**Digitálny certifikát a certifikačná autorita**

Samotné šifrovanie z predchádzajúcej kapitoly síce ochráni komunikáciu pred odpočúvaním, ale bez overenia autentickosti verejných kľúčov sa komunikujúce strany môžu stať obeťou tzv. útoku **Man in the middle** (z angličtiny *človek uprostred*). Podstatou tohto útoku je snaha útočníka odpočúvať komunikáciu tak, že sa stane jej aktívnym prostredníkom. Pri počiatočnej vzájomnej výmene verejných kľúčov získa verejné kľúče účastníkov odpočúvanej komunikácie a podsunie im namiesto nich svoj verejný kľúč:



Následnú šifrovanú komunikáciu preposiela cez seba ako sprostredkovateľ, pričom pôvodnú správu dokáže nielen prečítať, ale môže túto správu aj pozmeniť:



Predstavme si napríklad, že Alica má v elektronickej forme vyplnené daňové priznanie. Chcela by ho podpísať, a tak potvrdiť údaje v ňom uvedené. Ako to spraví? Tak, že zoberie dotyčný súbor a odšifruje ho pomocou svojho súkromného kľúča. Výsledkom tejto operácie je reťazec predstavujúci jej podpis. Ten Alica pripojí k samotnému dokumentu. Keď chce Karol overiť pravosť tohto podpisu, môže zobrať Alicin verejný kľúč, pomocou neho zašifrovať jej podpis a overiť, že sa výsledok rovná pôvodnému dokumentu.

Prečo to celé funguje? Pretože Karol vie, že Alica je jediná, kto vie pomocou jej kľúča aj dešifrovať – a teda dotyčný podpis musela vyrobiť ona, nik iný na to nemá dostatok informácií.

Ak by Alica teraz chcela takto podpísané daňové priznanie z pohodlia svojho domova podať, nefungovalo by to. Chýba totiž jeden dôležitý článok: prepojenie medzi verejným kľúčom (súborom získateľným kdesi na internete) a Alicou ako fyzickou osobou. Štát nemá prečo len tak uveriť, že Alicin verejný kľúč je zrovnal tento a nie jeden zo sta iných.

Aj na toto sa však myslelo. U nás na Slovensku túto problematiku rieši Zákon 215/2002 Z.z. o elektronickom podpise. Tento definuje tzv. **zaručený elektronický podpis**, ktorý má, zjednodušene povedané, rovnakú právnu váhu ako fyzický podpis na klasickom dokumente. Ako vieme takýto podpis vyrobiť? Chýbajúci medzičlánok – záruku korešpondencie medzi verejným kľúčom a fyzickou osobou – zabezpečujú inštitúcie nazývané **akreditované certifikačné autority**. Celý proces si môžeme jednoducho popísať nasledovne:

Alica zoberie svoj občiansky preukaz a navštívi niektorú akreditovanú certifikačnú autoritu (CA).( V zmysle zákona kvalifikovaný certifikát, ktorý je potrebný pre zaručený elektronický podpis, môže vydať iba certifikačná autorita akreditovaná NBÚ (Národný bezpečnostný úrad). Aktuálny zoznam akreditovaných certifikačných autorít pre zaručený elektronický podpis nájdeme na stránkach NBÚ (www.nbusr.sk).)

* Pracovník CA si overí jej totožnosť a následne jej vygeneruje súkromný a verejný kľúč.
* Ku kľúču jej navyše vydá certifikát, teda potvrdenie, že ide naozaj o Alicin kľúč. (Tento certifikát je vlastne elektronický dokument obsahujúci potrebné údaje a podpísaný kľúčom dotyčnej certifikačnej autority.)
* Od tejto chvíle vie Alica vyrábať zaručených elektronických podpisov, koľko len chce. Ku podpísanému dokumentu následne priloží aj certifikát, ktorý príjemcovi umožní overiť totožnosť odosielateľa.

Elektronický podpis funguje nasledujúcim spôsobom: z obsahu dokumentu sa vytvorí tzv. odtlačok (hash) – krátky (typicky niekoľko stoviek bitov) výťah vytvorený pomocou špecializovaných algoritmov (hašovacie funkcie) a takto získaný odtlačok sa následne zašifruje súkromným kľúčom autora. Zašifrovaný odtlačok predstavuje elektronický podpis, ktorý sa k podpisovanému dokumentu priloží. Pri overovaní podpisu sa z dokumentu opäť vytvorí rovnakým algoritmom nový odtlačok a z priloženého elektronického podpisu sa pomocou verejného kľúča autora dešifruje pôvodný odtlačok dokumentu. Novozískaný odtlačok sa porovná s dešifrovaným odtlačkom, a ak sú identické, tak sa

týmto zaručila integrita podpísaného dokumentu. Úspešným dešifrovaním elektronického podpisu konkrétnym verejným kľúčom je jednoznačne určený autor podpisu.



Je dôležité, aby súkromný kľúč ostal vždy súkromným, teda utajeným. V prípade straty alebo odcudzenia súkromného kľúča je dôležité okamžite zrušiť certifikát k príslušnému verejnému kľúču (predčasne ukončiť jeho platnosť). Certifikát na požiadanie vydáva, obnovuje a taktiež zneplatňuje certifikačná autorita. Vydaný certifikát k verejnému kľúču má definovanú dobu platnosti, zvyčajne jeden rok.

**Praktické aplikácie kryptografie**

Máloktorý používateľ počítača si uvedomuje, že keď si prezeráte webstránky, skoro všetky údaje posielané medzi vaším počítačom a servermi sa prenášajú (pomocou protokolu HTTP) v nešifrovanej podobe. Hocikto teda môže túto komunikáciu odpočúvať. Sú však situácie, kedy toto nechceme: napríklad také čítanie súkromnej elektronickej pošty, alebo platenie pomocou kreditnej karty. Na tieto účely bol vymyslený protokol HTTPS („S“ ako „secure“, presnejšie ide o kombináciu protokolov HTTP a SSL/TLS). Pri tomto protokole komunikácia prebieha v zašifrovanej podobe. Dôveryhodné webstránky, ako napríklad internet banking vašej banky, vás pri návšteve zväčša automaticky presmerujú na HTTPS verziu prihlasovacej stránky. To, že na stránku pristupujete prostredníctvom šifrovanej komunikácie, spoznáte ľahko priamo v prehliadači. V prvom rade podľa protokolu uvedeného v URL adrese stránky: tá nebude začínať znakmi „http://“, ale znakmi „https://“. Väčšina prehliadačov tiež zobrazí ikonku zámku, ak je obsah prenášaný šifrovane.

Samotné zabezpečenie komunikácie však ešte nestačí – ako vieme, že tá webstránka skutočne patrí našej banke, a nie nejakému zlodejovi? Tu, podobne ako pri zaručených elektronických podpisoch, musia prísť k slovu certifikáty. Niekto dostatočne dôveryhodný (certifikačná autorita) vydal banke certifikát potvrdzujúci jej totožnosť. A práve týmto certifikátom sa webserver banky potom preukáže vášmu prehliadaču. Prehliadač si overí, že certifikát banky je podpísaný certifikačnou autoritou, ktorej dôveruje, a výsledkom je to, čo vidíme na obrázku označené číslom 2: v adrese sa objaví farebne zvýraznená informácia o tom, že bol úspešne overený certifikát stránky, a tiež to, kto je jeho vlastníkom. Ak teda všetko prebehlo ako sme očakávali, môžeme pokojne zadať naše prihlasovacie údaje – máme dostatočnú dôveru, že ich skutočne posielame našej banke.



Ak overenie certifikátu neprebehlo úspešne, prehliadač vás presmeruje na stránku podobnú tej na obrázku. Ak sa vám toto zrazu stane pri prihlasovaní sa na stránku, ktorá „dovtedy fungovala“, je veľmi pravdepodobné, že ste práve obeťou nejakého útoku. V takomto prípade rozhodne nič neodsúhlasujte a nikam nepíšte svoje heslo. Pokúste sa pripojiť ešte raz, ideálne tak, že priamo zadáte adresu do prehliadača. V prípade neúspechu kontaktujte správcu stránky (teda napríklad svoju banku). Niekedy sa môže stať, že takéto varovanie uvidíte aj na legitímnej stránke. Uznávanou certifikačnou autoritou podpísané certifikáty sú totiž drahé, a tak webstránky prevádzkované neziskovými inštitúciami často takéto certifikáty nemajú.

Aby fungovalo HTTPs spojenie na ne, vygenerujú si teda certifikát samy. To však vedie k varovaniu ukázanému na obrázku: prehliadač nás upozorňuje, že síce mu stránka ukázala certifikát, ale nepodarilo sa mu overiť jeho pravosť. Ak pristupujete na takúto webstránku, skontrolujte si, či jej certifikát obsahuje správne údaje.

