis, nie je možné overiť existenciu súkromného kľúča elektronickým podpisom. Prvá z možností je nechať si vygenerovať kľúčový pár CA-tou. Iná možnosť, v prípade, že prvá je nevyhovujúca, je nechať si vydaný certifikát zašifrovať súkromným kľúčom CA-ty. V tom prípade nikto okrem žiadateľa nie je schopný certifikát dešifrovať.

Ak je kľúč určený na overovanie elektronického podpisu je možné postupovať podobne ako pri žiadosti PKCS#10. Zo žiadosti sa vygeneruje elektronický podpis, a ten sa spolu so žiadosťou pošle RA-te.

5.3. Žiadosť o odvolanie certifikátu

Existujú situácie, v ktorých je nutné zrušiť platnosť certifikátu. Ak napr. príde žiadosť o certifikáciu už certifikovaného existujúceho verejného kľúča, zruší platnosť certifikátu sama

CA. Ale v prípade, že prišlo napr. k diskreditácii súkromného kľúča, iniciuje jeho odvolanie sám majiteľ.

Ak súkromný kľúč niekto odcudzil, je možné poslať žiadosť podpísanú týmto kľúčom. Tým sa overí majiteľova totožnosť. V prípade, že by túto žiadosť postal útočník sa nič nestane. Certifikát sa odvolá, čo je správne, pretože súkromný kľúč je v rukách cudzej osoby. Toto však môže byť cielené, t.j. útočník chcel, by bol certifikát odvolaný. V tom prípade ide o zvláštny prípad, ktorý treba riešiť individuálne.

V prípade straty súkromného kľúča nie je možné poslať podpísanú žiadosť. V takej situácií musí majiteľ navštíviť CA osobne s dokladmi totožnosti a certifikát odvolať „osobne“. V istých prípadoch však CA-ty môžu vydať pre tento špeciálny prípad odvolávacie jednorázové heslo, ktoré je možné na odvolanie použiť rôznymi spôsobmi: e-mailom, faxom, telefonicky, prípadne cez špeciálne, pre tento účel pripravené web rozhranie CA-ty.

Presný postup odvolávania certifikátov zverejňuje každá CA v dokumente „Certifikačná politika CA“. Každý z uvedených postupov bol len príklad odvolávania. CA si postup a možnosti pre uvedené prípady definuje sama a sú v súlade s jej bezpečnostnou politikou.

5.4. CRL - Certificate Revocation List

CRL je zoznam odvolaných certifikátov danej CA. Tento zoznam obsahuje sériové čísla odvolaných certifikátov. CA udržuje odvolaný certifikát na zozname až do doby vypršania platnosti certifikátu. Tento oznam môže byť aj prázdny.

CRL sa vydáva v pravidelných intervaloch spôsobom a na miestach popísaných v dokumente „Certifikačná politika CA“. V čase medzi vydaním jednotlivých CRL sa zbierajú a spracovávajú jednotlivé žiadosti o odvolanie certifikátov. Z pohľadu poškodeného majiteľa certifikátu to však môže byť dlhá doba, aj keď ide približne o 24 hodinový interval. V tomto čase môže certifikačná autorita vydávať tzv. deltaCRL, teda čiastkové CRL. Tieto CRL neobsahujú všetky odvolané certifikáty, ale len certifikáty odvolané od posledného kompletného CRL. Každý deltaCRL musí obsahovať identifikátor posledného kompletného CRL.

Aj tento mechanizmus však nemusí by. dostačujúci. V prípade, že útočník stihne použiť odcudzený súkromný kľúč pred vydaním deltaCRL, má jeho bývalý majiteľ smolu. Riešenie môže spočívať napr. v tom, že banka po obdržaní podpísanej žiadosti počká do

vydania ďalšieho deltaCRL a v prípade že sa certifikát na ňom nenachádza uskutoční transakciu.

Tento problém však rieši online protokol OCSP, ktorý je schopný zistiť, či je certifikát v danom čase platný, alebo nie. A to aj v prípade, že certifikát je už zneplatnený, ale ešte sa nenachádza na CRL.

CRL vydáva CA, alebo CA tým poverená. V druhom prípade ide o nepriame CRL – indirectCRL.

Tvar CRL je podobný ako tvar certifikátu. Vychádza z normy X.509 v2 a je popísaný v RFC-3280. obsahuje nasledujúce súčasti.

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

TBSCertList  ::=  SEQUENCE  {
     version                 Version OPTIONAL,
                                  -- if present, MUST be v2
     signature               AlgorithmIdentifier,
     issuer                  Name,
     thisUpdate              Time,
     nextUpdate              Time OPTIONAL,
     revokedCertificates     SEQUENCE OF SEQUENCE  {
          userCertificate         CertificateSerialNumber,
          revocationDate          Time,
          crlEntryExtensions      Extensions OPTIONAL
                                        -- if present, MUST be v2
                                }  OPTIONAL,
     crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                        -- if present, MUST be v2
                                }
```

CRL obsahuje podobne ako certifikát samotné dáta a podpis CA, ktorá CRL vydala.

Polia CRL

version

Verzia CRL. Implicitne 1, čiže ide o X.509 verziu 2.

signature

Algoritmus použitý pri podpisovaní CRL.

issuer

Identifikátor CA, ktorá vydala a podpísala CRL.

thisupdate

Čas, kedy bol CRL vydaný.

nextupdate

Predpokladaný čas vydanie ďalšieho CRL. Ďalší CRL musí byť vydaný najneskôr do termínu uvedenom v tomto poli.

revokedCertificates

Samotné pole s odvolanými certifikátmi.

crlExtensions

Rozšírenia CRL. Rozšírenia CRL sú nasledovné:

- číslo CRL, ktoré musí vzrastať po jednej a musí byť uvedené v každom CRL.
- deltaCRL, ktorý indikuje, že nejde o kompletný CRL, ale len o prírastok k poslednému kompletnému CRL
- identifikátor kľúča certifikačnej autority
- alternatívne meno vydavateľa
- distribučné miesto CRL obsahuje URI s aktuálnym CRL CA, typ odvolaných certifikátov a informáciu o tom, či ide o nepriami CRL

Zoznam odvolaných certifikátov

Zoznam odvolaných certifikátov je sekvencia štruktúr, ktoré identifikujú samotné certifikáty. Štruktúra obsahuje sériové číslo certifikátu, čas, kedy prišlo k odvolaniu certifikátu a rozšírenia odvolaného certifikátu.

Rozšírenia odvolaných certifikátov

- dôvod odvolania certifikátu
- inštrukcie pre prípad odvolania, ktoré hovoria, ako postupovať pri zistení, že certifikát sa nachádza naCRL
- čas, kedy bola zistená diskreditácia súkromného kľúča.
- vydavateľ certifikátu. Toto pole sa používa v prípade nepriameho CRL, ktorý samozrejme vydala CA, ktorá nie je podpísaná pod

skompromitovaným certifikátom. Bez tejto položky by nebolo možné jednoznačne identifikovať certifikát.

5.5. Overovanie dokumentov

Overovanie dokumentu podpísaného elektronickým podpisom a samotného elektronického podpisu sa skladá z viacerých častí.

- Je treba nájsť certifikát prislúchajúci k verejnému kľúču potrebného na dešifrovanie.
- Je treba overiť tento certifikát. V prípade, že ide o starší dokument, stačí sa pozrieť do prislúchajúceho CRL, platného v danom čase a zistiť, či sa v ňom certifikát nenachádza. V prípade nového dokumentu je možné použiť server OCSP a spýtať sa ho, či certifikát nie je v danom čase zneplatnený, aj keď ešte nevyšlo nové CRL, v ktorom by tento certifikát figuroval.
- Musíme overiť platnosť podpisu tohoto certifikátu. To znamená overenie platnosti certifikátu CA, ktorá podpísala certifikát, ktorý overujeme.
- Takýmto postupom musíme overiť všetky certifikáty v ceste až po dôveryhodný certifikát, ktorým býva zvyčajne certifikát certifikačnej autority.

Nakoniec je treba overiť samotný dokument. Tento postup bol uvedený v úvode v časti o elektronickom podpise

5.6. Časová pečiatka

RFC-3161 špecifikuje protokol pre vydávanie časových pečiatok, Time Stamp Protocol – TSP. Pomocou tohto protokolu sa uskutočňuje komunikácia s Time Stamping Authority – TSA server.

Komunikácia je typu klient server. Žiadateľ o časovú pečiatku pošle žiadosť na opečiatkovanie TSA, tá skontroluje, či je žiadosť formálne správna a v kladnom prípade ju podpíše a pošle späť žiadateľovi. Žiadosť o časovú pečiatku obsahuje kontrolný súčet z dokumentu, ale nie je elektronicky podpísaná. Žiadosti o časovú pečiatku sú anonymné. Naopak, vydaná časová pečiatka je elektronicky podpísaná TSA a obsahuje identifikáciu TSA a kontrolný súčet zo žiadosti.

Keďže žiadosti o časovú pečiatku sú anonymné, časová pečiatka neslúži na overenie držania dokumentu konkrétnym subjektom, ale na overenie existencie dokumentu v danom čase.

Z uvedeného vyplývajú pre TSA isté povinnosti. Extrémne požiadavky sa kladú na dôveryhodné časové zdroje. Každá žiadosť musí mať svoje jedinečné sériové číslo. TSA musí vydať časovú pečiatku na každú formálne správnu žiadosť, prípadne odpovedať chybovým hlásením.

6. Použitá literatúra

[1] Zervan D.: Šifrovanie a elektronický podpis 1-3 časť PC Revue

[2] Rexa R., Fapšo R., Schreiber R.: Bezpečnosť elektronického bankovníctva v praxi. PC Revue 6/2001.

[3] Rexa R.: Od praktických skúseností k návrhu zákona o elektronickom podpise. PC Revue 10/2001.

[4] Občiansky zákonník č. 40/1964 Zb.

[5] Kršák, E.: Elektronický podpis. In: Zborník prednášok na medzinárodnú konferenciu Systémová integrácia 2001, SSSI Žilina 2001, str. 185 – 194, ISBN 80-7100-880-X.

[6] https://cert.utc.sk/ca.

[7] Poslanecký návrh zákona o elektronickom podpise http:// www.nrsr.sk/Slovak/Zakony/1citanie/984z.pdf

[8] Vládny návrh zákona o elektronickom podpise

[9] http://www.economy.gov.sk/doc/komentar.htm

[10] J. Pinkava: Elektronický podpis a Evropská Unie, DSM 2/2000

[11] http://crypto.aec.cz (séria článkov)

[12] Dostálek, L.: Velký průvodce protokoly TCP/IP: Bezpečnost, ISBN 80-7226-849-X, Computer Press Praha,2004

[13] RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://www.faqs.org/rfcs/rfc3280.html

[14] Z Á K O N z 15. marca 2002 o elektronickom podpise a o zmene a doplnení niektorých zákonov, http://www.zbierka.sk/get.asp?rr=02&zz=02-z215

7. Slovník základných pojmov

Asymetrické šifrovanie používa dva rôzne kľúče – verejný a súkromný (tajný). Súkromný kľúč je známy výlučne vlastníkovi kľúča, verejný kľúč je známy verejnosti. Tento pár kľúčov je komplementárny v tom zmysle, že to, čo sa zašifruje jedným z týchto kľúčov, je možné dešifrovať iba druhým kľúčom z tejto dvojice a naopak.

Autentifikácia rozpoznanie a jednoznačná identifikácia osoby podpisujúcej určitý dokument. Potvrdenie, že odosielateľ je skutočne tá osoba, za ktorú sa vydáva.

Certifikát elektronický dokument podpísaný súkromným kľúčom certifikačnej autority. Obsahuje verejný kľúč majiteľa certifikátu a ďalšie údaje týkajúce sa certifikátu ako aj držiteľa certifikátu – sériové číslo certifikátu, meno majiteľa, typ certifikátu, meno CA, elektronický podpis CA, dobu platnosti certifikátu a prípadne aj nejaké ďalšie údaje. CA svojím podpisom na certifikáte potvrdzuje, že majiteľom verejného kľúča obsiahnutého v certifikáte je skutočne ten, kto je v popise certifikátu uvedený.

Certifikát transakcie potvrdzuje, že daná transakcia sa naozaj uskutočnila, a tým znemožňuje popretie tejto transakcie v budúcnosti.

Certifikačná autorita inštitúcia, ktorá vystavuje certifikáty používané na identifikáciu majiteľa verejného šifrovacieho kľúča. Svojou funkciou sa podobá na štátneho notára.

Časová pečiatka potvrdenie, že nejaký dokument existoval v danom čase.

Digitálna obálka tajný kľúč pre symetrické šifrovanie (napr. pomocou DES algoritmu) sa zašifruje pomocou RSA algoritmu verejným kľúčom adresáta správy. Najprv sa musí dešifrovať tento tajný kľúč pre symetrické dešifrovanie (pomocou tajného kľúča adresáta pre asymetrické šifrovanie), aby sa potom pomocou tohto kľúča mohol dešifrovať obsah samotnej správy.

Digitálny odtlačok digitálny odtlačok je súhrn, zhrnutie správy. Digitálny odtlačok je pevnej dĺžky (nezávislej od dĺžky správy) a vypočíta sa pomocou tzv. *hash funkcie*.

Elektronický podpis digitálny odtlačok správy vygenerovaný odosielateľom, sa zašifruje pomocou asymetrického algoritmu šifrovania, pričom odosielateľ digitálny odtlačok zašifruje (podpíše) svojím tajným kľúčom. Výsledkom tohto postupu je elektronický podpis. Niekedy sa (ako synonymum) používa aj pojem „digitálny podpis“.

Integrita správy skutočnosť, že poslaný dokument sa dostal k adresátovi v nepozmenenej podobe, t.j. že to, čo odosielateľ odoslal, je skutočne to, čo prijímateľ dostal.

Metóda verejného kľúča (anglicky Public Key Infrastructure – PKI)

pozri Asymetrické šifrovanie.

Nepopierateľnosť	nepopierateľnosť znemožňuje podpisujúcemu tvrdiť, že podpis nie je jeho a že to nebol on, kto daný dokument podpísal a odoslal. Odosielateľ nemôže neskôr poprieť, že on poslal daný dokument.
Symetrické šifrovanie	správa sa šifruje aj dešifruje pomocou toho istého kľúča, čiže odosielateľ (na šifrovanie správy) aj prijímateľ (na dešifrovanie správy) používajú ten istý kľúč, ktorý musí byť samozrejme tajný (neprístupný tretej strane).
Odposluch	nežiadané sledovanie komunikácie iným subjektom ako sú tie, ktoré medzi sebou komunikujú
Jednocestný algoritmus	algoritmus, ktorého výpočet je veľmi jednoduchý, ale spätné počítanie je náročné
Internetbanking	bankové operácie realizované pomocou internetu
Gridcard	Karta z uloženými sériami čísiel slúžiacimi na autentifikáciu používateľa
USB port	Hardvérové rozhranie používané na počítači.
USB kľúč	Zariadenie na ukladanie dát pripojiteľné k počítaču pomocou USB portu

8. Skratky

CA	*Certificate Authority*: Certifikačná autorita
Hash	Funkcia , ktorá ľubovoľne dlhý reťazec znakov transformuje na reťazec pevnej dĺžky
MD 5	*Message Digest 5*: Hash funkcia vyvinutá v roku 1991 R. Rivestom
PGP	*Pretty Good Privacy*: Kryptografický balík využívaný predovšetkým na šifrovanie správ a súborov a vytváranie/overovanie digitálnych podpisov
RFC	*Request For Comment*: Dokumenty špecifikujúce štandardy pre Internet
RSA	*Rivest-Shamir-Adleman*: Asymetrický šifrovací algoritmus
SHA	*Standard Hash Algoritmus*: Najčastejšie používaná hašovacia funkcia
X.509	Štandardizovaný formát pre certifikáty