Certifikačná Autorita

Úvod

Spoločnosť vstupuje do informačného veku. Globálne siete a celosvetové informačné toky sa stávajú prirodzenou súčasťou nášho života. Internet už dávno prestal byť študentskou hračkou a predstavuje jedinečný zdroj informácií a unikátne komunikačné médium. Len ťažko niekto spočíta koľko správ elektronickej pošty sa denne prenesie pomocou Internetu. Jedno je však isté, veľká väčšina prenášaných informácií postráda akúkoľvek ochranu. Správy sú prenášané v otvorenom tvare, osobné údaje zadávané do formulárov bez akejkoľvek ochrany a najbežnejšie používaná autentifikačná metóda sú statické heslá.

S nárastom dôležitosti informácií dostupných na Internete však začína narastať aj snaha chrániť ich. Mnohé organizácie začínajú nasadzovať lokálne bezpečnostné systémy a neštandardné riešenia s malou pôsobnosťou. Globálna sieť však potrebuje globálne riešenie, štandardizované riešenie, prijaté širokým okruhom používateľov.

Infraštruktúra certifikačných autorít má ambície stať sa kľúčovou časťou riešenia bezpečnostných problémov globálnych sietí. Je to riešenie prijaté veľkými softvérovými firmami a tak dodávané v softvérových produktoch miliónom používateľov. Je to riešenie flexibilné, prispôsobiteľné lokálnym podmienkam a požiadavkám. Hierarchia certifikačných autorít v hrubých rysoch zodpovedá hierarchií prirodzených autorít, preto sa ľahko implementuje v organizovaných spoločnostiach.

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

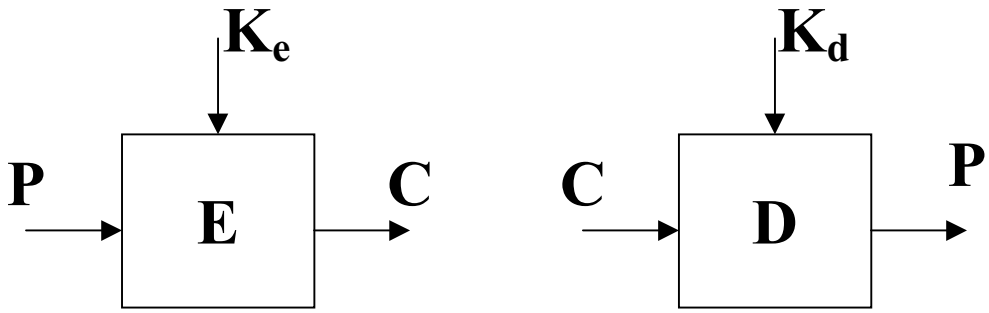
Základy kryptografie

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

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 (K_e). Dešifrovací algoritmus naopak transformuje šifrovanú správu (C) na správu v otvorenom tvare (P) pomocou dešifrovacieho kľúča (K_d). Schematicky je šifra zobrazené na obrázku Obr. 1.



Obr. 1 Šifra

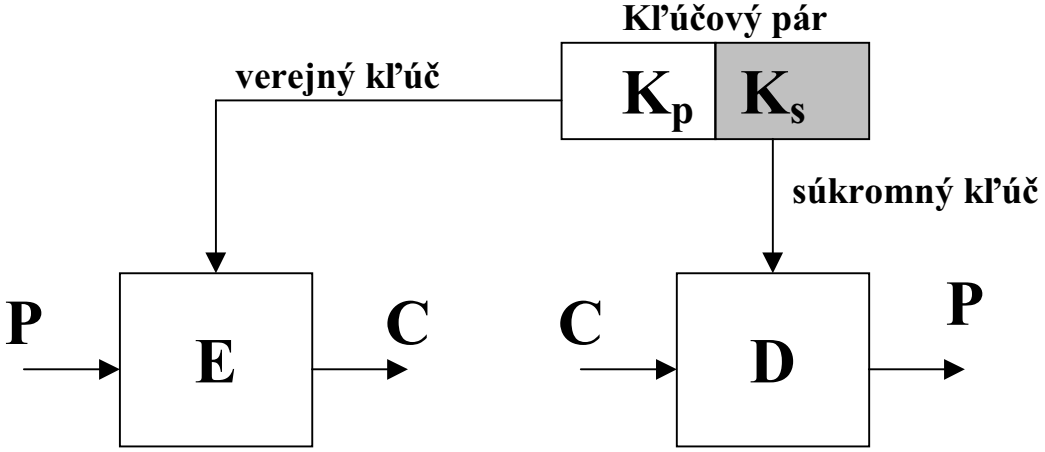
Správa v šifrovanom tvare (C) je čitateľná len pre toho, kto vlastní dešifrovací kľúč (K_d). Šifrovací aj dešifrovací algoritmus sú v o väčšine prípadov verejne k dispozícii a jediná tajná informácia sú použité kľúče.

Symetrické šifry

Klasické historické šifry a aj mnoho súčasných šifier používa rovnaký kľúč na šifrovanie aj dešifrovanie ($K_e = K_d$). 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.

Asymetrické šifry

Na druhej strane pri *asymetrických* šifrách je šifrovací a dešifrovací kľúč rozdielny ($K_e \neq K_d$). 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 Obr. 2.

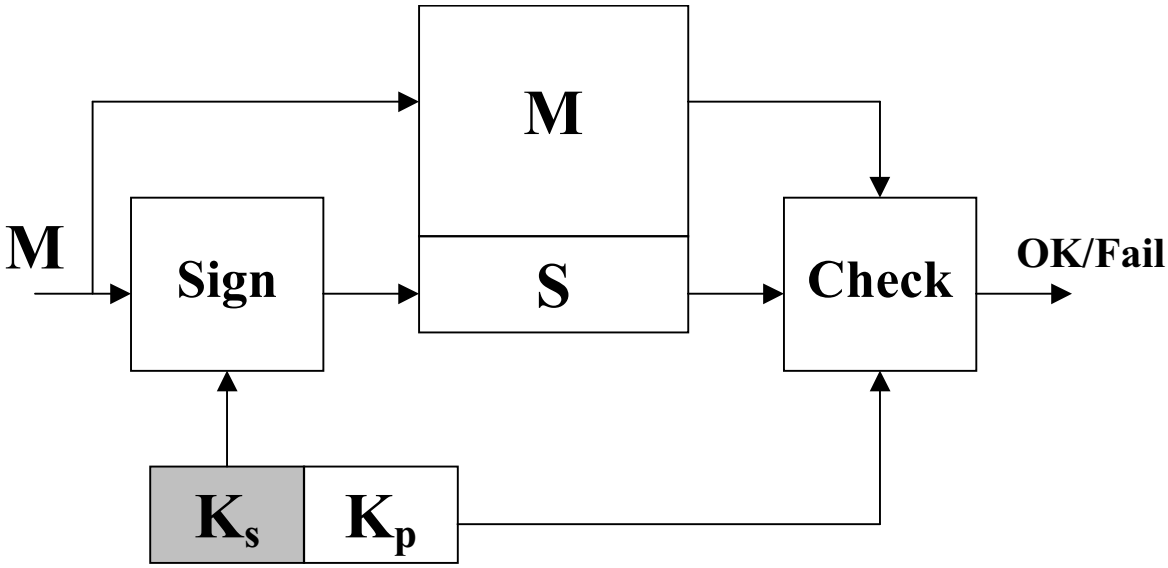


Obr. 2 Asymetrická šifra

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.

Elektronický podpis

Elektronický podpis je obdoba klasického podpisu. Zaručuje autenticitu podpísanej správy. Po matematickej stránke je elektronický podpis funkciou obsahu správy (*M*) a súkromného kľúča (Obr. 3). 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.



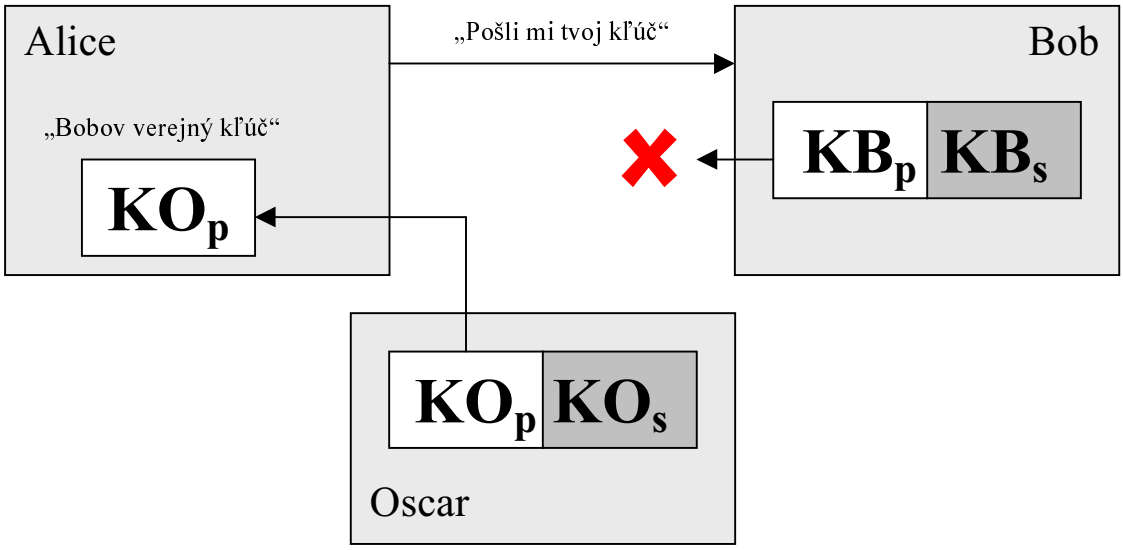
Obr. 3 Elektronický podpis

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.

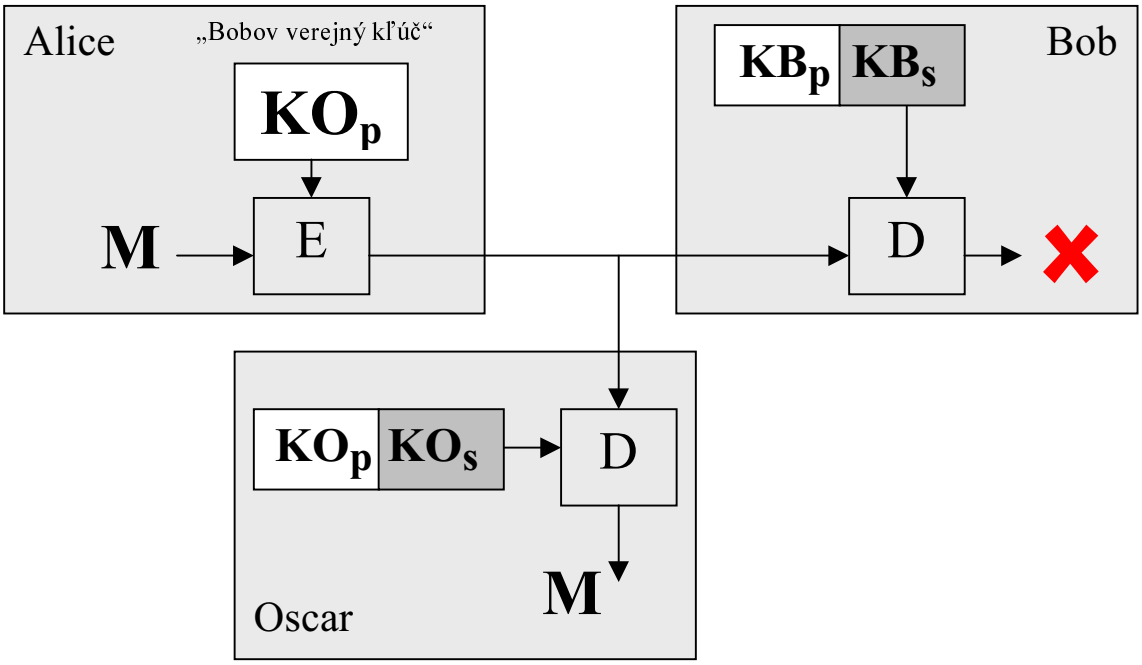
Získavanie kľúčov

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. 4).



Obr. 4 Zámena kľúčov 1

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. 5) 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.



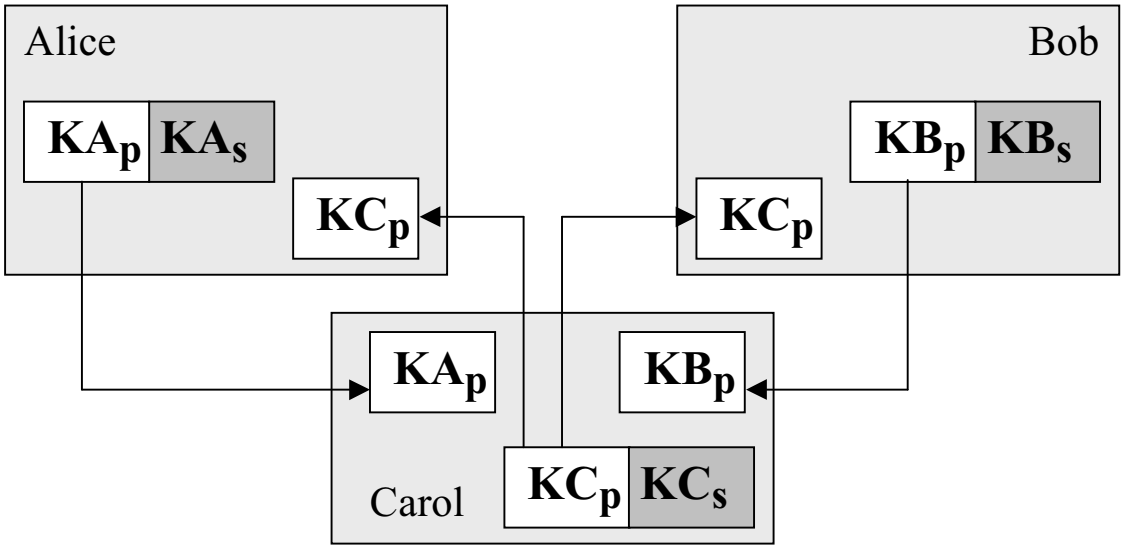
Obr. 5 Zámena kľúčov 2

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.

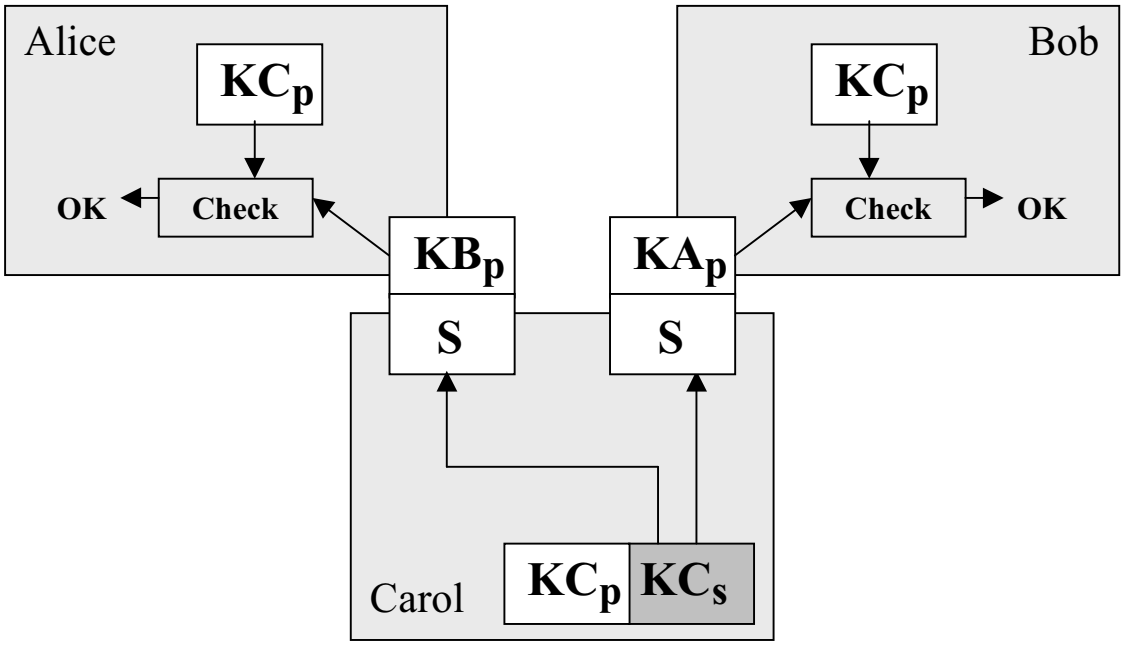
Sprostredkovateľ

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. 6).



Obr. 6 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. 7).



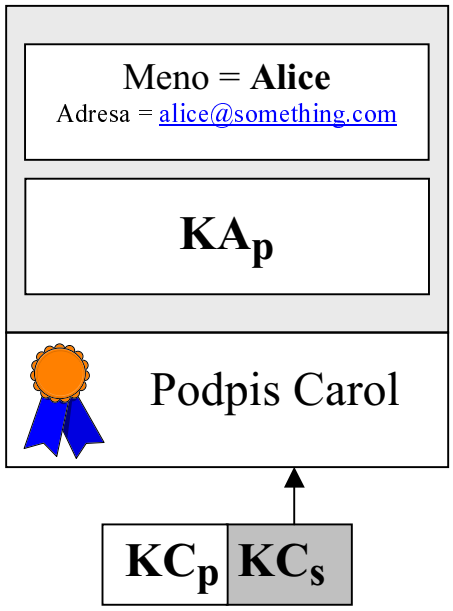
Obr. 7 Sprostredkovateľ - distribúcia kľúčov

Alica aj Bob si môžu spoľahlivo overiť Carolin podpis (S), keďže vlastnia jej verejný kľúč (KC_p). 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.

Certifikáty

V predchádzajúcom prípade Carol predstavovala Boba a Alice manuálne, pomocou podpísaných správ. Keďže tento proces „predstavovania“ sa pravdepodobne bude odohrávať často, bolo by výhodné ho formalizovať a automatizovať. Z tohoto dôvodu vznikla dátová štruktúra nazývaná *certifikát*.

Certifikát je spojenie identity subjektu (meno, adresa, ...) a verejného kľúča patriaceho subjektu. Toto spojenie je kryptograficky viazané digitálnym podpisom dôveryhodnej tretej strany. Ak by sme chceli uviesť certifikát pre Alice z nášho predchádzajúceho príkladu, vyzeral byt tak, ako je zobrazený na Obr. 8.

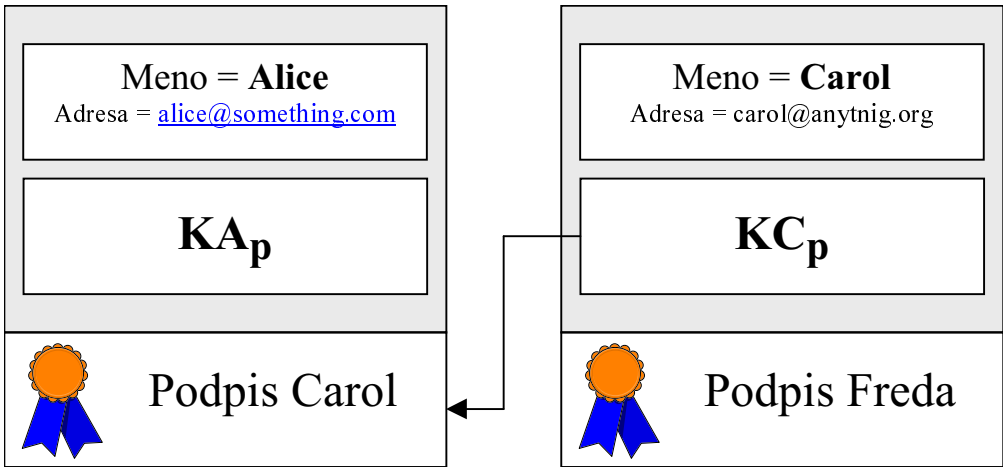


Obr. 8 Certifikát

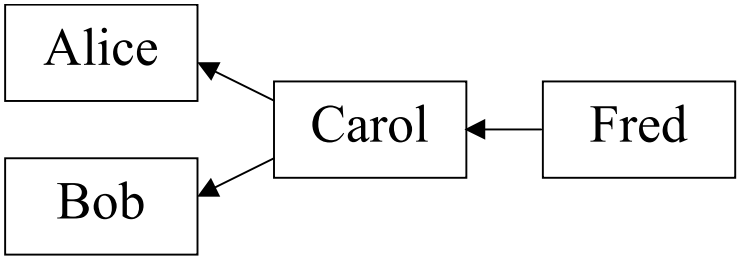
Certifikát obsahuje údaje o Alicinej identite, čiže jej meno a elektronickú adresu. K týmto údajom je pripojený Alicin verejný kľúč (KA_p) a celá táto štruktúra je podpísaná pomocou súkromného kľúča Carol (KC_s). Elektronický podpis chráni integritu celej štruktúry certifikátu pred modifikáciou. Takto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

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. 9). 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. 10. 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. 9 Reťazenie certifikátov



Obr. 10 Príklad hierarchie certifikátov

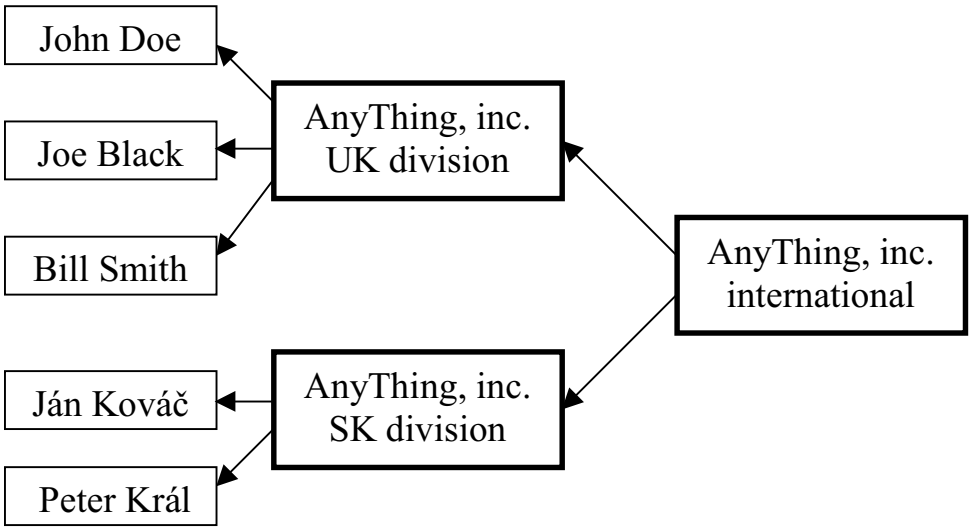
PKI – Infraštruktúra

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.

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. 11. 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.

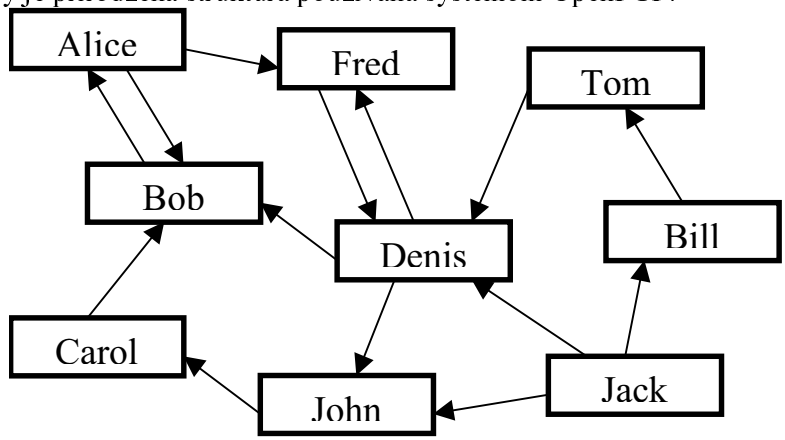
Hierarchia je najbežnejšia používaná štruktúra PKI, pretože dobre modeluje existujúce štruktúry reálneho sveta. Táto štruktúra je podporovaná štandardmi X.509, SSL, S/MIME, IPsec a mnohými ďalšími.



Obr. 11 Príklad hierarchie certifikačných autorít

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. 12. 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 OpenPGP.



Obr. 12 Pavučina dôvery

Certifikačná autorita

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 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.

Digital ID

Ako už bolo povedané, certifikát kryptograficky 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*[1], 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).

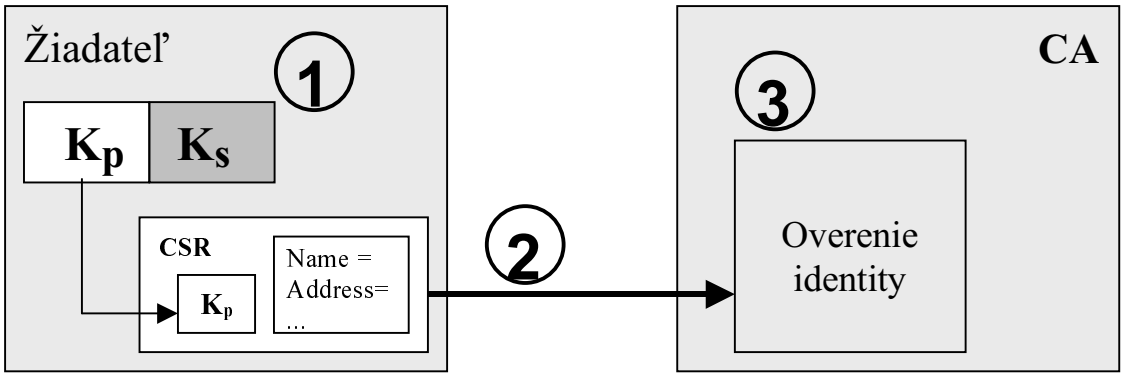
Krok 1	Generovanie páru kľúčov
Krok 2	Odoslanie žiadosti o certifikát (*certification request*)
Krok 3	Overenie totožnosti žiadateľa certifikačnou autoritou a podpísanie certifikátu
Krok 4	Odoslanie certifikátu žiadateľovi

Tab. 1 Proces certifikácie

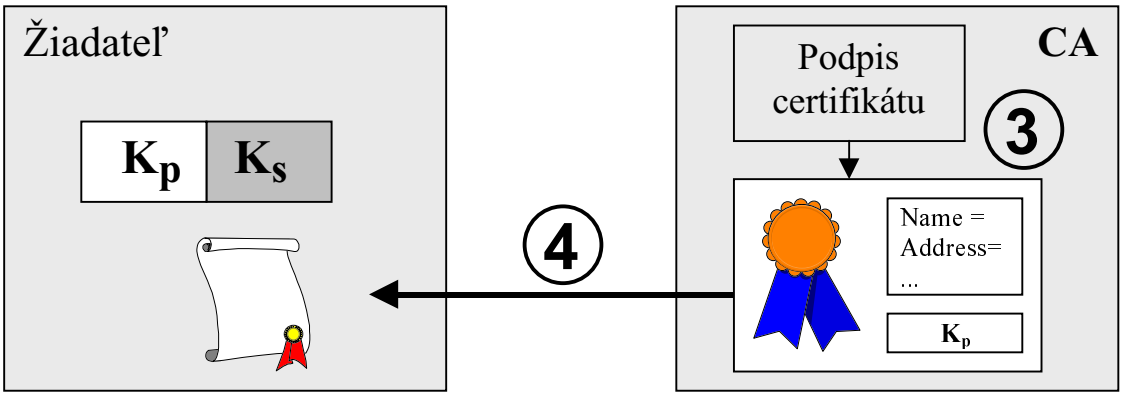
Prvým krokom je generovanie kľúčového páru na strane žiadateľa o certifikát. Vygenerovaný súkromný kľúč sa bezpečne uloží na strane žiadateľa a neprenáša sa na stranu certifikačnej autority, takže certifikačná autorita nemusí, a ani by nikdy nemala, poznať súkromný kľúč žiadateľa o certifikát. Druhým 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. Táto žiadosť o certifikát je odoslaná certifikačnej autorite. V treťom kroku si certifikačná autorita overí identitu žiadateľa o certifikát (Obr. 13). 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

[1] V prostredí Internetu a informačných systémov firiem je skôr známa jednoduchšia verzia štandardu *X.500* pod menom „LDAP directory“.

o jeho identite uloženými vo formáte X.509, čím vznikne výsledný certifikát (Obr. 14). Posledným krokom je odoslanie certifikátu žiadateľovi.



Obr. 13 Žiadosť o certifikát



Obr. 14 Podpis certifikátu

Odobraté certifikáty

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.

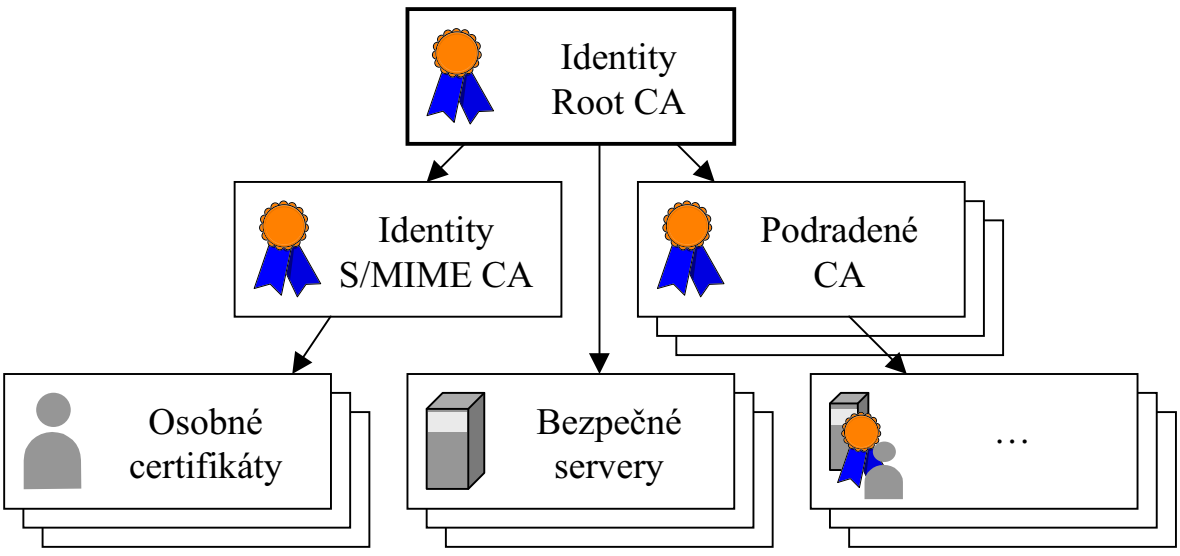
Identity

Certifikačná autorita Identity sa snaží riešiť nepriaznivú situáciu v oblasti bezpečnostných služieb Internetu na Slovensku. Identity sa snaží byť jednoduchou a každému prístupnou certifikačnou autoritou, podnecujúc tak nasadzovanie a rozvoj bezpečnostných technológií. Svojou jednoduchosťou a flexibilitou by mala zaujať širokú oblasť používateľov služieb Internetu ako aj prevádzkovateľov a vývojárov týchto služieb.
Pomocou osobných certifikátov vydávaných certifikačnou autoritou Identity je možné okamžite začať používať bezpečnostné mechanizmy elektronickej pošty. Navyše osobné certifikáty umožňujú používanie silných autentifikačných algoritmov, čo môže dramaticky zlepšiť bezpečnosť prístupu vzdialených používateľov k vášmu informačnému systému.

Certifikáty bezpečných serverov umožňujú prevádzkovateľom Internetových služieb (napr. WWW) okamžite zvýšiť bezpečnostnú úroveň svojich serverov inicializovaním transparentných kryptografických metód.
Certifikačná autorita Identity poskytuje aj možnosť vydávania certifikátov pre zreťazené podradené certifikačné autority, čo poskytuje plnú flexibilitu a splnenie aj tých najnáročnejších požiadaviek koncového zákazníka.

Infraštruktúra

Certifikačná autorita Identity je z bezpečnostných a funkčných dôvodov rozdelená na niekoľko úrovní (Obr. 15).
Najvyššiu úroveň tvorí koreňová certifikačná autorita „**Identity root CA**“. Táto certifikačná autorita je základom celej štruktúry. Na bezpečnosti kľúča koreňovej certifikačnej autority je založená bezpečnosť všetkých podradených štruktúr, preto je technické prevedenie „Identity root CA“ jedným z kľúčových prvkov systému. Systém, ktorý realizuje túto koreňovú certifikačnú autoritu je fyzicky zabezpečený a nie je pripojený priamo ani nepriamo do žiadnej komunikačnej siete. Prenos informácií medzi systémom koreňovej certifikačnej autority a okolitým svetom je realizovaný len pomocou výmenných médií dávkovým spôsobom. Dôležité informácie na médiách sú kryptograficky zabezpečené. Koreňová certifikačná autorita slúži na overovanie bezpečných serverov a podradených certifikačných autorít.
Overovanie jednotlivých používateľov, ak má byť flexibilné, sa musí realizovať automaticky. Pri automatickom overovaní je však nutné, aby aj privátny kľúč certifikačnej autority bol dostupný automatizovanému systému on-line. Nech je automatizovaný systém akokoľvek dobrý, vždy by tu bolo riziko prieniku a prezradenia privátneho kľúča certifikačnej autority. Z tohoto dôvodu sa automatické overovanie koncových používateľov nerealizuje pomocou koreňovej certifikačnej autority, ale podradenej „**Identity S/MIME CA**“. Táto certifikačná autorita slúži výhradne na automatické overovanie koncových používateľov.



Obr. 15 Infraštruktúra certifikačnej autority Identity

S/MIME – Bezpečná pošta

Štandard pre zabezpečenie elektronickej pošty S/MIME bol navrhnutý organizáciou RSA Labs. a prijatý množstvom výrobcov. 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 Identity 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 Tab. 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 Identity

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 Identity 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[2] 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.

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

[2] Všimnite si, že certifikačná autorita nikdy neuvidí váš súkromný kľúč. Kľúč generuje váš prehliadač a potom je uložený na disku vašej pracovnej stanice. Ani samotná certifikačná autorita nebude vedieť čítať vaše šifrované správy, dešifrovať ich môžete len vy.

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 Identity 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.

S/WAN – Bezpečné siete

Iniciatíva S/WAN (Secure WAN) vznikal na podnet RSA Laboratories a smeruje k vytvoreniu bezpečného prostredia pre rozľahlé a globálne počítačové siete. Hlavnou aktivitou iniciatívy S/WAN je podpora bezpečnostných rozšírení protokolovej rodiny TCP/IP – IPsec. IPsec je štandardizované rozšírenie TCP/IP prinášajúce bezpečnostné služby na sieťovú úroveň. Zabezpečenie je realizované už na úrovni IP paketov tak, že transportné a aplikačné dáta zostávajú nezmenené. Ochrana pomocou IPsec je teda pre aplikácie absolútne transparentná. Sieťové zariadenia, a v prípade mobilných alebo vzdialených používateľov aj sieťové operačné systémy, však musia dokázať medzi sebou komunikovať pomocou IPsec.
Automatická výmena kľúčov v IPsec je založená na certifikátoch. V globálnych sieťach je totiž takmer nemožné vytvoriť funkčný a efektívny bezpečnostný systém bez použitia kryptografickej infraštruktúry (PKI). Certifikačná autorita Identity by mala byť v dohľadnom čase schopná vydávať certifikáty aj pre zariadenia zabezpečené pomocou IPsec.

Záver

Rozvoj modernej kryptografie prispel k širokému rozšíreniu kryptografických bezpečnostných služieb, a tak spôsobil aj vznik infraštruktúry certifikačných autorít. Certifikačná autorita sa stáva základným stavebným prvkom siete dôvery, akousi elektronickou baštou moderného sveta. Dúfajme, že certifikačné autority nesklamú na ne vloženú dôveru a že ich služby budú vždy bezpečné a spoľahlivé.