Bezpečnost elektronických dat a elektronické komunikace

Andrea Kropáčová, CESNET

Svět moderních počítačových technologií a Internetu je pro řadu uživatelů světem bez jasně daných pravidel a základních záruk, které znají z běžného života. Světem, kde je možné existovat pod smyšlenou identitou, vytvořit si identitu novou, popřít své činy a spoléhat se na anonymitu, nepostižitelnost a nedokazatelnost. Na druhou stranu ale existuje mnoho lidí, možná většina, kteří si uvedená fakta neuvědomují, a všem informacím vystaveným na Internetu či šířeným prostřednictvím elektronické pošty slepě a nekriticky věří. Přitom i v případě papíru, základního záznamového média lidstva, si obvykle uvědomují, že je to snadno zfalšovatelná věc. Že na papír je možné napsat cokoliv, že podpis je možné dokonale napodobit, a že i podepsaný dokument je poté možné modifikovat. Vždyť právě proto si lidé v průběhu staletí vypracovali řadu metod pro *ověření věrohodnosti obsahu, podpisu a integrity* psaných dokumentů. Každý jistě zná podpisové vzory vyžadované bankou, notářsky ověřený podpis, podpis potvrzený přítomnými svědky, soudně ověřený podpis, dokument prověřený pomocí metod grafologie a dalších věd, ověřené kopie dokumentů a další bezpečnostní technologie.

Podobným problémem, jakým je zajištění věrohodnosti dokumentu, je i *bezpečný přenos* dat. Při něm je žádoucí, aby přenášený obsah znali pouze odesílatel a příjemce. Pro mnoho uživatelů je obvykle šokující zjištění, že běžný přenos dat po Internetu je ve své podstatě nezabezpečený a data jsou přenášena v té podobě (obvykle otevřené), jakou jim dal uživatel. Nejvíce je tato neznalost patrná v prostředí elektronické pošty, kdy se často uživatelé diví, že obsah jejich zpráv si cestou může přečíst i někdo jiný, než pouze adresát.

Přitom i ve světe počítačů existuje bezpečný způsob, jak vybavit elektronické zprávy podpisem a pravost tohoto podpisu ověřit, či jak zajistit obsah přenášených dat před nežádoucími slídily. Je jím *elektronický podpis* a *šifrování obsahu zprávy*.

Zašifrování zprávy

Pro vytvoření bezpečné (šifrované) zprávy a elektronického podpisu se v současné době využívají principy tzv. *asymetrické kryptografie*, která pracuje s *dvojicí klíčů (keypair)*. Jeden z klíčů – *veřejný* – se užívá k zašifrování dat a je možné jej zveřejnit. Druhý z klíčů, tzv. *privátní*, je určen k dešifrování; ten musí být pečlivě chráněn a musí jej znát pouze jeho majitel. Dvojice privátní/veřejný klíč je navržena tak, že z klíče veřejného není možné žádným způsobem odvodit ani spočítat klíč privátní. To zaručuje, že pouze držitel privátního klíče může zašifrovanou zprávu dešifrovat a získat její obsah.

Výměna zabezpečené (zašifrované) zprávy mezi odesílatelem a příjemcem vypadá následovně: odesílatel zašifruje data veřejným klíčem příjemce a odešle je na adresu příjemce; příjemce vezme svůj privátní klíč a zprávu rozšifruje. Podmínkou takové komunikace ovšem je, že odesílatel má k dispozici veřejný klíč adresáta. Získat jej může např. tak, že před započetím šifrované komunikace si uživatelé vymění elektronicky podepsané zprávy, čímž si vzájemně vymění i své veřejné klíče.

Základní algoritmy pro šifrování jsou algoritmy RSA (pojmenované po autorech - Ron Rivest, Adi Shamir and Len Adleman), pro el. podpis pak DSA (Digital Signature Algorithm). Zašifrování obsahu zprávy řeší utajení jejího obsahu tak, aby jej znali pouze odesílatel a příjemce (majitel privátního klíče ke klíči veřejnému, kterým byla zpráva zašifrována).

Elektronický podpis

Elektronický podpis supluje u elektronických zpráv v počítačovém světě ručně vytvořený podpis na písemných dokumentech. Měl by tedy zajistit, že:

- uvedená osoba podepsala data vědomě;
- podepsaná osoba je el. podpisem dostatečně ověřena;
- dokument je pravý a nebyl následně modifikován.

Elektronický podpis je vlastně informace, která se připojuje k datům, aby identifikovala odesílatele. Při procesu vytvoření el. podpisu není podepisována samotná zpráva, jak je u mnoha uživatelů zakořeněno z ekvivalentu papír-tužka, ale ze zprávy se nejprve pomocí tzv. *hashovací funkce* spočítá kontrolní součet (message digest) a ten se zašifruje privátním klíčem odesílatele. Kontrolní součet zašifrovaný privátním klíčem odesílatele je požadovaný el. podpis zprávy. Hashovací funkce pro výpočet kontrolního součtu musí splňovat následující požadavky:

- pro stejnou zprávu spočítá hashovací funkce vždy stejný kontrolní součet;
- z kontrolního součtu není možné zjistit tvar vstupních dat, ze kterých byl kontrolní součet spočítán;
- dvě různé zprávy nesmí vést ke stejnému kontrolnímu součtu.

Důvod, proč se šifruje pouze otisk zprávy (kontrolní součet) a ne celá zpráva, je ryze praktický. Zašifrování celé původní zprávy by vedlo k jejímu zdvojnásobení, kdežto připojením podepsaného otisku se zpráva zvětší pouze o pár bytů. Pro výpočet kontrolního součtu se v současné době používají algoritmy SHA1 a SHA2, které nahradily dříve používaný algoritmus MD5.

Uživatel, který chce zprávu vybavit el. podpisem, k tomu použije svého privátního klíče. Každý, kdo zná jeho veřejný klíč, může pomocí tohoto klíče ověřit pravost připojeného el. podpisu. Přesný postup je následující:

Vytvoření elektronického podpisu: Z dat se pomocí hashovací funkce vytvoří kontrolní součet zprávy. Kontrolní součet zašifrovaný privátním klíčem je požadovaný elektronický podpis vstupních dat, který se připojí k podepsané zprávě.

Ověření elektronického podpisu: Při ověřování elektronického podpisu se postupuje tak, že se pomocí stejné hashovací funkce vypočte kontrolní součet zprávy, pomocí veřejného klíče osoby, která data podepsala, se dešifruje el. podpis a získá kontrolní součet zprávy. V případě, že se oba kontrolní součty shodují, je pravost elektronického podpisu potvrzena. Příjemce el. podepsané zprávy si tak ověří:

- Autenticitu podepisující osoby, protože zprávu mohl podepsat pouze ten, kdo má k deklarovanému veřejnému klíči odpovídající klíč privátní.
- Integritu zprávy. Je-li el. podpis vyhodnocen jako korektní, znamená to, že zpráva nebyla cestou v době mezi vytvořením el. podpisu a jeho ověřením modifikována, protože hash je stejná jako při vzniku podpisu.
- Odpovědnost odesílatele. Protože privátní klíč zná pouze jeho držitel, je platný elektronický podpis důkazem, že danou zprávu opravdu vytvořil ten, kdo ji také podepsal.

Bezpečnost elektronického podpisu a šifrovaných zpráv

Z předchozího odstavce se může zdát, že el. podpis je plnohodnotným ekvivalentem ručně vytvořeného podpisu papírového dokumentu. Je ale nutné mít na paměti, že ruční podpis je výsledkem vědomé činnosti člověka, který drží v ruce psací pomůcku a v souladu se svými schopnostmi a vědomostmi za plného vědomí vytváří podpis. Kdežto elektronický podpis je řetězec dat, která vytváří software na základě vstupních dat a podmínek, které zná pouze podepisující se osoba.

Z výše popsaných principů el. podpisu a šifrovaných zpráv tedy plynou jeho bezpečnostní rizika a záruky, které jsou postavené především na ochraně privátního a veřejného klíče a bezpečnosti použitých algoritmů. Dá se tedy říci, že bezpečnost používání elektronického podpisu a šifrovaných zpráv je závislá na splnění následujících podmínek:

1. Nedošlo k narušení ochrany privátního klíče, tzn. může s ním disponovat pouze jeho držitel.
2. Nebyl prolomen algoritmus hashovací a šifrovací funkce.
3. Je zaručena a ověřena autenticita veřejného klíče ve vztahu k deklarovanému držiteli, tzn. je doložena pravost klíče (je nutné si být jistý na 100%, že daný klíč patří skutečně dané osobě).

V dnešní době supervýkonných počítačů, které usnadňují práci hackerů a lámání šifer, se kupodivu jako nejproblematičtější jeví podmínka číslo tři – ověření pravosti klíče a jeho vazby na deklarovaného držitele. Představte si, že byste rádi napsali šifrovanou zprávu člověku, který se jmenuje *Pepa Pádlo*, jeho adresa je možná *padlo@kajak.voda* a podaří se vám získat jeho veřejný klíč. Kdo vám ale zaručí, že je to opravdu Pepa Pádlo, a ne někdo, kdo se za něj poťouchle vydává? Tento problém je možné vyřešit v zásadě dvěma způsoby:

- Osobním předáním veřejného klíče danou osobou, kdy tato osoba vám osobně předá svůj veřejný klíč, např. na disketě, a vy máte zároveň možnost ověřit si její totožnost vyžádáním dokladu totožnosti.
- Poskytovatelem certifikačních služeb, tj. Certifikační autoritou.

V menším kolektivu lidí je možné jít první cestou a uživatelé mohou použít např. systém PGP (Pretty good privacy), kde je autentičnost veřejných klíčů postavena na vyslovené důvěře, kterou si držitelé klíčů vzájemně udělují.

V prostředí s velkým počtem uživatelů, kteří se často navzájem neznají, je vhodné jít cestou používání certifikátů a certifikační autority (CA).

Certifikát

Certifikát veřejného klíče je de-facto elektronický průkaz totožnosti, který spojuje člověka s jeho veřejným klíčem. Totožnost se prokazuje na základě znalosti soukromého klíče. Certifikát je podepsaný CA, která jej vydala.

Z hlediska počítačů je certifikát datová struktura obsahující informace o uživateli a především jeho veřejný šifrovací klíč. Nejrozšířenější je struktura certifikátu dle normy X.509 (zavedená doporučením ITU v roce 1988).

Kromě veřejného klíče obsahuje certifikát následující informace:

- Verzi vydaného certifikátu. Nula určuje, že se jedná o certifikát verze 1, jednička určuje verzi 2, dvojka verzi 3. Certifikáty verzí 2 a 3 jsou tzv. *rozšířené certifikáty*.
- Jednoznačné sériové číslo vydaného certifikátu. Je nutné, aby v rámci CA měl každý certifikát vydané unikátní číslo.
- Specifikaci algoritmu použitého pro el. podpis.
- Vymezení platnosti certifikátu od-do (data `notBefore` a `notAfter`). Před dosažením data `notAfter` by si uživatel měl nechat vystavit nový certifikát, z čehož vyplývá, že každý může vlastnit několik platných certifikátů současně.
- dentifikaci CA, která certifikát vydala.
- Identifikaci uživatele, pro kterého je certifikát vydáván, tzn. vlastníka dvojice veřejný/soukromý klíč.
- Alternativní jména/identifikátory subjektu (uživatele), např. e-mail adresu.

Certifikační autority

CA (Certifikační autority) jsou důvěryhodné objekty, které vystavují certifikáty a ověřují totožnost žadatelů. Certifikační autorita plní dvě základní funkce:

- Certifikační – zaručuje, že deklarovaný veřejný klíč přísluší dané osobě.
- Validační – potvrzuje platnost certifikátu.

V případě certifikační role se jedná o vydávání certifikátů uživatelům, kdy certifikát je de-facto dokument, který potvrzuje, že veřejný klíč patří jednoznačně dané osobě. Certifikát je podepsán certifikační autoritou.

Obecně se tedy dá říci, že certifikát je zpráva podepsaná certifikační autoritou, která říká zhruba následující: „Člověku, který se jmenuje Pepa Pádlo, patří adresa padlo@kajak.voda a jeho veřejný klíč je ‘bflmpsvz’“.

CA ručí především za dvě věci – za jednoznačnost vydaných certifikátů a za svázání veřejného klíče s jeho držitelem.

CRL (Certificate Revocation List)

Certifikáty se obvykle vydávají na dobu určitou, tzn. že jejich platnost je omezena. Certifikát může ztratit svou platnost dvěma způsoby:

1. Vyprší, tzn. uplyne čas `notAfter`.

2. Je zneplatněn před časem `notAfter`, přičemž zneplatněn může být na základě žádosti vlastníka nebo na popud CA, která jej vydala.

Ke zneplatnění na žádost vlastníka dochází v okamžiku, kdy došlo např. k prozrazení, nebo zcizení privátního klíče a hrozí tedy zneužití identity, nebo při změně údajů souvisejících s certifikátem. CA může certifikát zneplatnit v okamžiku, kdy ze strany vlastníka dojde k porušení politiky CA (např. jeho nedovolené použití), při chybě způsobené CA, nebo při změně údajů. Certifikáty se také odvolávají v případě, že některý z uvedených identifikátorů subjektu už není platný (např. změna e-mail adresy, příjmení, vztahu k organizaci uvedené v subjektu apod.)

Zneplatněné certifikáty CA uveřejňuje v tzv. seznamu zneplatněných certifikátů – CRL (Certificate Revocation List). Postup, jakým vlastník certifikátu může požádat o jeho zneplatnění, je popsán v politice dané CA, která certifikát vydala.

CRL obsahuje sériová čísla zneplatněných certifikátů a může být i prázdný! Certifikáty revokované před naplněním data `notAfter` se v CRL zveřejňují až do vypršení jejich původní doby platnosti.

Součástí CRL jsou kromě sériových čísel ještě další údaje, např. datum vydání předchozího CRL a datum vydání následujícího CRL. Uživatel si tak může ověřit, jestli nepropásl vydání předchozího CRL. Další užitečná položka je položka `RevocationDate`, která říká, kdy byl certifikát zneplatněn, tzn. shledán podezřelým. Od tohoto data by všechny podpisy tímto certifikátem měly být považovány za nevěrohodné.

O způsobu zveřejňování CRL rozhoduje daná CA, která tak může učinit například prostřednictvím el. listů nebo vystavením na webu.

Je v zájmu každého uživatele, aby si seznamy zneplatněných certifikátů těch CA, jejichž certifikáty používá, pravidelně aktualizoval a používal je.

Použití certifikátu

Aby uživatel mohl certifikát úspěšně používat, musí být splněno několik podmínek:

- Certifikát musí být platný, tzn. čas je mezi `notBefore` a `notAfter` a není uveden v CRL (nesmí být revokovaný).
- Certifikát musí být podepsaný CA, které uživatel důvěřuje, a který tudíž má v seznamu důvěryhodných CA.
- Uživatel musí mít k dispozici veřejný klíč té CA, která certifikát vydala.

V případě komunikace mezi dvěma uživateli si uživatelé nejdříve ověří podpis svého protějšku pomocí jeho veřejného klíče a posléze si ověří autentičnost veřejného klíče ověřením podpisu certifikátu pomocí veřejného klíče certifikační autority, která jej vydala. V daném případě se požadavek na důvěryhodnost vztahuje pouze k certifikační autoritě.

V případě validace se uživatel dotazuje certifikační autority na platnost certifikátu svého protějšku. Dotazy mohou být kladeny on-line, nebo lze využít CRL.

CESNET CA

Certifikační autorita CESNETu byla založena v roce 2001, původně pro potřeby projektu DataGrid. Od roku 2003 poskytuje své služby členům sdružení CESNET z.s.p.o. CESNET CA (`https://www.cesnet.cz/pki`) nabízí v současnosti tři základní služby:

1. Vydávání osobních certifikátů – slouží pro zabezpečení komunikace prostřednictvím el. pošty (standard S/MIME) a autentizaci (např. k privátním WWW stránkám)
2. Vydávání certifikátů serverů a služeb – slouží k autentizaci služeb a počítačů, největší uplatnění mají při chráněné WWW komunikaci
3. Certifikuje další úřady – členové sdružení CESNET mohou založit vlastní certifikační autoritu, kterou CESNET CA certifikuje. Tím mezi certifikačními autoritami vzniká vazba, tzv. *řetězec důvěry*, což v praxi znamená, že ti uživatelé, kteří věří CESNET CA, budou automaticky věřit i nově vzniklé CA, která má certifikaci od CESNET CA.

Přínos el. podpisu a šifrování zpráv

Přínos šifrování zpráv je zřejmý: ochrana citlivých dat na cestě mezi odesílatelem a adresátem a tím minimalizování jejich zneužití.

Elektronický podpis má mnohem větší efekt a uplatnění, když si uživatel uvědomí všechny souvislosti; nikoliv pouze tu, že vybavení zprávy el. podpisem příjemci potvrdí odesílatele a ukáže, jestli zpráva nebyla cestou změněna (třeba ani ne úmyslně s cílem škodit, ale např. špatně nebo příliš restriktivně nakonfigurovanou antispamovou ochranou). Zřejmě každý, kdo používá elektronickou poštu, se již setkal s tím, že mu od něj samotného přišla zpráva, o které ví, že si ji neposlal. Nebo mu kolega sdělí, že od něj obdržel zprávu, kterou ale ve skutečnosti odesílatel uvedený v dopise neposlal. Je to důsledek problému nazývaného „spamming“ a faktu, že do položky „Odesilatel“ v prostředí e-mailové komunikace, může být vloženo cokoliv, tedy i adresa někoho úplně jiného, než kdo zprávu skutečně odesílá. Člověk pak může být obviněn z něčeho, čeho se nedopustil. Řešením je opět (částečně) el. podpis. Částečně proto, že tento případ již vyžaduje znalost a používání principů el. podpisu v širším měřítku. Představte si svět, ve kterém každý člověk používající el. poštu, má osobní certifikát a odesílanou poštu poctivě podepisuje. V takovém světě je pak ověření, jestli daná zpráva skutečně pochází od v ní uvedeného odesílatele, záležitostí vteřin. V případě, že dopis podepsán není nebo podpis není korektní, platí, že je nepravděpodobné, že zprávu skutečně odeslal uvedený odesílatel a tudíž jej za obsah zprávy není možné činit zodpovědným. Ano jistě, takový svět je teprve budoucností.

Uživatelé často kladou otázku „Kdy mám podepisovat a kdy mám šifrovat?“. Samozřejmě je možné obojí současně. Osobně *doporučuji podepisovat každou odesílanou zprávu*, *šifrovat je pak vhodné ty zprávy, které nesou citlivý obsah*, který by měl znát pouze příjemce.

K čemu se to dá použít dál?

Elektronický podpis a možnost zašifrovat zprávu posílanou el. poštou nejsou jedinými možnostmi jak využít veřejný a privátní klíč (X509 certifikát, nebo PGP). Elektronický podpis se dá využít např. také pro podepsání WWW stránky s citlivými údaji a obecně pro podepsání, a tím ochranu integrity jakýchkoliv el. dat – souboru, obrázku a podobně.

Osobní X509 certifikát nebo PGP klíč je možné použít také pro ochranu osobních dat na pracovní stanici a na záznamovém médiu. Stačí soubor s citlivými daty zašifrovat.

Dalším využitím je *autentizace*. Autentizace je proces ověření identity uživatele (nebo služby). Nejrozšířenější metodou autentizace je kombinace uživatelského jména (login) a hesla (password), které se ověřují proti nějaké databázi. Autentizační mechanismy založené na PKI (Public Key Infrastructure), kdy každý uživatel (a služba) mají vydán vlastní certifikát veřejného klíče podepsaný důvěryhodnou CA, přinášejí do oblasti autentizace škálovatelnost, robustnost a usnadňují administraci.

Závěr

Možná vás po přečtení tohoto článku napadne otázka – „A jak vlastně ten elektronický podpis získám?“. Elektronický podpis sám o sobě samozřejmě získat nelze. Prvním krokem na cestě k jeho používání je získání PGP klíče nebo X509 certifikátu. V případě PGP klíčů doporučuji podívat se například na stránky `http://www.pgp.cz` a konzultovat to se zkušenějšími kolegy. V případě X509 certifikátů je zásadní otázkou „Na kterou CA se mohu obrátit se žádostí o certifikát?“ V tomto případě doporučuji porozhlédnout se v rámci university a zjistit, jestli ta CA neprovozuje.

Získání certifikátu veřejného klíče samozřejmě není pro ochranu dat a el. komunikace posledním krokem, není samospasitelné a určitě není jednorázovým řešením. Ruku v ruce s používáním certifikátu jde ochrana privátního klíče před zcizením a zničením. To v praxi znamená dobře uvážit, kde je možné privátní klíč uložit (pouze na zabezpečený stroj, který je plně pod vaší správou) a jak s ním nakládat (mít zálohu, nikomu jej „nepůjčovat“ a podobně). Samozřejmě je vhodné být připraven i na možnost zcizení privátního klíče a na tuto skutečnost rychle reagovat zneplatněním.

Co říci závěrem? Snad jen doporučení – podepisujte a šifrujte. Není tak daleko doba, kdy tyto mechanismy budou nedílnou součástí běžného života, a čím větší počet lidí si na jejich užívání navykne, tím bude efektivnější. Bezpečná komunikace už v dnešní době není planá fráze, ale nutnost a realita. □