



Elektronický podpis

Lukáš Jakubík



Motivačně

Celá osobní komunikace, nyní přenesena do světa Internetu, stojí na důvěryhodnosti v email

- **Věříte tomu, co vám přijde emailem?!**



Vytvořit email s podvrženou identitou (*fake email*) není tak těžká věc – freeSMTP serverů je dost

- **Věříte tomu, co čtete, že mohl napsat váš známý?!**



Dostat se k heslu (*keylogging*) nebo využít slabou chvíli (*social engineering*) majitele účtu jde snadno

- Používejte elektronický podpis!

... sken podpisu není to, oč tu kráčí



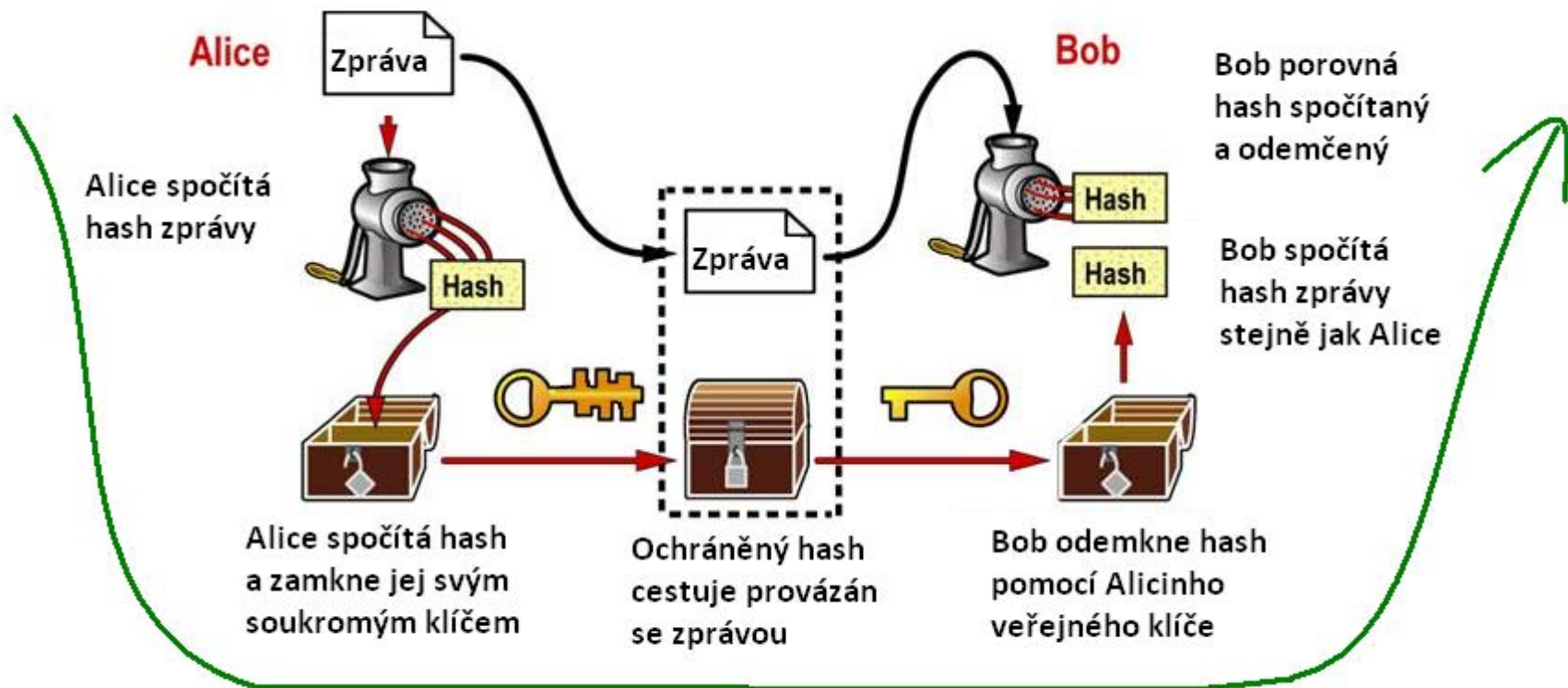
Principy z kryptografie

- Potřebujeme data chránit
důvěrně (šifrovat, utajovat)
důvěryhodně (podepisovat, razítkovat)
- Běžně známe symetrické metody (společný klíč) které jsou však nepoužitelné při větším počtu lidí
- Využívají se spíš **asymetrické metody** (klíčový pár veřejného a soukromého klíče), protože veřejný můžeme zveřejnit a rozšiřovat i neznámým lidem

klíč/činnost	šifrování	podepisování
veřejný	kdokoliv zašifruje	kdokoliv ověří
soukromý	jen my odšifrujeme	jen my podepíšeme

Digitální podpis

- Je mechanismus zajišťující **nepopiratelnost dat** (důkaz pravosti zprávy), že ji napsala právě Alice
- **Hash** je otisk dat, chrání **integritu** (důkaz, že se nic nezměnilo), že nikdo nepřidal, nezměnil nic v zprávě



Elektronický podpis

- Je digitální podpis s integritou, který má navíc i vlastnost **autenticity** (je jednoznačně jasné komu patří, kdo podepsal)
- Je kodifikován ve směrnici EU 1999/93/ES v místním zákonu č. 227/2000 Sb. o elektronickém
- Jako **kvalifikovaný elektronický podpis** již plně nahrazuje rukou psaný podpis v rámci zemí EU
- Souvisí s certifikátem, který musí být vydán akreditovanou kvalifikovanou certifikační autoritou



Certifikát a certifikační autorita

- Certifikát je důvěryhodný dokument potvrzující nějakou skutečnost (občanský průkaz s fotografií)
- Elektronický certifikát je jistý datový soubor, který se používá na **důvěryhodné provázání identity a veřejného klíče** (certifikát s emailem a klíčem)
- Certifikát vydává certifikační autorita, která ověřila data v něm a stvrzuje je tím, že certifikát podepíše
- Bohužel, každý si může udělat vlastní certifikát i celou certifikační autoritu
... jen málo jich je skutečně důvěryhodných

Certifikační autorita Comodo

- Komerční bezpečnostní společnost s celým spektrem produktů a služeb
- Jedna z posledních světových autorit, které vydávají **emailové certifikáty pro běžné použití zdarma**
- Standardně předinstalovaná a důvěryhodná ve **většině emailových klientů**



Certifikační autorita PostSignum

- jedna z **kvalifikovaných certifikačních autorit**
- vlastněná Českou poštou, akreditovaná MV
- vydává kvalifikované certifikáty již od září 2005
- dostupná **na poště**, kde je i CzechPOINT
- přiděluje i identifikátor sociálního zabezpečení
- probojovala se na seznam kořenových certifikátů Microsoftu, tedy jí vydané certifikáty by měli být **taky rozeznány jako důvěryhodné**

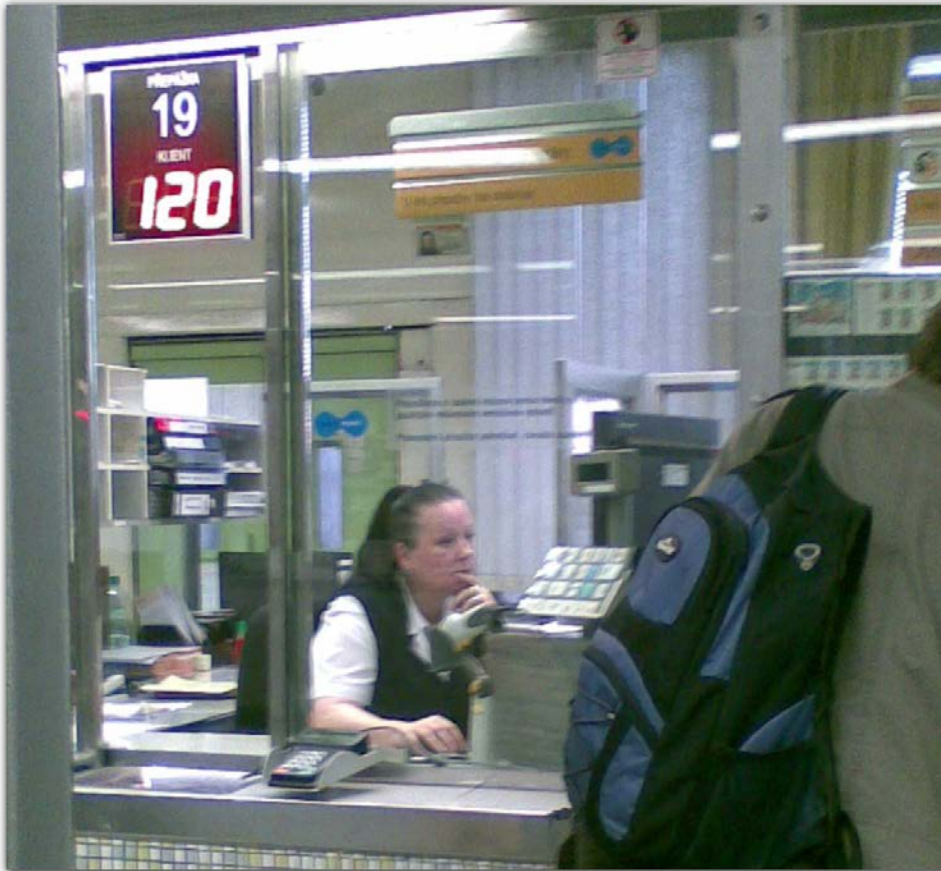


Certifikační autorita po vás chce

- doma vygenerovaný veřejný klíč – na USB nebo zaslaný
 - elektronickou žádost podepsanou soukromým klíčem
 - 2 doklady totožnosti
 - kopu papírů (2 smlouvy, 2 formuláře, 2 povolení...)
 - 400 Kč
-
- *8 fyzických podpisů*
jeden elektronický



Certifikační autorita je



- Dostupná
 - ale plexisklem chráněná
- Vytížená
 - ale v pořadí dosažitelná
- Ochotná
 - ale předpisově striktní
- Milá a znalá!
 - nato jak je placená

Praxe

- na elektronické podepisování emailů je potřebný emailový klient s podporou S/MIME ~ Thunderbird
- musíme si vytvořit soukromý a veřejný klíč
- požádat certifikační autoritu o vydání certifikátu, kde bude naše emailová adresa a náš veřejný klíč
- certifikát (záloha.p12) **nikdy nikomu nesvěříme**, jen svému emailovému klientu, který chráníme heslem
- posíláme, přijímáme a ověřujeme podpisy zvesela

Děkuji za vaši účast a pozornost

Použité zdroje

DOSTÁLEK, L. – VOHNOUTOVÁ, M. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Brno: Computer Press, 2009. 534 str. ISBN 978-80-251-2619-6

NEVOSÁD, L. *Jak jsem si pořídil elektronický podpis České pošty* [online]. Lupa.cz, 19. 9. 2005. [cit. 2015-02-15]. Dostupné z: <http://www.lupa.cz/clanky/jak-jsem-si-poridil-elektronicky-podpis-ceske-posty/>

Digital signature [online]. Hill associates, revize 24 August 2009. [cit. 2015-02-15]. Dostupné z http://wiki.hill.com/wiki/index.php?title=Digital_signature&oldid=10140