Základy bezpečnosti v cloudových a gridových systémoch

Bezpečnosť zastáva široké pole záujmu v oblasti informačných technológií s veľmi rozmanitými cieľmi, ktoré môžu siahať od ochrany dôvernosti informácií, cez autentifikáciu a integritu údajov, až k zachovaniu dostupnosti služieb. Realizácia uvedených cieľov môže byť opäť implementovaná rôznymi spôsobmi. Môžu byť použité opatrenia ako ľudská kontrola prístupu, špeciálne hardvérové nástroje, či sofistikovaný bezpečnostný softvér a protokoly. Táto úvodná kapitola prináša základné pojmy, princípy a techniky zameriavajúce sa najmä na bezpečnostné aspekty, ktoré sú využívané alebo sú inak spojené so sieťovou bezpečnosťou a s cloudovými a gridovými technológiami.

Základné kryptografické pojmy

Kryptografia je základným kameňom bezpečnosti údajov v tradičných informačných technológiách a nie je tomu inak ani pri cloudových a gridových technológiách. Kryptografia sa zaoberá dvoma základnými bezpečnostnými konštrukciami: dôvernosťou údajov a integritou údajov. Práve šifrovanie je v kryptografii dôležitým nástrojom na ich zabezpečenie.

Šifrovanie dát je proces, ktorým sa nezabezpečené (otvorené) elektronické dáta prevádzajú za pomoci kryptografie na dáta zašifrované, čitateľné len pre majiteľa kryptografického kľúča. Šifrovanie dát slúži na ich ochranu proti ich nežiaducemu zisteniu cudzou, neautorizovanou osobou a uplatňuje sa pri ukladaní dát aj pri ich prenose cez sieť.

Symetrické/asymetrické kryptosystémy

Pojem kryptosystém je možné intuitívne chápať ako systém umožňujúci šifrovanie a dešifrovanie správ.

Kryptosystémy sa v súčasnosti delia na dve skupiny: na *symetrické* kryptosysystémy a kryptosystémy *verejného kľúča* (asymetrické kryptosystémy).

Symetrické kryptosystémy patria medzi historicky staršie a sú postavené na symetrickom šifrovaní, t. j. na šifrovanie a aj dešifrovanie správy používajú rovnaký kľúč. Súčasným symetrickým šifrovacím štandardom je šifra AES (Advanced Encryption Standard). V praxi sa objavujú aj ďalšie symetrické šifry, ako napr. 3DES, či ChaCha20.

Hoci sú symetrické šifry rýchle, ich nevýhodou je nutnosť zdieľania rovnakého tajného kľúča na obidvoch stranách a nevyhnutnosť jeho bezpečnej výmeny pred šifrovanou komunikáciou.

Kryptosystémy verejného kľúča sú postavené na asymetrickom šifrovaní, t. j. na zašifrovanie správy používajú verejný kľúč a na dešifrovanie iný, privátny (tajný) kľúč, pričom nie je možné (výpočtovo zvládnuteľné) odvodiť jeden kľúč od druhého.

Jedným z najpoužívanejších kryptosystémov verejného kľúča je algoritmus od autorov Rivesta, Sharmira a Adlemana, známy ako RSA algoritmus [RSA78]. Kryptografická sila algoritmu je založená na obťažnosti faktorizácie veľkých zložených čísel.

V praxi je symetrické šifrovanie často používané v kombinácii s asymetrickým šifrovaním, pričom sa využívajú výhody každého z nich, t. j. rýchlosť symetrického šifrovania a dostupnosť verejného šifrovacieho kľúča v asymetrickom šifrovaní. Správa je potom v praxi symetricky zašifrovaná náhodne vygenerovaným symetrickým tajným kľúčom, ktorý je následne zašifrovaný asymetrickým verejným kľúčom príjemcu, ktorý môže dešifrovať jedine vlastník asymetrického privátneho kľúča.

Hašovacia funkcia

Hašovacie funkcie používané v kryptológii sú algoritmy, ktoré z ľubovoľne dlhého vstupu vypočítajú reťazec bitov pevnej dĺžky, nazývaný aj odtlačok hašovacej funkcie. Napr. zo súboru veľkosti 200MB vyrobí hašovacia funkcia SHA-512 odtlačok s pevnou dĺžkou 512 bitov. Samostatné použitie hašovacej funkcie slúži na kontrolu integrity údajov, tzn. že dáta neboli neoprávnene zmenené.

Hašovacia funkcia h je funkcia minimálne s dvomi nasledujúcimi vlastnosťami [MOV96]:

(i) kompresia – funkcia h zobrazuje vstupné údaje x ľubovoľnej dĺžky na výstupnú hodnotu $h(x)$ pevnej bitovej dĺžky,

(ii) jednoduchosť výpočtu – pre zvolenú funkciu h a vstup x je ľahké vypočítať hodnotu $h(x)$.

Funkciu $f: X \rightarrow Y$ nazývame jednosmernou (jednocestnou), keď pre každé $x \in X$ je výpočtovo ľahké[1] vypočítať hodnotu $y = f(x)$, ale pre náhodne zvolené $y \in Y$ je nemožné (výpočtovo obťažné) nájsť $x \in X$ tak, aby platilo $f(x) = y$. To znamená, že ktokoľvek vie hašovací odtlačok vypočítať k ľubovoľnému vstupu a tento odtlačok je jednoznačne určený (pre rovnaký vstup je odtlačok vždy ten istý). Spätne to nie je možné, nie je možné z hašovacieho odtlačku určiť pôvodnú správu.

Okrem toho, funkciu $f: X \rightarrow Y$, pre ktorú je výpočtovo nemožné pre danú hodnotu x nájsť hodnotu $x_0 \in X$ takú, že $f(x) = f(x_0)$, nazývame *slabo bezkolíznou*. To znamená, že k jednej správe nie je možné (výpočtovo zvládnuteľné) nájsť inú s rovnakým odtlačkom.

[1] Problémy, ktoré sú riešiteľné v polynomiálnom čase sa považujú za výpočtovo zvládnuteľné alebo ľahké. Problémy, ktoré vyžadujú čas horší ako polynomiálny čas, sa nazývajú výpočtovo nezvládnuteľné, výpočtovo nemožné, resp. ťažké [MOV96].

A funkciu $f: X \rightarrow Y$, pre ktorú je výpočtovo nemožné nájsť dve rôzne hodnoty $x_{1,2} \in X$ také, že $f(x_1) = f(x_2)$, nazývame *silno bezkolíznou*. To znamená, že nie je možné (výpočtovo zvládnuteľné) nájsť dve rozdielne správy s rovnakým odtlačkom. Je potrebné zdôrazniť, že správy s rovnakým odtlačkom existujú, nie je ich však možné na základe opisu algoritmu hašovacej funkcie nájsť[2].

Od hašovacích funkcií používaných v bežných kryptografických systémoch sa požaduje:

(i) popis funkcie *h* je verejný a neobsahuje žiadne tajné prvky,
(ii) funkcia *h* je jednosmerná a silne bezkolízna.

V súčasnej dobe sa využíva hlavne funkcia SHA-2 označovaná aj podľa dĺžky odtlačku ako SHA-256, SHA-384 a SHA-512 a neodporúča sa už používanie starších štandardov funkcií MD5, SHA-1 a RIPEMD160, ktoré nespĺňajú podmienku bezkolíznosti. Novými sú štandardy SHA3-256, SHA3-384 a SHA3-512.

Podpisová schéma

Digitálnym podpisom je reťazec dát, ktorý asociuje správu (v digitálnej podobe) s entitou, ktorá podpis vytvorila, pričom použila algoritmus na generovanie digitálneho podpisu [MOV96]. Inak povedané, digitálny podpis je ekvivalentom písaného podpisu a používa sa na podpísanie, teda potvrdenie originality elektronického dokumentu, t. j. na potvrdenie, že údaje sa nezmenili a sú správne.

Algoritmom verifikácie digitálneho podpisu (verifikačný algoritmus) je metóda pre verifikáciu digitálneho podpisu, ktorá overí, či je digitálny podpis autentický, t. j. či bol naozaj vytvorený predpísanou entitou. Algoritmus tak overí správnosť podpisu.

Podpisová schéma pozostáva z (matematického) algoritmu na generovanie digitálneho podpisu a z príslušného verifikačného algoritmu a vychádza z vlastností asymetrického šifrovania [MOV96].

Od podpisových schém používaných v bežných kryptografických schémach sa požaduje [Sta99]:

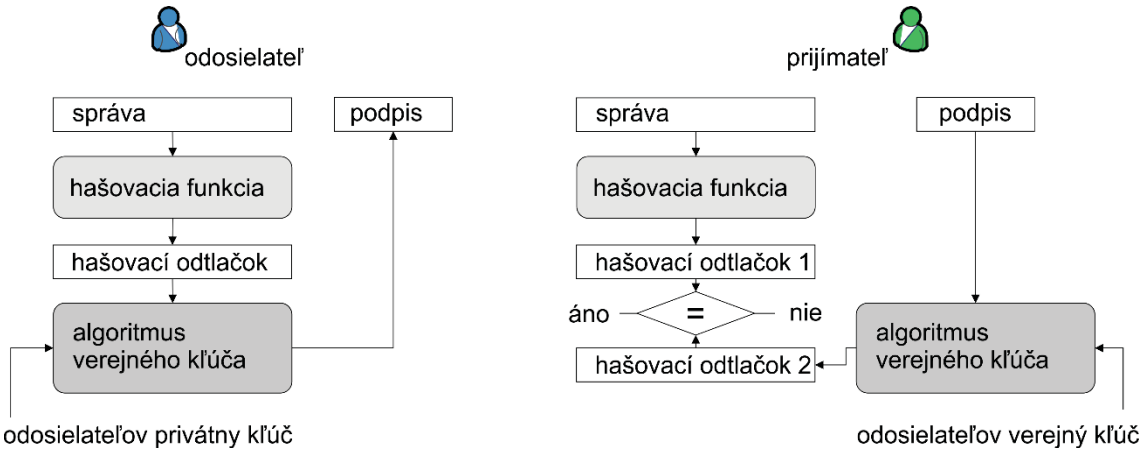
- digitálny podpis musí byť bitovým obrazcom závislým od správy, ktorá bola podpísaná,
- digitálny podpis musí používať informácie jedinečné pre odosielateľa, aby sa zabránilo popretiu a podvrhu,
- v schéme musí byť relatívne jednoduché vytvoriť digitálny podpis,
- musí byť relatívne jednoduché rozpoznať a verifikovať digitálny podpis,

[2] Napr. pre hašovaciu funkciu s veľkosťou odtlačku 128 bitov stačí zobrať množstvo správ $2^{128}+1$ a určite dve správy musia mať rovnaký odtlačok. Na druhej strane, vygenerovanie takéhoto obrovského počtu správ nie je v súčasnosti výpočtovo zvládnuteľné.

- musí byť výpočtovo nezvládnuteľné sfalšovať digitálny podpis, či už vytvorením novej správy k existujúcemu digitálnemu podpisu, alebo vytvorením falošného digitálneho podpisu pre existujúcu správu,
- kópia digitálneho podpisu sa musí dať vhodne zálohovať.

Zvyčajne je digitálny podpis vytvorený nasledovným postupom: z podpisovaného (digitálneho) dokumentu je vytvorený hašovací odtlačok, pričom akákoľvek zmena v dokumente spôsobí, že zmenený dokument už nesúhlasí s vypočítaným odtlačkom. Následne je na odtlačok aplikovaná asymetrická šifra s použitím privátneho kľúča podpisovateľa, čo už okrem integrity zaistí aj nepopierateľnosť autorstva. Príjemca si pravosť podpisu overí aplikovaním asymetrického šifrovania s použitím verejného kľúča podpisovateľa, čím získa pôvodný odtlačok dokumentu a ten si porovná s vygenerovaným odtlačkom z overovaného dokumentu. Ak sú odtlačky zhodné, digitálny podpis je platný, Obrázok 0-1.

V súčasnosti medzi najpoužívanejšie podpisové schémy patria RSA, DSA a ECDSA.



Obrázok 0-1 Vytvorenie a overenie digitálneho podpisu.

Autentifikácia

Proces *autentifikácie* je zvyčajne chápaný ako potvrdenie identity určitej entity (t. j. autentifikovaného subjektu), alebo ubezpečenie, že IT systém alebo IT služba je dôveryhodná. Existuje celý rad postupov a mechanizmov na zabezpečenie autentifikácie. Medzi základné metódy pre overenie identity patrí:

- niečo, čo používateľ má (technický prostriedok, napr. hardvérové tokeny, čipové karty, privátny kľúč alebo mobilný telefón),
- niečo, čo používateľ vie (napr. heslo alebo PIN),
- niečo. čím používateľ je alebo nie je (biometrické vlastnosti, napr. hlas, odtlačky prstov, geometria tváre…).

V poslednej dobe sa v IT systémoch do popredia dostáva aj štvrtý faktor, ktorým je sociálna sieť pre používateľa [BJR+06], alebo inými slovami:

- niekto, koho používateľ pozná.

Okrem uvedených spôsobov môžu byť požadované aj ďalšie metódy overovania vychádzajúce z aplikačnej domény, napr. autentifikácia na základe lokality (za účelom zabrániť používaniu kreditných kariet na dvoch miestach) alebo autentifikácia na základe času (napr. umožniť prístup iba v úradných hodinách).

V súvislosti s informačnými systémami sú zvyčajne využívané kryptografické metódy pre stanovenie pravosti ako digitálny podpis, založený na asymetrickej kryptografii, či MAC kóde (Message Authentication Code), založený na symetrickej kryptografii, a ktoré sa dodnes považujú za spoľahlivé, ak pôvodný privátny/tajný kľúč nebol kompromitovaný.

Autorizácia

Úlohou procesu *autorizácie* je rozhodnúť, či bude požadovanému subjektu umožnený prístup k určitým IT zdrojom. Prístup je udeľovaný iba tým používateľom, ktorým bolo povolené dané zdroje používať. Takéto oprávnenie môže byť uvádzané napr. pomocou zoznamu na riadenie prístupu (Access Control Lists, ACL), v ktorom sú uvedené subjekty zadávané vlastníkom zdrojov, prípadne správcom zdrojov. Zdroje môžu zahŕňať všetky typy dát, aplikácie, zariadenia alebo služby, ku ktorým je potrebné sa autorizovať. K zdrojom môžu mať prístup buď používatelia, alebo iné zdroje.

V zásade sa proces autorizácie deje na základe autorizačných informácie, ktoré poskytuje určitá autorita. Takéto autority musia mať priamy alebo prenesený (pridelený, delegovaný) vzťah buď k autorizovanému subjektu, napr. používateľ alebo člen organizácie, ktorej je povolenie vydané, alebo musia mať priamy vzťah k zdroju, ktorý je predmetom žiadosti autorizácie, ako napr. vlastník alebo správca zdroja. Uvedené vzťahy môžu byť realizované pomocou mechanizmov dôvery založených na niektorých kryptografických metódach, napr. pomocou asymetrickej kryptografie, alebo môžu byť vykonávané nezávisle pomocou iných dôveryhodnými mechanizmov.

V procese autorizácie vystupujú tri základné entity [BGM+03]:

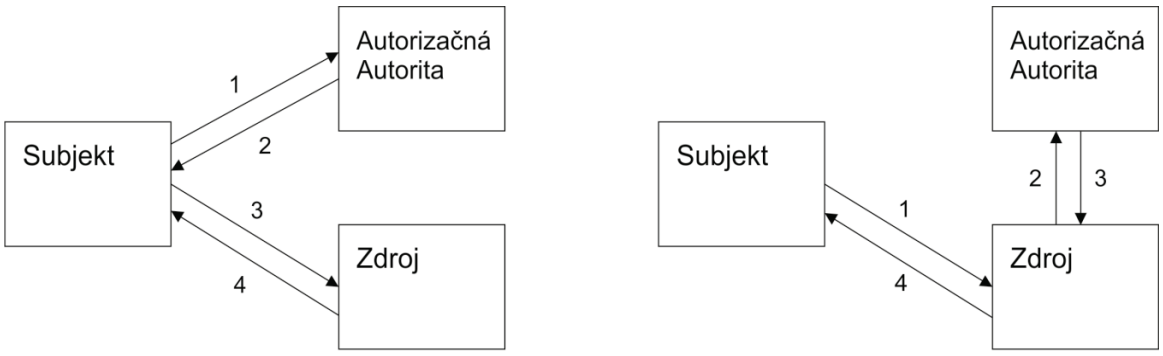
Subjekt: entita (napr. osoba alebo proces), ktorý môže požadovať, prijímať, vlastniť, presúvať, prezentovať alebo delegovať autorizáciu na vykonanie určitých práv. Subjekt môže byť identifikovaný ako jednotlivý používateľ, alebo ako člen skupiny používateľov. Subjektom môže byť aj proces, ktorý koná v mene iného používateľa a ako taký má delegované prístupové práva od daného používateľa.

Zdroj: Komponent systému, ktorý poskytuje alebo hostí služby a môže pripustiť iné entity k týmto službám na základe súboru pravidiel a politík definovaných entitami, ktoré spravujú alebo riadia daný zdroj. Typickými zdrojmi v cloudovom/gridovom prostredí môžu byť počítače poskytujúce výpočtovú kapacitu, alebo poskytujúce úložný dátový priestor. Prístup k zdroju môže byť uskutočňovaný priamo samotným zdrojom, alebo inou entitou (Enforcement Point, gateway), ktorá je umiestnená medzi zdroj a žiadateľov, a tak chráni zdroj pred neoprávneným prístupom.

Autorita: Administratívna jednotka, ktorá je zodpovedná za vydávanie, overovanie a rušenie elektronických potvrdení s tým, že držiteľ daného potvrdenia je oprávnený na výkon určitých práv, alebo mu prislúchajú určité vlastnosti. Práva môžu byť implicitne alebo explicitne prítomné v elektronickom potvrdení. Navyše, súbor politík môže určovať ako sa povolenie vydáva, či overuje, atď.

Z pohľadu cloudových/gridových systémov je autorizáciu možné zjednodušene definovať ako dohodu medzi vlastníkom zdrojov a používateľmi, pričom prístup k zdrojom je vo všeobecnosti kontrolovaný obidvomi stranami na základe rozličných rolí.

Autorizácia je často delená na tri nadväzujúce kroky: 1) definovanie autorizačnej politiky na vysokej úrovni určitou osobou alebo organizáciou, 2) implementácia danej politiky do digitálnej podoby, ktorá môže byť interpretovaná počítačom, 3) hodnotenie digitálnej podoby politiky procesom, ktorý následne rozhodne o vydaní osobitného povolenia subjektu alebo vykoná určitú akciu [L+03].



a) Autorizačný push model b) Autorizačný pull model

Obrázok 0-2 Delenie autorizácie podľa spôsobu vyžiadania povolenia.

Autorizácia rozlišuje dva základné modely žiadostí o povolenie, tzv. push model a tzv. pull model, Obrázok 0-2.

Autorizačný push model: V tomto modeli najskôr subjekt žiada o autorizačné povolenie od príslušnej autority (napr. autorizačný server). Autorita môže, ale nemusí akceptovať žiadosť daného subjektu. V prípade akceptovania, autorita vydá pre daný subjekt zabezpečené potvrdenie (token alebo certifikát), ktoré slúži ako doklad o oprávnení využívať práva v ňom uvedené. Tradične má takéto potvrdenie určitú časovú platnosť. Potvrdenie môže byť následne použité subjektom pri žiadosti o stanovenú službu kontaktovaním príslušného zdroja. Zdroj akceptuje alebo odmietne predložené autorizačné potvrdenie a spätne to oznámi žiadajúcemu subjektu. Príklady autorizačného pull modelu sa nachádzajú v mnohých systémoch založených na použití tzv. lístkov/tokenov vydávaných centrálnym serverom ako Kerberos [NT94] alebo Keynote [RFC2704].

Autorizačný pull model: V tomto prípade subjekt so žiadosťou priamo kontaktuje zdroj. Aby bolo možné prijať alebo odmietnuť požiadavku na stanovenú službu, musí

zdroj kontaktovať autorizačnú autoritu. Autorizačná autorita vykoná rozhodnutie o autorizácii a vráti zdroju správu, ktorá obsahuje výsledné autorizačné rozhodnutie. Zdroj následne akceptuje alebo odmietne poskytnutie služby danému subjektu, o čom mu zašle správu. Napr. v gridovom prostredí je tento postup realizovaný v autorizačných systémoch PERMIS [CO02] a Akenti [TEM03].

Certifikáty

Pri verifikácii digitálneho podpisu, ale taktiež pri odosielaní zašifrovanej správy je potrebná dôveryhodná znalosť verejného kľúča príjemcu, t. j. či daný verejný kľúč naozaj patrí uvedenému vlastníkovi. Distribúciu kľúčov je možné riešiť pomocou tretej strany, ktorej dôverujú všetky zúčastnené entity.

Certifikačná autorita (CA) je dôveryhodná tretia strana, ktorej podpis zaručuje pravosť verejného kľúča zviazaného s vlastníkom uvedeným v certifikáte.

Certifikát verejného kľúča je dátová štruktúra, ktorá pozostáva z *dátovej časti* a *podpisovej časti*. Dátová časť pozostáva z textovej časti, a minimálne z verejného kľúča a reťazca identifikujúceho účastníka/vlastníka (*entitu subjektu*). Podpisová časť pozostáva z digitálneho podpisu dátovej časti, ktorý je vytvorený certifikačnou autoritou, čím je previazaná identita vlastníka so špecifikovaným verejným kľúčom [MOV96].

Formálne je certifikát verejného kľúča možné zapísať ako:

$Cert_{id}(U) = (cert(ID(U), pk_U), sig_{CA}(ID(U), pk_U))$,

kde *cert* je dátová časť certifikátu, pričom *ID(U)* je informácia o identite a pk_U je verejný kľúč entity uvedenej v certifikáte; $sig_{CA}(ID(U), pk_U)$ je digitálny podpis vytvorený CA.

Entita, využívajúca informácie z certifikátu musí vlastniť verejný kľúč CA[3], ktorá certifikát digitálne podpísala, aby bola schopná verifikovať jeho integritu. Verejný kľúč CA je možné získať z certifikátu CA.

Pri pojme certifikátu je potrebné brať do úvahy, že existuje množstvo rozdielnych typov certifikátov, ako napr.:

- X.509 certifikát verejného kľúča,
- certifikát štandardu Simple Public Key Infrastructure (SPKI),
- Pretty Good Privacy (PGP) certifikát,
- X.509 atribútový certifikát.

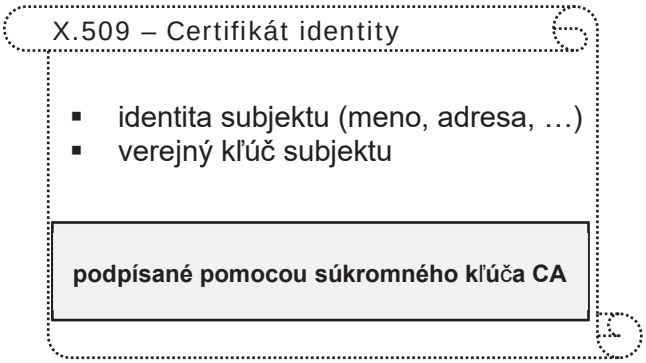
[3] Množstvo renomovaných svetových certifikačných autorít má svoje certifikáty s verejným kľúčom už priamo zahrnuté vo webových prehliadačoch ako sú Google Chrome, MS Edge, Firefox, či Opera a odpadá tým potreba získavať verejný kľúč bezpečne od certifikačnej autority.

Certifikáty identity

Certifikáty verejného kľúča sa zvyknú označovať aj ako certifikáty identitovo-orientované, resp. certifikáty identity, keďže spájajú verejný kľúč s identitou vlastníka certifikátu, ako je tomu v štandarde X.509 a PGP.

Štandard X.509 využíva striktne hierarchický a centralizovaný model dôvery. Na overenie podpisu certifikátu je nutný verejný kľúč certifikačnej autority, ktorá certifikát vydala, pričom je potrebné získať jej certifikát, v ktorom je kľúč uvedený. Certifikát certifikačnej autority je podpísaný nadriadenou certifikačnou autoritou, jej verejný kľúč je uvedený v ďalšom certifikáte, ktorý bol vydaný jej nadriadenou CA, atď., až k najvyššej koreňovej CA. Jednotlivé po sebe nasledujúce certifikáty vytvárajú postupnosť certifikátov – *reťazec certifikátov*[4], ktorý je potrebný na overenie dôveryhodnosti certifikátu koncového používateľa.

PGP model na druhej strane využíva filozofiu dôvery založenej na *sieti dôvery* (Web-of-Trust), kde každý uzol môže byť certifikačnou autoritou, každý používateľ môže vydať certifikát inému používateľovi [Zim95].



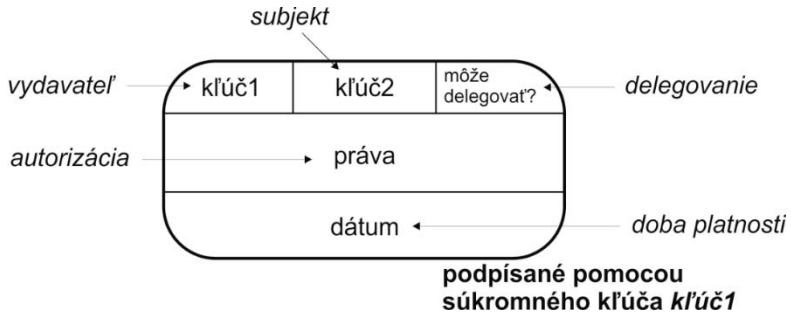
Obrázok 0-3 X.509 certifikát identity.

Autorizačné certifikáty

Rozdielnym prístupom k certifikátom je *autorizačný prístup*. Autorizačný prístup využíva certifikáty nielen na väzbu medzi identitou a verejným kľúčom, ale aj na autorizáciu, ktorá zaručí povolenie vlastníka certifikátu na dosiahnutie určitej služby. Autorizačnými certifikátmi sú napríklad certifikát na písanie elektronických šekov, certifikát na riadenie auta, certifikát na otvorenie garážovej brány …

Obrázok 0-4 uvádza štruktúru autorizačného certifikátu, pričom sú zobrazené základné položky certifikátu: vydavateľ certifikátu; subjekt, pre ktorý bol certifikát vydaný; možnosť ďalšieho delegovania práv; práva uvedené v certifikáte a doba platnosti certifikátu.

[4] Dĺžka reťazca X.509 certifikátov sa zvyčajne pohybuje v rozmedzí od 2 do 15 certifikátov.



Obrázok 0-4 Autorizačný certifikát.

Formálne je autorizačný certifikát možné zapísať ako:

$Cert_{aut}(U) = (cert(pk_U, right), sig(pk_U, right)),$

kde *cert* je dátová časť certifikátu, pričom pk_U je verejný kľúč entity a *right* sú práva delegované entite jednoznačne určenej pomocou pk_U; $sig(pk_U, right)$ je digitálny podpis vytvorený entitou, ktorá práva delegovala.

Atribútové certifikáty

Atribútové certifikáty sú navrhnuté na poskytnutie určitých informácií – atribútov, iných ako je verejný kľúč subjektu, ale relevantných k entite, príp. jej verenému kľúču, na ktorú sa atribúty vzťahujú. Atribútové certifikáty prepájajú atribúty s príslušnou identitou. Zväčša sa k atribútovému certifikátu prikladá aj certifikát verejného kľúča. Atribútové certifikáty sú podpísané atribútovou autoritou [MOV96].

Formálne je atribútový certifikát možné zapísať ako:

$Cert_{att}(U) = (cert(ID(U), attr), sig_{AA}(ID(U), attr)),$

kde *cert* je dátová časťcertifikátu, pričom *ID(U)* je informácia o identite a *attr* sú atribúty zviazané s entitou uvedenou v certifikáte; $sig_{AA}(ID(U), attr)$ je digitálny podpis vytvorený atribútovou autoritou.

Zrušenie certifikátu

Certifikát podľa štandardu X.509 je platný v časovom rozpätí uvedenom v položke Validity period. Platnosť certifikátu je možné zrušiť aj predčasne v prípade odcudzenia, straty súkromného kľúča, príp. odchodu pracovníka z organizácie. Na základe žiadosti klienta o zrušenie certifikátu je certifikát zahrnutý do zoznamu zrušených certifikátov (Certificate Revocation List – CRL), ktorý je zverejnený certifikačnou autoritou. Zoznamy zrušených certifikátov vydáva CA periodicky, pričom nový CRL ruší platnosť predchádzajúceho.

Verifikácia reťazca certifikátov

Pri verifikovaní reťazca certifikátov je potrebné prejsť celým reťazcom.

Verifikujúci musí skontrolovať, či je prvý certifikát v reťazci podpísaný súkromným kľúčom vydavateľa certifikátu, pomocou verifikácie digitálneho podpisu certifikátu. Ďalej musí skontrolovať, či je druhý certifikát v reťazci podpísaný súkromným kľúčom

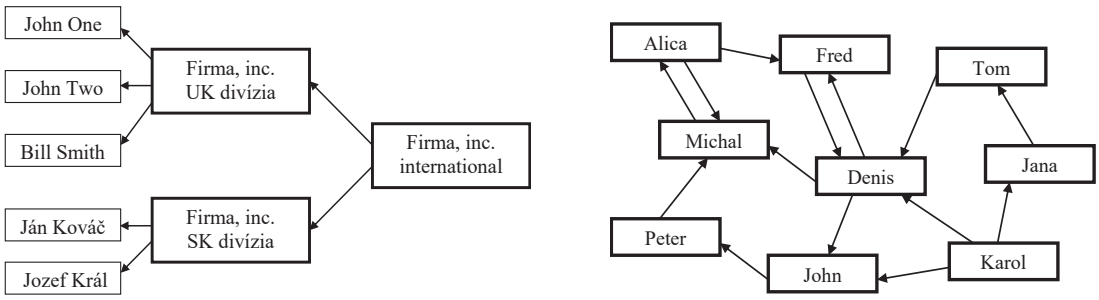
kľúča umiestneného v prvom certifikáte, potom či tretí certifikát súkromným kľúčom kľúča v druhom certifikáte, atď.

Verifikujúci musí taktiež vypočítať periódu platnosti reťazca ako prienik periód platnosti všetkých certifikátov v reťazci. Takúto verifikáciu reťazca nazývame klasická verifikácia reťazca certifikátov. Navyše vypršanie doby platnosti jedného certifikátu v reťazci automaticky znamená, že už nie je potrebné skúmať dobu platnosti zvyšných certifikátov v reťazci.

Model dôvery

Hlavným pilierom využitia digitálnych certifikátov v rámci infraštruktúry verejného kľúča (PKI, Public Key Infrastructure) je dôvera. Presné stanovenie a úroveň dôvery sú definované modelom dôvery. Model dôvery v PKI definuje ako je vytvorená a udržiavaná dôvera medzi vydavateľom certifikátu a tým, kto certifikát overuje, Obrázok 0-5. Medzi tri základné modely dôvery patria:

- hierarchický model PKI,
- krížová certifikácia,
- decentralizovaný model (Web of Trust).



Obrázok 0-5 Hierarchický model PKI verzus decentralizovaný Web of Trust [M04].

Hierarchický model PKI: Hierarchický model vyžaduje koreňovú (root) autoritu, ktorá je dôveryhodná pre všetkých účastníkov. V reálnom svete, t. j. v globálnom meradle na Internete, niečo ako centrálna koreňová certifikačná autorita neexistuje. Preto krajiny, príp. medzinárodné spoločnosti alebo nadnárodné projekty využívajú hierarchický model PKI s vlastnou koreňovou certifikačnou autoritou. Dôvodom je, že prevádzkovatelia PKI preferujú skôr plnú kontrolu nad pravidlami v PKI (napr. politika vydávania certifikátov) ako dôveru ďalšej, cudzej certifikačnej autorite.

Krížová certifikácia: Jedna z možností používanie certifikátov prostredníctvom viac hierarchických PKI je krížová certifikácia. Dve certifikačné autority (väčšinou koreňové certifikačné autority) si vydajú navzájom krížové certifikáty s cieľom vytvoriť vzťah dôvery medzi všetkými účastníkmi oboch PKI. Hlavným problémom krížovej certifikácie je jej miera, pretože počet krížových certifikátov kvadraticky narastá s počtom koreňových certifikátov. Možným riešením je zavedenie neutrálnej CA, tzv. mostu, resp.

mostovej CA, ktorá sprostredkováva krížové certifikáty so všetkými zúčastnenými autoritami a tak pomocou krížových certifikátov vybudovať vzťah dôvery medzi jednotlivými PKI. V takomto modeli predstavuje mostová CA centrum dôvery.

Decentralizovaný model Web of Trust: Model Web of Trust predstavuje nehierarchický koncept na zabezpečenie autentifikácie previazania medzi verejným kľúčom a používateľom. Ako alternatíva k hierarchickému modelu dôvery, ktorý je založený na jednej alebo viacerých certifikačných autoritách, je model decentralizovaný pre každého používateľa, ktorý má svoju vlastnú sieť dôveryhodných používateľov, ktorí zase dôverujú iným, atď., čím vzniká určitá „sieť dôvery“. Navyše dôveryhodní používatelia sa môžu svojim podpisom zaručiť za dôveru pre používateľa neznámych subjektov. Tento model po prvýkrát formuloval Phil Zimmermann, autor Pretty Good Privacy (PGP) systému [Zim95].