Využití elektronického podpisu v praxi VŠ

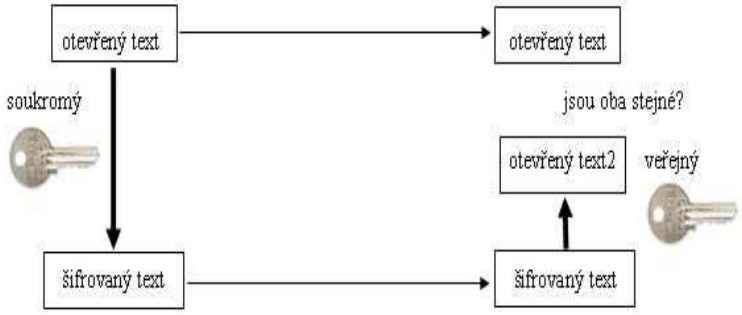
Milan Hála – SVŠES, s. r. o.

Zprávy přenášené komunikačními prostředky, především Internetem, mohou být relativně snadno zneužity (odposlechnuty, modifikovány). Proti odposlechu ochrání zpráby šifrování. Představte si ale situaci, kdy tajnou zprávu zašifrujete odešlete. Útočník zprávu zachytí, smaže a nahradí jinou. A adresát nemusí záměnu zjistit. Šifrování zprávu ochrání před přečtením, vůbec nechrání například před změnou atd. K těmto účelům slouží elektronický (digitální) podpis [2].

Připomeňme si princip elektronického podpisu. Základní požadavky na něj jsou dva:

- zajistit integritu (zpráva nemůže být nepozorovaně změněna)
- zajistit neodmítnutelnost (autor nemůže popřít svůj podpis)

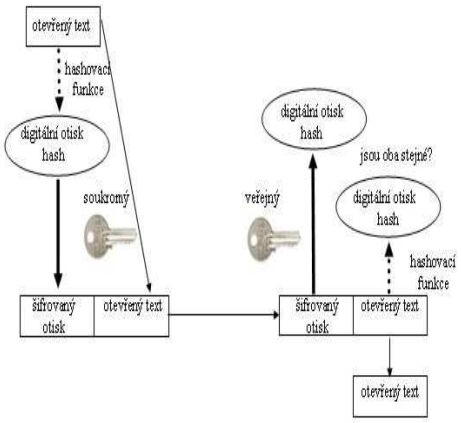
Tyto dva základní požadavky lze zajistit využitím asymetrické kryptografie - odesílatel zprávu zašifruje svým soukromým klíčem a obě zprávy (otevřený text i šifrovaný) odešle adresátovi. Ten dešifruje šifrovaný text veřejným klíčem odesílatele a výsledek (na obrázku označený otevřený text2) porovná s otevřeným textem, který obdržel. Budou-li oba texty stejné ví, že



1. text nebyl po cestě změněn
2. text byl podepsán vlastníkem klíče, jehož veřejnou část sám má

Nevýhodou popsaného způsobu je zbytečná velikost odesílané zásilky (zprávu vlastně posíláme dvakrát) a také to, že zároveň odesíláme otevřený text i text zašifrovaný, což by případnému útočníkovi mohlo usnadnit zjištění klíče. Navíc by šifrování (dešifrování) dlouhé zprávy mohlo trvat příliš dlouho.

Proto se při elektronickém podepisování využívá skutečnosti, že existují tzv. jednosměrné funkce (umožňují snadno vypočítat hodnotu ze zadaných vstupů, ale prakticky není možné z výsledné hodnoty určit vstupní). Vstupem této jednosměrné funkce je otevřený text, výstupem digitální otisk (mnohem kratší než vstupní otevřený text – např. jen 160 bitů).



Je ale velmi malá pravděpodobnost, že by dvě zprávy měly stejný otisk (počet všech možných otisků je 2^{160}). Digitálnímu otisk označujeme jako hash, funkci hashovací.

1. odesílatel nejprve vytvoří pomocí hashovací funkce digitální otisk otevřeného textu
2. digitální otisk (hash) zašifruje svým soukromým klíčem
3. připojí šifrovaný otisk k otevřenému textu a odešle adresátovi

4. adresát vytvoří pomocí stejné hashovací funkce jako odesílatel digitální otisk
5. adresát dešifruje pomocí veřejného klíče odesílatele zašifrovaný otisk
6. adresát porovná oba digitální otisky

Použití veřejných a soukromých klíčů pro podepisování zpráv skutečně funguje. Pokud program, ověřující platnost podpisu zprávy sdělí, že je vše v pořádku, stále není vyhráno - ani teď nelze říci, že je vše v pořádku. Ve skutečnosti víme jen následující:

- zprávu v době přenosu nikdo nezměnil
- k šifrování byl použit váš veřejný klíč
- klíč použitý k podpisu odpovídá známému veřejnému klíči

Bohužel není zaručeno, že zpráva je podepsána konkrétní osobou. A jediné, co to může dokázat je, že veřejný klíč byl od této osoby získán osobně. Veřejný klíč získaný na Internetu žádnou zárukou není.

Informaci, že klíč patří konkrétní osobě –dá certifikát, který vystaví třetí osoba (ani odesílatel, ani příjemce) – certifikační autorita. Je to podobné situaci, kdy matrika ověří podpis dokumentu.

Certifikační autorita musí být důvěryhodná. Důvěryhodnost může získat dohodou obou stran (odesílatel, příjemce) nebo „státním souhlasem“ – tedy oprávněním, které po splnění podmínek daných zákonem certifikační autorita získá od kompetentního státního orgánu. CA pak musí zaručit, že jí ověřené (certifikované) klíče skutečně patří osobě, která je používá. Musí zveřejnit svůj veřejný klíč (např. na Internetu), aby si mohl jí vydaný certifikát kdokoliv ověřit. Svůj soukromý klíč musí chránit snad lépe než oko v hlavě – prozrazení soukromého klíče CA by pravděpodobně vedlo k její likvidaci.

Tatáž autorita také musí evidovat jí vydané certifikáty ale musí také evidovat certifikáty neplatné. Vždyť i certifikát může být zneužit, ztracen či ukraden. A protože doba jeho platnosti ještě nevypršela, musí být všem řečeno, že certifikát již neplatí. Proto certifikační autority zveřejňují tzv. CRL (Certificate Revocation List – seznam neplatných certifikátů). A v něm uvede všechny zneužitelné certifikáty.

Typy certifikátů

Protože nic není jednoduché, existují různé typy certifikátů – a to hned čtyři označované **class 1** až **class 4**.

Class 1: certifikační autorita ověří pouze skutečnost, zda již neexistuje klíč pro stejné jméno, takže si kdokoliv může certifikovat klíč na libovolné „volné“ jméno.

Class 2: identitu osoby musí ověřit třetí strana, třeba formou notářského zápisu

Class 3: žadatel musí osobně navštívit certifikační autoritu, která ověří jeho identitu. Způsob tohoto ověření je věcí certifikační autority.

Class 4: i zde se musí osoba dostavit k certifikační autoritě, ale musí splnit i další podmínky, například oprávnění k určité činnosti. Pak může svůj podpis používat např. pro ověřování výkresů jako autorizovaný projektant.

Sami usoudíte, k čemu jsou certifikáty použitelné – class 1 na hraní, class 2 prakticky taky a od třídy tři i pro seriozní práci.

Zákon 227/2000 Sb. o elektronickém podpisu

V českém právním řádu je elektronický podpis zakotven v zákoně č. 227/2000 Sb. ze dne 29. června 2000 o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), který byl (jak je u nás zvykem) již několikrát novelizován (226/2002 Sb., Změna: 517/2002 Sb., Změna: 440/2004 Sb., Změna: 635/2004 Sb., Změna: 501/2004 Sb.)

Zákon definuje tři typy certifikačních autorit (poskytovatelů certifikačních služeb):

a) poskytovatele certifikačních služeb (fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy)
b) kvalifikovaného poskytovatele certifikačních služeb (poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6 zákona)
c) akreditovaného poskytovatele certifikačních služeb (poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona)

Certifikáty, vydané autoritou typu a) jsou použitelné při osobní korespondenci, uvnitř firmy – nemají právní platnost. Poskytovatel typu b) vydává tzv. **kvalifikované certifikáty**, pomocí nichž lze vytvářet **zaručené elektronické podpisy**. Ty jsou na úrovni obyčejného podpisu a jsou použitelné pro podepisování občanskoprávních nebo obchodních smluv.

Poskytovatel typu c) musí splňovat náročné požadavky dané zákonem, ale jím vystavené certifikáty jsou použitelné i pro podepisování úředních listin, tedy i ke komunikaci se státní správou. Certifikáty tohoto typu jsou samozřejmě také nejdražší.

Využití ve školní praxi

Pro elektronickou komunikaci mezi studentem a školou je zapotřebí, aby studentem zaslaný e-mail byl řádně autorizován a aby byl neodmínutelný. Navíc je nutné najít co nejlevnější řešení alespoň na úrovni certifikátu Class 3. Bylo by možno využít zaručený elektronický podpis založený na kvalifikovaném certifikátu ve smyslu zákona č. 227/2000 Sb. o elektronickém podpisu. Takový podpis by škola pro běžnou komunikaci akceptovala [3], ale jeho vystavení není levná záležitost a pro účely, o které se zde jedná, je zbytečný.

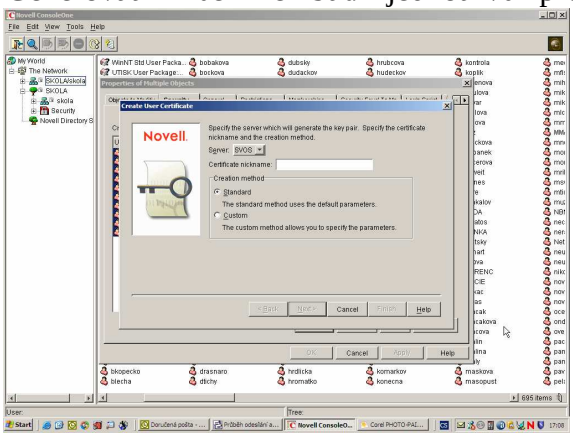
Lze využít freewareových nástrojů typu PGP, ale vystavení velkého množství podpisů pro studenty a výměna klíčů by byla organizačně velmi náročná (a prakticky nemožná). Zůstala tedy pouze možnost vytvoření vlastní certifikační autority razící certifikáty pro potřeby výše zmiňované komunikace. Tato certifikační autorita musí umožňovat ražení certifikátů pokud možno hromadně pro všechny studenty a musí být propojena s informačním systémem obsahujícím informace o všech studentech, aby si studenti mohli certifikáty exportovat sami. Protože SVŠES využívá OS NOVELL, padla volba na Novell certificate server 2.0.

NCS2 (podle [URL1]) je NLM modul typu Public Key Infrastructure (PKI NLM). Pro správu je dodáván Snap-in pro ConsoleOne a klientská aplikace Novell Certificate Console. NCS2 vytváří certifikáty vyhovující standardu X.509v3 obsahující mimo jiné jméno majitele certifikátu a veřejný klíč. Oba klíče – jak veřejný, tak i soukromý jsou uloženy v zašifrované podobě v NDS.

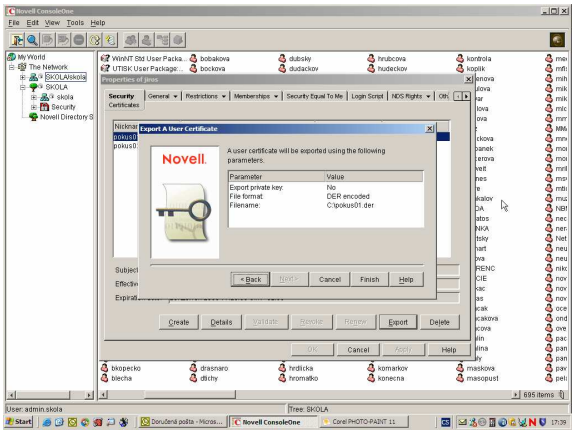
Při instalaci NCS2 je třeba vytvořit „Organizational CA“ (certifikační autoritu pro organizaci). Je pochopitelné, že optimální využití této technologie je ve spojení s ostatními produkty NOVELL (Novell LDAP Services for NDS, NetWare Enterprise Web Server a NetWare Management Portal, NOVELL Groupwise). Tyto produkty ale škola nevyužívá a ani to neplánuje. V průběhu instalace je vygenerován pár klíčů pro interní certifikační autoritu. Protože vůči již nejsou České republice stanovena omezení pro export šifrovacích technologií, bude vygenerován klíč o délce 2048 bitů. Soukromý klíč certifikační autority bude zašifrován a uložen jako skrytý atribut objektu Organizational CA v NDS. Veřejný klíč je přístupný pro export v NDS.

Vytvoření certifikátu

Výhodou použití NCS2 je možnost snadného generování párů klíčů a certifikátlů v libovolném počtu pro každého uživatele. Generovat klíče lze buď jednotlivě pro konkrétního uživatele (objekt USER v NDS) nebo hromadně. Při hromadném vytváření certifikátů je nutné pouze předchozí explicitní definování e-mailové adresy jako vlastnosti objektu USER (při individuálním vytváření je tvůrce vyzván k zadání).



Pro tvorbu se používá administrativní rozhraní Console One, které je standardní součástí OS NOVELL. Jde o JAVA aplikaci (pracuje tedy stejně prakticky na libovolné platformě, ale je poněkud pomalejší), kde označíme uživatele, pro které chceme razit certifikáty. Certifikát je třeba pojmenovat, zvolit jeho typ a vygenerovat. Po generování se uloží do NDS. Při ražení certifikátu jsou vygenerování i oba klíče (soukromý i veřejný) a v zašifrované podobě uloženy v NDS. Přístup k nim je také přes ConsoleOne. Současně je zpřístupněna volba „Export“



K exportu certifikátů jsou určeny dvě aplikace. Výše zmíněná Console One nebo Novell Certificita Console, což je jednoúčelová aplikace sloužící jen k exportu.

Exportovat je umožněn vlastníkovi certifikátu, ale i kterýkoliv jinému uživateli. Chování systému záleží na osobě přihlášené do NDS. Pokud certifikát exportuje jeho vlastník má možnost exportu veřejného i soukromého klíče. Ostatní mohou exportovat pouze klíč veřejný.

Certifikační autorita a její certifikát

S výjimkou instalace všechny činnosti provádí uživatel (v našem případě student) sám. A všechny činnosti splňují požadavky zadání – jsou pro průměrně IT zdatného uživatele jednoduché a přehledné (předpokládáme-li alespoň průměrnou znalost anglického jazyka). Pro účely využití podepsaného e-mailu školou – tedy jednoznačného určení odesílatele a vyloučení možnosti jeho zpochybnění – musíme zabezpečit, že příjemce (v našem případě učitel) může pohodlně ověřit důvěryhodnost podepsané zprávy. Protože ve škole využívají i učitelé MS Outlook či Outlook Expres, je situace ulehčena.

Outlook umožňuje definovat důvěryhodnost certifikátu ve třech úrovních

- absolutní důvěra
- absolutní nedůvěra
- důvěra odvozená od důvěry v certifikační autoritu

Protože je využívána certifikační autorita vlastní – dokonale důvěryhodná – nevzniká žádný problém. Každý uživatel (učitel) si musí do svého klienta importovat certifikát certifikační autority. Ten může získat opět každý uživatel pomocí administrativního rozhraní ConsoleOne.

Certifikát je třeba importovat mezi důvěryhodné kořenové certifikáty. V operačním systému MS Windows je k tomuto účelu využíván internetový prohlížeč MS Internet

Explorer. Od importu certifikátu můžeme všechny certifikáty, vydané naší certifikační autoritou považovat za důvěryhodné

Příjem e-mailu

Pokud uživatel odešle podepsaný e-mail, oznámí to MS Outlook při jeho načtení z POP3 serveru ikonou  . Ta sděluje pouze informaci, že zpráva je podepsaná elektronickým podpisem. Neříká nic o jeho důvěryhodnosti ani o tom, která certifikační autorita (a pokud vůbec nějaká) vystavila certifikát.

Pokud certifikační autorita nepatří mezi důvěryhodné, sdělí to Outlook při pokusu zprávu otevřít. Podpis je prohlášen za neplatný a je pouze na nás, jak se zachováme. Můžeme zprávu bez ohledu na kvalitu podpisu zobrazit, zobrazit podrobnosti o podpisu nebo upravit důvěryhodnost podle pokynů popsaných výše.

Pokud je certifikát certifikační autority naimportován do úložiště důvěryhodných kořenových certifikačních úřadů, není zobrazeno žádné hlášení (podpis je považován za platný) a zpráva je zobrazena.

Logo  v pravém rohu zobrazené zprávy indikuje platný podpis. Při klepnutí na něj jsou zobrazeny údaje o certifikátu. Zde můžeme individualizovat náš vztah k tomuto certifikátu – například prohlásit ho za nedůvěryhodný. Zpráva s nedůvěryhodným podpisem je v pravé části označeno logem  .

Závěr

Použití Novell Certificate serveru splňuje naše požadavky - *vytvořit systém, ve kterém s minimálními náklady (pokud možno žádnými) bude možno ověřit, že autorem (odesílatelem) e-mailu je konkrétní student.*

Ověření, zda je autorem e-mailu student školy je možno dodržet, protože export soukromého klíče je umožněn pouze konkrétnímu studentovi. Rizikem je prozrazení přístupového jména a hesla do systému Novell ve škole, ale zde je jen na studentovi, zda dodrží podmínky stanovené v bezpečnostní politice SVŠES.

Literatura

[URL1] www.novell. cz

[2] Rak, R., Janíček, P., Porada, V.: *Identifikace v policejní praxi podporovaná výpočetní technikou*. In: Sborník Bezpečnostní teorie a praxe. Praha : PA ČR, 2001

[3] Brechlerová, D.: *Elektronická dokumentace v univerzitním informačním systému – lze opravdu použít*? In. Pedagogický software 2004, sborník z odborné konference. České Budějovice – Jihočeská univerzita, 2004

[4] Doseděl, T.: *Počítačová bezpečnost a ochrana dat*. Brno : Computer Press, 2004

[5] Látal, I. a kol. *Ochrana informací, dat a počítačových systémů*. Praha : Eurounion, s. r. o. , 1996

[6] Přibyl, J., Kodl J.: *Ochrana dat v informatice*. Praha : vydavatelství ČVUT, 1997

Ing. Milan Hála, SVŠES, s. r. o., Lindnerova 575/1, Praha 8,
E-mail: milan.hala@svses.cz