Elektronický podpis v praxi

Radovan Semancík

Elektronický podpis a témy, ktoré sú s ním spojené, si v poslednom čase získali veľkú popularitu u odbornej aj laickej verejnosti. Elektronický podpis je jedným z hlavných technologických nástrojov budovania infraštruktúry verejných kľúčov (public key infrastructure, PKI). A práve PKI sa považuje za jeden z rozhodujúcich prvkov pri rozbiehaní efektívneho a bezpečného elektronického obchodu a uplatňovaní globálnych informačných systémov.

Elektronický podpis

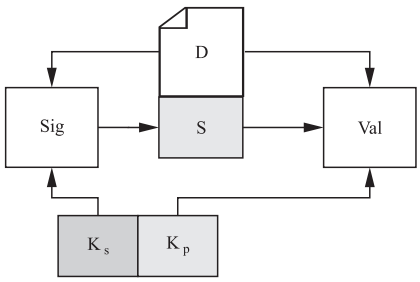
Pojem „elektronický podpis" je v oblasti informačných technológií pomerne nový. Viac sa o ňom začalo rozprávať až koncom sedemdesiatych a začiatkom osemdesiatych rokov, keď nástup asymetrickej kryptografie poskytol dostatok nástrojov na vytváranie a overovanie elektronických podpisov. V súčasnosti je drvivá väčšina aplikácií elektronického podpisu založená práve na metódach asymetrickej kryptografie a je reprezentovaná v digitálnej forme ako reťazec číselných údajov. V takejto podobe je elektronický podpis (S) výsledkom funkcie (Sig), ktorej parametrami sú podpisovaný dokument (D) a súkromný kľúč podpisovateľa (K_s). Na overovanie (Val) elektronického podpisu sa potom používa verejný kľúč podpisovateľa (K_p). Keďže podpis je funkciou obsahu dokumentu, modifikáciou dokumentu sa elektronický podpis stáva neplatným. Takto podpísaný dokument je možné transportovať pomocou nedôveryhodných komunikačných kanálov bez rizika nedetekovaného porušenia integrity dokumentu.

Hlavným problémom pri overovaní podpisu je však identita osoby, ktorá dokument podpísala. Bez dodatočného overenia verejného kľúča podpisujúcej osoby si príjemca podpísanej správy nemôže byť istý, že autorom podpisu je skutočne správna osoba. A práve na overovanie identity podpisujúcej osoby je nutné vytvoriť zložité štruktúry a mechanizmy infraštruktúry verejných kľúčov (PKI).

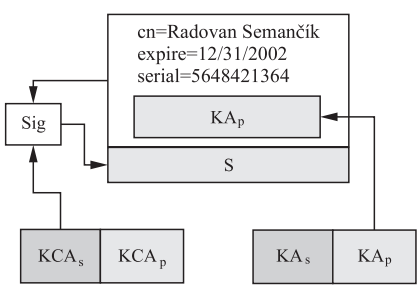
Infraštruktúra verejných kľúčov

Ako už bolo spomenuté, jedným z hlavných problémov pri používaní elektronického podpisu v reálnych systémoch je dostatočne dôveryhodná väzba medzi verejným kľúčom osoby a jej identitou. V prostredí otvorených sietí ako je napríklad internet väčšinou neexistuje dôveryhodný kanál na distribúciu kľúčového materiálu. Vzťahy dôvery medzi každými dvomi subjektmi v systéme by predstavovali štruktúru kvadratickej zložitosti, navyše silne distribuovanú a zle manažovateľnú. Preto v moderných rozsiahlych distribuovaných systémoch je jediným efektívnym riešením použitie dôveryhodnej tretej strany (trusted third party), ktorá slúži ako centrálna autorita pre správu verejných kľúčov a identít koncových entít v systéme.

V terminológii PKI sa takáto dôveryhodná tretia strana označuje ako certifikačná autorita (CA). Jej primárnou úlohou je vydávať certifikáty, ktoré dôveryhodným spôsobom viažu verejný kľúč entity (KA_p) s jej identifikáciou (napr. menom, sieťovou adresou atď.). Táto väzba je realizovaná dátovou štruktúrou, ktorá je podpísaná súkromným kľúčom certifikačnej autority (KCA_s). Takto vytvorená a podpísaná štruktúra sa nazýva certifikát verejného kľúča (public key certificate, PKC) alebo jednoducho digitálny certifikát. Zjednodušený príklad digitálneho certifikátu je na obr. 2. Digitálny certifikát väčšinou obsahuje okrem mena certifikovaného subjektu aj iné údaje, ako napríklad dobu platnosti certifikátu, sériové číslo, obmedzenia použitia certifikátu atď. Takto vydaný certifikát je potom možné overiť pomocou verejného kľúča certifikačnej autority (KCA_p), ktorý musí byť verejne známy. Formát digitálneho certifikátu je definovaný všeobecne uznávaným štandardom ITU-T X.509 [1], niektoré systémy však definujú svoje vlastné formáty, väčšinou z historických a implementačných dôvodov. Štandard X.509 vo verzii 3 pripúšťa rozširovanie certifikátu o ľubovoľné hodnoty, čo prináša veľký stupeň flexibility a voľnosti pre systémy implementujúce PKI. Na druhej strane však táto voľnosť viedla k množstvu rôznych variantov použitia X.509 certifikátov, čo viedlo k zníženej interoperabilite PKI implementácií. Z tohto dôvodu väčšie organizácie a niektoré štáty zaviedli vlastné profily pre interpretáciu X.509 certifikátov a ich rozšírení, ktoré upresňuje použitie týchto certifikátov. Pre prostredie internetu bol pracovnou skupinou PKIX organizácie IETF štandardizovaný internetový profil X.509 certifikátu [2].



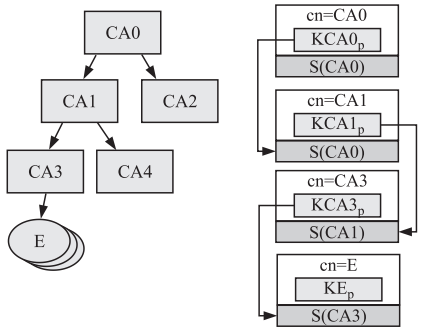
Obr.1 Elektronický podpis



Obr.2 Certifikát verejného kľúča

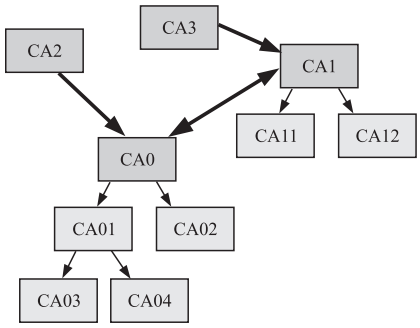
Subjektom certifikácie môže byť aj samotná certifikačná autorita. Podpisujúca CA takto vyjadruje dôveru inej CA, ktorej vydáva certifikát. Týmto spôsobom môže vzniknúť hierarchia certifikačných autorít, pričom koncový používateľ musí explicitne dôverovať len najvyššie postavenej (koreňovej) certifikačnej autorite. Akýkoľvek certifikát vydaný ktoroukoľvek z certifikačných autorít v hierarchii je možné overiť zreťazením koncového certifikátu s certifikátmi všetkých certifikačných autorít v danej vetve hierarchie až po najvyššie postavenú koreňovú CA (obr. 3). Overovanie certifikátu sa potom realizuje po krokoch, vždy po jednej úrovni hierarchie.

Rôznym uplatňovaním vzájomnej certifikácie certifikačných autorít je možné dosiahnuť rôzne druhy štruktúr, nielen stromovú štruktúru hierarchie. V praxi sa práve stromová štruktúra vo svojej čistej forme



Obr.3 Hierarchia PKI

vyskytuje len veľmi zriedka. Ak certifikačná autorita vydá certifikát inej certifikačnej autorite, ktorá nie je jej podriadenou certifikačnou autoritou, ale napríklad tvorí koreň nezávislej hierarchie, takáto akcia sa nazýva krížová certifikácia (cross certification). Krížová certifikácia môže byť jednostranná alebo obojstranná, vždy však vyjadruje vzťah dôvery medzi certifikačnými autoritami. Príklady niektorých štruktúr, ktoré môžu vzniknúť krížovou certifikáciou je znázornený na obr. 4.



Obr.4 Krížová certifikácia

Validácia digitálnych certifikátov

Vydaním certifikátu certifikačná autorita potvrdzuje väzbu medzi verejným kľúčom a identitou certifikovaného subjektu. Súkromný kľúč prislúchajúci k certifikovanému verejnému kľúču však môže byť kompromitovaný alebo identita certifikovaného subjektu sa môže zmeniť. V takom prípade je nutné platnosť vydaného certifikátu zrušiť. Certifikáty vydávané podľa štandardu X.509 obsahujú informácie o dobe platnosti certifikátu a certifikačné autority vydávajú certifikáty vždy len na určité obdobie. Po uplynutí tohto obdobia je nutné certifikát obnoviť. Certifikáty, ktorých platnosť je nutné zrušiť okamžite a ktoré nemôžu zostať platné až do konca svojej pôvodnej doby platnosti, je však potrebné explicitne zneplatniť. Na tento účel certifikačná autorita vydáva zoznamy zneplatnených certifikátov (certificate revolation list, CRL) v ktorých sú uvedené všetky certifikáty, ktorých platnosť bola zrušená pred uplynutím doby platnosti certifikátu. Klient, ktorý si potrebuje overiť platnosť prijatého certifikátu, lokalizuje zoznam zneplatnených certifikátov na príslušnej certifikačnej autorite a vyhľadá overovaný certifikát. Zoznamy zneplatnených certifikátov sú dátové štruktúry taktiež definované v štandarde X.509 a sú chránené podpisom certifikačnej autority, preto ich možno skladovať a prepravovať aj v nedôveryhodnom prostredí. Certifikačná autorita vydáva zoznamy zneplatnených certifikátov v pravidelných intervaloch, ale môže vydať nový zoznam kedykoľvek skôr, napríklad ak je nutné zneplatniť dôležitý certifikát.

Zoznamy zneplatnených certifikátov však majú jednu podstatnú nevýhodu. Ak bol zoznam vydaný mimo pravidelného intervalu, klient sa nemusí dozvedieť, že existuje nový zoznam a môže stále používať v danom čase neaktuálny zoznam zneplatnených certifikátov. Na elimináciu tejto nevýhody PKI vzniklo niekoľko protokolov na okamžitú validáciu certifikátov. Najpoužívanejší z nich je protokol OCSP [3], ktorý umožňuje v reálnom čase získať informáciu o aktuálnom stave daného certifikátu. Ďalšie protokoly pre validáciu certifikátov sú momentálne v procese štandardizácie.

Ďalšie služby PKI

Pre plnohodnotné využitie PKI v praxi je nutné okrem už spomínaných služieb certifikácie verejných kľúčov poskytovať aj ďalšie dodatočné služby. Tieto služby sú spojené najmä so zabezpečením neodmietnuteľnosti (non-repudiation) elektronického podpisu. Pomocou certifikácie verejného kľúča entity sa dá dokázať, že na vytvorenie podpisu bol použitý súkromný kľúč prislúchajúci k certifikovanému verejnému kľúču. Nedá sa však presvedčivo dokázať, či v čase podpisovania dokumentu mal platnosť certifikát, vydaný na tento verejný kľúč. Potencionálny útočník mohol daný kľúč kompromitovať, teda aj napriek umiestneniu certifikátu na zoznam zneplatnených certifikátov má útočník možnosť vytvoriť dokument s dátumom v čase, keď bol ešte certifikát platný, a takto spätne vytvoriť neoprávnene podpísaný dokument. Na druhej strane majiteľ certifikátu môže predstierať kompromitovanie svojho privátneho kľúča a na základe predchádzajúcej úvahy môže spochybniť dôveryhodnosť ním podpísaných dokumentov, a zbaviť sa tak nežiaducich záväzkov.

Na riešenie problémov tohto druhu sa využívajú služby časových pečiatok (time stamping) a certifikácie údajov (data certification). Autorita časových pečiatok (time stamping authority, TSA) je dôveryhodná tretia strana, ktorá potvrdzuje existenciu údajov v časovom momente. Svojím podpisom zaručuje, že v čase podpisu daný dokument existoval. Časovou certifikáciou tak možno predchádzať problémom opísaným v predchádzajúcom odstavci, pretože majiteľ podpisu sa nebude môcť zrieť zodpovednosti za svoj podpis, ak k nemu existuje časová pečiatka, ktorú vydala dôveryhodná TSA. Pomocou techník certifikácie údajov je zase možné dôveryhodne dokázať, že daný certifikát bol v čase jeho použitia skutočne platný, a teda aj podpis vykonaný súkromným kľúčom prislúchajúcim k certifikátu je platný. Táto služba navyše potvrdzuje, že entita overujúca podpis skutočne vykonala všetky kroky potrebné na overenie platnosti certifikátu tak, ako to nariaďujú príslušné predpisy.

Ďalšou nadstavbou PKI je infraštruktúra správy privilégií (privilege management infrastructure, PMI), ktorá umožňuje jednotlivým entitám prideľovať ľubovoľné atribúty pomocou atribútových certifikátov (attribute certificate, AC). Tieto atribúty sa väčšinou spájajú s funkciami a privilégiami entity v systéme, čo umožňuje efektívne realizovať autorizáciu entít aj v často sa meniacich systémoch bez nutnosti zneplatňovať a znovu vydávať certifikáty verejných kľúčov.

Využitie PKI v praxi

Certifikáty verejných kľúčov majú široké uplatnenie v moderných informačných systémoch. Vďaka značnej škálovateľnosti infraštruktúry je možné spravovať veľké množstvá entít bez neprimeraného nárastu zložitosti systému. Výhody PKI využívajú systémy na všetkých architektonických úrovniach informačných systémov.

Na transparentné zabezpečenie sieťovej komunikácie a na vytváranie virtuálnych privátnych sietí v prostredí IP sietí sa dnes vo veľkej miere používa protokol IPsec [4]. Na zabezpečenie výmeny kľúčového materiálu je možné využiť PKI a X.509 certifikáty, čo zaručí jednoduchšiu správu a škálovateľnosť rozsiahlych virtuálnych privátnych sietí.

Zabezpečenie komunikácie na sieťovej úrovni je vhodné väčšinou len na používanie v rámci jednej organizácie. Na globálne služby prístupné pomocou internetu alebo extranetov je vhodnejšie použiť zabezpečenie na vyšších úrovniach. V súčasnosti najpoužívanejším bezpečnostným protokolom na všeobecné použitie je protokol TLS [5] a jeho staršia verzia SSL. Protokol TLS je umiestnený nad transportnou vrstvou protokolovej rodiny a jeho úlohou je poskytovať bezpečnostné služby protokolom vyššej úrovne. Najznámejším použitím protokolu TLS je HTTPS, bezpečná verzia protokolu HTTP. Protokol TLS umožňuje vzájomnú autentifikáciu obidvoch strán spojenia pomocou výmeny X.509 certifikátov a umožňuje zostaviť bezpečný šifrovaný kanál pre ďalšiu komunikáciu. Pomocou TLS sú zabezpečené aj ďalšie bežne používané služby, ako napríklad POP3, IMAP, LDAP, SMTP atď.

Okrem všeobecne použiteľných bezpečnostných protokolov vznikli aj protokoly (a ich rozšírenia) na špecifické použitie. Najznámejším príkladom je protokol na zabezpečenie elektronickej pošty S/MIME [6]. Pomocou S/MIME je možné podpisovať a šifrovať správy elektronickej pošty, pričom na správu kľúčového materiálu sa plne využívajú vlastnosti PKI.

Ďalšie možné využitie PKI je v podnikových systémoch, kde pomocou kombinácie PKI s existujúcou infraštruktúrou možno vytvoriť efektívny základ pre flexibilnú a bezpečnú autentifikačnú a autorizačnú platformu. V tomto smere sa PKI integruje najmä s adresárovými službami založenými na protokole LDAP [7].

Hlavné využitie PKI sa však v budúcnosti predpokladá v oblasti elektronického obchodovania. PKI by mala poskytnúť základ pre spoľahlivé a bezpečné podnikanie v elektronickom priestore, umožniť obchodníkom prevádzkovať bezpečnú obchodnú komunikáciu, uzatváranie právoplatných elektronických zmlúv, jednoduchšiu a rýchlejšiu komunikáciu s orgánmi štátnej správy atď. PKI teda skutočne predstavuje kľúčový prvok na ceste k informačnej spoločnosti.

Literatúra

[1] ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection. The Directory: Authentication Framework, 1997.

[2] HOUSLEY, R., FORD, W., POLK, W., SOLO, D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459, 1999.

[3] MYERS, M., ANKNEY, R., MALPANI, A., GALPERIN, S., ADAMS, C.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. RFC 2560, 1999.

[4] KENT, S., Atkinson, R.: Security Architecture for the Internet Protocol. RFC 2401, 1998.

[5] DIERKS, T., ALLEN, C.: The TLS Protocol Version 1.0. RFC 2246, 1999.

[6] RAMSDELL, B.: S/MIME Version 3 Message Specification. RFC 2633, 1999.

[7] YEONG, Y., HOWES, T., KILLE, S.: Lightweighted Directory Access Protocol. RFC 1777, 1995.

Ing. Radovan Semančík

Business Global Systems, a. s.
Pluhová 2, 832 48 Bratislava 3
e-mail: semancik@bgs.sk