Technologie PKI a Evropská Unie

Ing. Jaroslav Pinkava, CSc., AEC spol. s r.o.,
Norman Czech Republic

Internet se, jak všichni již víme, stává novou celosvětovou infrastrukturou. V tisku, v dalších mediích se můžeme pravidelně setkávat s různě fomulovanými, většinou vysoce optimistickými pohledy na informační revoluci, před kterou nyní stojíme. A je pravdou, že v době, kdy vlády a průmyslová odvětví se snaží redukovat náklady a rozpočty, přičemž je nezbytné zabezpečit stávající vysokou úroveň poskytovaných služeb, jsou otevřené sitě klíčem k budoucnosti.

Stejně však jako si lidská společnost vybudovala regulační pravidla pro jiná odvětví své činnosti, buduje je nyní i pro tuto stále ještě novou sféru. A jestliže chceme, aby byla splněna veškerá naše očekávání, nejedná se jen o vytváření širokých dálnic, ale i o zákazy vjezdu, semafory, o to jak mají vypadat doklady o převáženém nákladu a další regulátory.

Svěřujeme svá data tomuto novému subjektu a chceme, aby nám sloužil, aby tato data byla nejen správně přenesena správné straně, ale aby během tohoto přenosu byla i patřičným způsobem ošetřena a dokonce chráněna.

Obecně jsou formulovány v tomto směru čtyři následující základní požadavky: **utajení, autentizace, nepopiratelnost, integrita**. Na základě prací dlouhé řady odborníků z oblasti softwaru, kryptografie, norem, legislativy vzniká nový prostředek jehož cílem je naplnění výše uvedených požadavků.

Tento prostředek nese označení **PKI** – Public Key Infrastructure (český pojem infrastruktura veřejných klíčů se zatím tak nevžil).

Cílem PKI – je ustavit a ošetřovat důvěryhodné prostředí v otevřené síti jako je Internet. Prostředky PKI jsou především služby řídící práci s klíči a digitálními certifikáty, tedy jedná se o šifrování dat, o digitální podpisy elektronických zpráv.

Základní nástroje PKI jsou vytvářeny na bázi tzv. asymetrické kryptografie. Tato kryptografi používá dvojici klíčů: veřejný a soukromý. Veřejný klíč slouží obvykle k šifrování dat (a tento VK nemusí být utajován, jak napovídá samotný název) a naopak soukromý klíč slouží k dešifrování (tento soukromý klíč smí znát jen oprávněný příjemec zašifrovaných dat).

Jak je technologie asymetrické kryptografie používána k vytváření digitálních podpisů? Nejdříve z datové zprávy vytvoříme její jedinečný otisk (pomocí hashovací funkce) a nyní postupujem obráceně (oproti předešlému popisu). Tento otisk zašifrujeme s pomocí svého soukromého (utajovaného) klíče a přidáme ke zprávě (je to její digitální podpis). Kdokoliv, kdo má možnost získat můj veřejný klíč, může si nyní s jeho pomocí ověřit tento podpis. Aby toto vše fungovalo musí být ještě zabezpečena důvěryhodná distribuce veřejných klíčů spolu s důvěryhodným přiřazením těchto klíčů příslušným osobám (majitelům odpovídajících soukromých klíčů). To je v praxi prováděno pomocí tzv. **digitálních certifikátů**. Digitální

certifikát je tedy vlastně prostředek, jehož cílem je dát možnost ověřit propojení totožnosti stran s jejich veřejnými klíči. Fakticky to je zpráva obsahující totožnost uživatele a jeho veřejný klíč, a prostředky, které umožňují ověřit, že certifikátu lze důvěřovat (zpráva je digitálně podepsána důvěryhodnou třetí stranou).

Platnost digitálních certifikátů je omezena v čase a existuje přitom možnost odvolání (revokace) DC v důsledku: kompromitace soukromého klíče, změna dat (např. adresy), chyba v obsahu, změna zaměstnavatele atd. Digitální certifikáty vydává specializovaný subjekt, kterému se říká **certifikační autorita** (CA). CA zodpovídá za spolehlivost práce s digitálními certifikáty: Jednotliví uživatelé PKI musí být zde registrovani z hlediska své totožnosti, aby ostatní mohli této totožnosti důvěřovat. CA pracuje v PKI vlastně jako důvěryhodný agent –je třeba, abychom důvěřovali podpisu CA na DC. Kromě CA existují další komponenty PKI: registrační autorita, autorita časových značek, seznamy (databáze) certifikátů, seznamy odvolaných certifikátů, autority vydávyjící tzv. atributové certifikáty atd. Práce CA se řídí dvěma zásadními dokumenty: certifikační politika a certifikační prováděcí směrnice (CPS).

Tolik jen k nastínění základních technologických východisek PKI. Je toho ještě opravdu hodně, o čem by bylo možno hovořit, ať jsou to technické detaily ohledně použitých algoritmů asymetrické kryptografie (RSA, DSA, ECDSA), varianty podpisových schémat, potřebné vlastnosti použitých generátorů náhodných znaků, navazující metody symetrické kryptografie – tj. hlubší rozbor tchnických aspektů.

Fakt, že PKI jako prostředek je určen pro takovou otevřenou síť jako je Internet se všemi důsledky na nezbytnost jeho fungování v rámci styku mezi jednotlivými státy klade jeden další důležitý požadavek. Tím je interoperabilita používaných konkrétních PKI řešení. A to vše souvisí s vytvářením a využíváním **mezinárodních norem** v dané oblasti.

V současné době existuje v této sféře již dlouhá řada využívaných norem a to velice různorodého charakteru, které popisují různé výše zmíněné stránky vytváření digitálních podpisů. Další normy jsou připravovány – např. v návaznosti na legislativní řešení v rámci Evropské Unie.

Pokrýt jednotně pouze oblast norem se však ukázalo jako nepostačující. Je třeba, aby jednotící prvky zasáhli i legislativní sféru. Např. je třeba, aby podpis vytvořený v jedné zemi, mohl být právně uznán v jiné zemi, aby totéž platilo o digitálních certifikátech a konec konců i o vlastních certifikačních autoritách.

V současné době takovou technologicky nejvyspělejší a nejucelenější platformou je Směrnice Evropské Unie o elektronickém podpisu, která byla schválena Evropskou komisí v prosinci 1999 – tj. právě před rokem.

Tato Směrnice si položila za cíl splnit následující tři základní principy:

I. Technologická neutralita

II. Vydávání oprávnění pro poskytovatele certtifikačních služeb nebude direktivně omezeno žádným schématem

III. Nezbytnost rozpoznání zákonné platnosti elektronických podpisů.

Směrnice EU definuje poměrně exaktně takové základní pojmy, jako jsou el. podpis, zaručený el. podpis, digitální certifikát, kvalifikovaný digitální certifikát, poskytovatel certifikačních služeb, národní akreditační schéma, podpisový prostředek, atd. Následně rozebírá jejich základní a hlubší vlastnosti, stanoví právní účinky těchto pojmů.
Dle závazného doporučení mají členské země EU uvést svoji legislativu do souladu s touto Směrnicí do konce června roku 2001.

Směrnice se zabývá elektronickými podpisy používanými pro autentizační účely jak z hlediska obecného přístupu, tak i z hlediska speciálního typu tzv. zaručených elektronických podpisů (kvalifikovaný podpis), které mají být právně ekvivalentní klasickým ručně psaným podpisům. Zaměřuje se tedy na právní platnost elektronického podpisu, který je připojen

k elektronickému dokumentu. Direktiva rovněž stanoví požadavky, které mají být splněny poskytovateli služeb, kteří podporují elektronické podpisy a další požadavky vztahující se k podepisující a ověřující straně. Tyto požadavky nutně vyžadují podporu v detailních normách a veřejných specifikacích, které rovněž splní požadavky evropských obchodních organizací.

Přes některé dílčí nedostatky ve formulacích již vychází český zákon (227/2000 Sb.) o elektronickém podpisu z této Směrnice a lze ho považovat za jeden z progresivních českých zákonů posledního období. Přesto není vůbec od věci konstatování, že vydání zákona neznamená automaticky vyřešení celkového stavu problematiky.

Potřebné jsou návazné vyhlášky, které připravuje Úřad na ochranu osobních údajů. Není to věc jednoduchá a nejde zde jen o zpracování jakýchsi dokumentů. Složitou (a novou z českého hlediska) je zde zejména problematika evaluace (vyhodnocení shody) podpisových prostředků (bezpečných nástrojů dle formulace zákona – paragraf 6.1.j). Je třeba zajistit praktické fungování institucí provádějících evaluaci podpisových prostředků dle mezinárodně uznávaných norem. Tyto instituce musejí být pro svou činnost akreditovány postupem adekvátním postupům běžným v Evropské Unie. Zde napomůže již existující Český akreditační institut. Pokud by totiž tyto instituce tímto procesem akreditace neprošly, nebudou jejich výsledky mezinárodně uznávány.

Nové technologie a PKI mezi ně nesporně patří nám nemohou sloužit pokud s nimi nebudeme patičným způsobem seznámeni. Jednou skutečností je získání potřebných informací a jiným faktem je aktivní ovládání těchto poznatků. Teprve potom se dá hovořit o osvojení dané technologie. Jestliže budu hovořit za celkový stav problematiky v tomto státě, pak je třeba říci, že zatímco někde se již můžeme setkat se skutečnými odborníky, aktivně se podílejícími na rozvoji dané oblasti, celková situace není zdaleka tak růžová. Problematika elektronického podpisu, jestliže má doznat skutečného praktického využívání má před sebou ještě celou řadu met.

Některé se týkají potřebného materiálního a softwarového vybavení (elektronické podatelny, podpisové prostředky,...) a řada z nich se týká znalostí lidského činitele. I taková zdánlivě jednoduchá problematika jako je ochrana svého podpisového soukromého klíče se totiž může ukázat netriviální záležitostí. Např. tolik oblíbené internetové kiosky – šly by jste tam podepsat něco téměř nezáludného jako je daňové přiznání? Myslíte, že obsluha počítače v kiosku se k Vašemu soukromému klíči nedostane a nepoužije ho k něčemu zdaleka ne tak už nezáludnému? Dobrá, Vy už to víte a vyvarujete se toho, ale co ty tisíce dalších?

Nevadí Vám, že soukromým klíčem podepisujete v kanceláři příkazy v hodnotách desetitisíců korun? Po odchodu z práce počítač řádně vypínáte. No, ale zapomněl jste, že máte šikovnou sekretářku a ta zrovna potřebuje nějakou almužnu na dovolenou. Tak dobrá, pořídíte si vyjímatelný harddisk a uschováte ho při odchodu do trezoru. Ale zapomněl jste na podnikovou síť a že jste tam nedávno najal skutečně fachmana, ten se v sítích vyzná. O tom, že Vám poslal trojského koně se možná dovíte až ze soudní síně, když z Vás budou vymáhat ztracené miliony.

Tj. bezpečnost Vašeho soukromého klíče není vůbec věc zanedbatelná a je třeba ji věnovat náležitou pozornost. Ještě v podstatnější míře to platí pro podpisové klíče takových institucí jako jsou certifikační autority, banky, atd.

Ještě jen malou poznámku bych dodal na závěr. Problematika PKI tak, jak ji koncipuje dnešní teorie a jak je uváděna do praxe, není zdaleka uzavřenou záležitostí. A více nových cest praxe ještě nepochybně ukáže – např. v návaznosti na oblast elektronického obchodu. Tyto technologie nebudou po odborné stránce jednoduchou záležitostí. Úlohou lidí, kteří tyto technologie připravují pro praktické použití (ať již z hlediska technologického, kryptologikého, normativního či legislativního), je (mimo jiné) zajistit jejich bezpečné používání běžným uživatelem.

Literatura:
[1] Carl Ellison and Bruce Schneier: Ten Risks of PKI, http://www.counterpane.com
[2] Jaroslav Pinkava: Elektronické podpisy a Evropská Unie, DSM 2/2000