Stručný obsah

Obsah

Kapitola 3

Kapitola 4

Kapitola 8

Kapitola 9

Kapitola 10

Kapitola 11

Kapitola 12

Kapitola 13

Kapitola 14

Kapitola 18

Kapitola 19

Kapitola 23

Kapitola 24

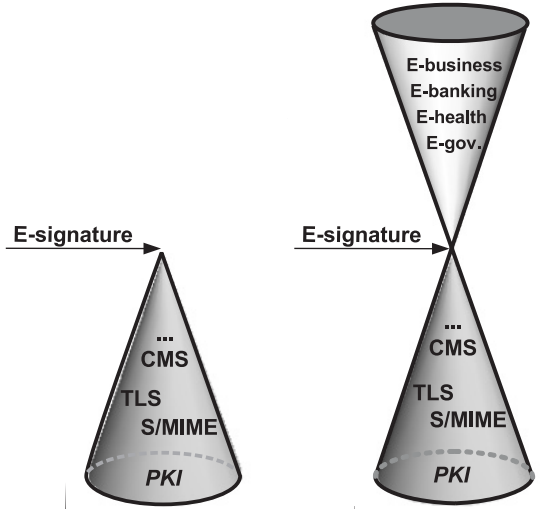
Kapitola 25

Kapitola 27

Úvod

Je to již několik let, kdy jsme byli naposledy v Paříži. I tenkrát jsme si vzpomněli na Petera Sylvestera. A hned nás napadlo, že se u něj opět zastavíme. P. Sylvester je spoluautor legendárního standardu-nestandardu RFC-3029 *„Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols*“, který už tehdy mnozí kritizovali, ale přitom nikdo nedokázal vymyslet nic lepšího. Což bohužel víceméně platí dodnes.

I přes stávku pařížských dopraváků jsme dorazili včas a začali naši diskusi. Uprostřed diskuse Peter namaloval kužel (obr. ú.1 vlevo), který komentoval slovy, že PKI si můžeme představit jako podstavu kužele, nad níž je vybudována řada protokolů (S/MIME, TLS, CMS, IPsec, EAP-TLS…). Na vrcholu kužele je pak elektronický podpis.



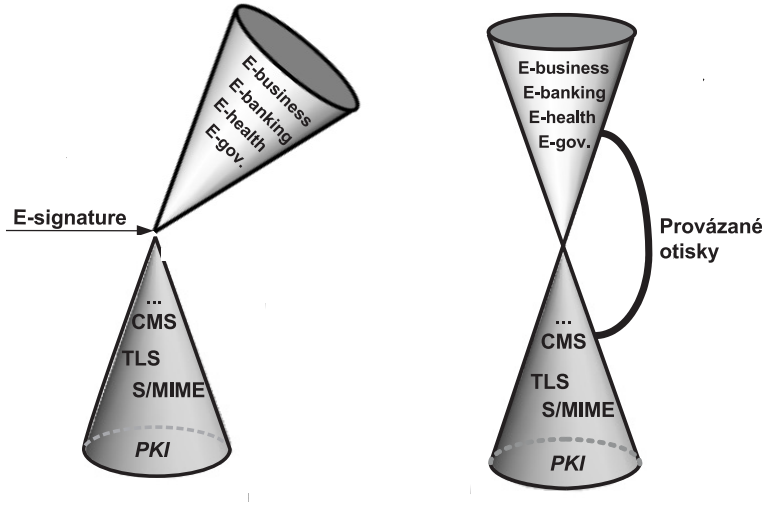
Obrázek ú.1: Sylvesterovy kužely

Vedle namaloval týž kužel, ale na jeho vrchol přidal ještě další kužel otočený vrcholem dolů (obr. ú.1 vpravo). A pokračoval tvrzením, že na tom jediném elektronickém podpisu stojí všechny nejrůznější aplikace jako E-government, E-health, E-banking, E-business, E-procurement a kdoví jaké další „E-“.

„No a nyní si stačí představit“, zaníceně pokračoval, „že někdo jen zpochybní ten elektronický podpis.“ A už maloval další kužely (obr. ú.2). Hned bylo vidět, jak se celý ten humbuk „E-“ kácí jako krabička sirek. Zdůrazňoval, že je třeba hledat i jiné algoritmy a postupy, které ty užitečné aplikace podepřou, a jako rozumný mu připadal systém provázaných otisků (viz kapitola 20).

Nás tyto Sylvesterovy kužely přímo nadchly. Avšak u mnohých kolegů jsme s nimi nepochodili. Připadalo jim to totiž nadnesené.

Cílem této publikace je začít zkoumat Sylvesterovy kužely od spodní podstavy, kterou je PKI. Dále si objasníme zejména protokoly popsané ve spodním kuželu a elektronický podpis. Pochopitelně že kužely rovněž pořádně zatřepeme, když si položíme otázku o platnosti elektronického podpisu po vypršení platnosti certifikátu určeného k ověření tohoto podpisu. A nebojte se, i na provázané otisky dojde.



Obrázek ú.2: Provázané otisky možná pomohou udržet Sylvesterovy kužely ve správné poloze nad sebou

Jak tuto knihu číst

Kniha je určena jak pro začátečníky v oblasti PKI, tak i pro odborníky, kteří se potřebují dozvědět řadu detailů. Aby začátečníci nebyli zahlceni, je prvních deset kapitol napsáno populární formou tak, aby byly dobře srozumitelné i pro ně. Těchto prvních 10 kapitol objasňuje princip certifikátu veřejného klíče a jeho životní cyklus.

Kapitoly 11, „Má první certifikační autorita", a 12, „Wireshark", jsou určeny šťouralům, kteří si chtějí pohrát s jednoduchou certifikační autoritou a připravit se na pitvání nejenom certifikátu po jednotlivých bitech.

Přelomovou kapitolou je kapitola 13, „ASN.1, BER, DER,UTF-8 a Base64", zabývající se jazykem ASN.1 sloužícím k definování jednotlivých datových struktur. Dále se zabývá kódováním BER a DER těchto struktur pro počítačovou komunikaci. Pokud se laskavý čtenář seznámí s jazykem ASN.1 a kódováním BER a DER (tj. s obsahem této kapitoly), pak bez jakýchkoliv problémů může rozebírat dále popisované datové struktury po jednotlivých bitech. Stane se tak pokročilým čtenářem této publikace.

Kapitoly 14, „Žádost o vydání certifikátu pod lupou", 15, „Certifikát pod lupou", 16, „Žádost a odvolání certifikátu pod lupou", a 17, „CMP a CMC", jsou určeny pro pokročilé čtenáře. Mají obdobný obsah jako kapitoly 1–10, ale zaměřují se na detailní popis jednotlivých datových struktur.

Zbývající část publikace pak obsahuje tematicky zaměřené kapitoly (Atributové certifikáty, Časová razítka, Bezpečný web, Bezpečná pošta, Dlouhodobý digitální podpis a Dlouhodobá archivace). Tyto kapitoly jsou určeny jak začátečníkům, tak i pokročilým čtenářům. Začátečníci jen přeskočí popisy jednotlivých datových struktur.

Kapitola 27, „Budujeme PKI, TSA a důvěryhodné archivy", je pak závěrem celé publikace.

Poděkování

Chtěli bychom poděkovat všem, kteří nám zapůjčili nejrůznější zařízení, abychom mohli připravit jednotlivé příklady. Dále bychom chtěli poděkovat Luďku Raškovi za podnětnou odbornou korekturu a Michalu Hojsíkovi, který rukopis pozorně přečetl a opravil mnohé chyby.