Zákon o elektronickom podpise bol prijatý, jeho úplná aplikácia v praxi je však ešte veľmi vzdialená. Technológie PKI (Public Key Infrastructure) je však možné úspešne využívať aj bez priamej závislosti na prijatom zákone a očakávaných vykonávacích predpisoch. Je zrejmé, že samotná PKI a jej podkladové technológie majú obrovský potenciál, využiteľný aj v prostredí Internetu aj v podnikovom prostredí. Vhodným využitím týchto technológií je možné dosiahnuť značný pokrok v oblasti globálnych informačných systémov.

TECHNOLOGICKÉ POZADIE

Základom PKI je bezpochyby kryptografia, a to hlavne asymetrické kryptografické metódy. Základy tejto technológie boli položené roku 1976 keď W. Diffie a M. Hellman publikovali svoj slávny článok "New Directions in Cryptography" . Za posledných vyše 25 rokov však technológia výrazne pokročila, najmä čo sa týka praktickej použiteľnosti kryptografickým metód. Hlavným prínosom asymetrickej kryptografie je použitie dvoch kľúčov namiesto jedného. Jeden z kľúčov môžem ľubovoľne zverejniť, druhý zostáva tajný. Takáto asymetria sa s výhodou využíva najmä pri rozsiahlych systémoch obsahujúcich tisícky participantov. Aj pri použití asymetrickej kryptografie však zostáva jeden zásadný problém: autenticita kľúča. Ako môže môj obchodný partner na druhej strane sveta s určitosťou vedieť, že verejný kľúč ktorý práve dostal je naozaj môj? Ako môže vedieť, že kľúč pomocou ktorého bol vytvorený podpis na správe je platný?

Na vyriešenie tohto problému bolo navrhnutých niekoľko riešení, časom sa však ukázalo, že infraštruktúra dôveryhodných tretích strán - certifikačných autorít (CA) je asi najvhodnejšia pre požiadavky dnešných distribuovaných informačných systémov. Certifikačná autorita vydáva Certifikáty verejného kľúča (PKC, Public Key Cetificate), ktoré slúžia ako potvrdenie identity osoby, ktorej bol certifikát vydaný. Všeobecne uznávaným štandardom v tejto oblasti je doporučenie ITU-T X.509, ktoré definuje kostru pre budovanie bezpečnostnej infraštruktúry.

DNEŠNÉ VYUŽITIE PKI

Vytvorenie kvalitnej PKI infraštruktúry je pomerne náročná úloha, ktorá využíva nie len technologické zdroje, ale buduje najmä organizačné pravidlá, procesy a štandardy. Infraštruktúra samotná však prinesie len veľmi málo priamych výhod. Oveľa dôležitejšie ako infraštruktúra budú aplikácie a systémy, ktoré budú na nej stavať a využívať jej služby.

Tradičnými "PKI-enabled" aplikáciami sú S/MIME a SSL. Každý z nás sa už určite stretol s podpísanou správou elektronickej pošty alebo s "bezpečným" WWW serverom prístupným pomocou protokolu HTTPS. V oboch týchto prípadoch sa využíva tradičná PKI infraštruktúra vybudovaná v prostredí Internetu, za ktorou sa väčšinou skrývajú mená ako Verisign alebo Thawte. Aj keď takto postavená infraštruktúra dobre slúži svojmu účelu, poskytuje len relatívne nízku úroveň bezpečnosti. Takáto bezpečnosť je v dnešných podmienkach postačujúca pre jednoduchšie aplikácie, v budúcnosti však bude nevyhnutné vybudovať PKI infraštruktúry poskytujúce vyššiu bezpečnostnú úroveň.

Nové aplikácie, ktorých bezpečnosť sa priamo opiera o PKI si však v poslednom čase stále viac nachádzajú cestu do praxe. V moderných aplikáciach už nestačí krátkodobo chrániť prenášané údaje pomocou SSL, už nestačí elektronický podpis na neštrukturovaných správach elektronickej pošty. Moderné aplikácie si vyžadujú dlhodobo bezpečný spôsob práce so štrukturovanými údajmi. Do popredia sa tlačia flexibilné štrukturované formáty údajov založené na XML a pomaly vznikajú štandardy na využitie PKI pre prácu s takto štrukturovanými údajmi.

BUDÚCNOSŤ PKI

Najväčšia hodnota PKI je však v jej budúcom využití. Infraštruktúra globálneho charakteru je ideálna pre široko distribuované moderné aplikácie, ktorých nástup je citeľný už aj dnes. Predpokladá sa, že drvivá väčšina informácii, ktoré sa dnes vymieňajú pomocou nezabezpečených, neštrukturovaných komunikačných kanálov (telefón, fax, e-mail) sa v budúcnosti bude vymieňať pomocou štrukturovaných formátov podobných XML a zabezpečených pomocou služieb PKI infraštruktúry. Informačné systémy podnikov budú priamo spolupracovať vzájomným volaním externých služieb založených na Web Secvices. Ďalšie rozšírenie PKI poskytujú rôzne autentifikačné a single-sign-on služby, služby používateľských profilov, PMI (Privilege Management Infrastructure), atď.

ZÁVER

Služby PKI skutočne predstavujú obrovský prínos pre distribuované informačné systémy. Už dnes je možné efektívne využívať niektoré vlastnosti PKI v podnikovom prostredí ako aj v globálnych podmienkach Internetu. Súčasná využiteľnosť PKI je však len zlomkom budúcej hodnoty takto vybudovanej infraštruktúry. PKI umožní nie len šifrovanie a autentifikáciu údajov, ale aj zjednotenú identitu, globálnu spoluprácu informačných systémov a platformu pre zabezpečenie rozsiahlych distribuovaných systémov. Zostáva len dúfať, že aspoň základná PKI infraštruktúra si nájde dostatočnú podporu a jej plné nasadenie sa čoskoro stane realitou.

Ing. Radovan Semančík
Business Global Systems, a.s., www.bgs.sk
e-mail: semancik@bgs.sk