Masarykova univerzita v Brně

Filozofická fakulta

Ústav české literatury a knihovnictví

Kabinet informačních studií a knihovnictví

ELEKTRONICKÝ PODPIS

(Úvod do problematiky)

Seminární práce k předmětu Informační politika

Autor: Pavlína Habrovanská

UČO: 215551

Typ studia: prezenční

Ročník: 2. NMgr.

Brno

2. listopadu 2012

2. 11. 2012

Elektronický podpis

Úvod do problematiky

Kvůli vzrůstajícímu počtu elektronických dokumentů, a to jak původně elektronických, tak následně digitalizovaných, se zvýšila potřeba vymyslet způsob, jak zaručit funkce vlastnoručního podpisu u elektronických dokumentů [1, s. 5]. Proto byl zaveden – fakticky i právně – pojem **elektronický podpis**.

„*elektronickým podpisem se rozumí (pro účely tohoto zákona) údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě*“ [5, § 2, písm. a]

Dle této definice se nepožaduje časové razítko, není definován žádný konkrétní formát nebo standard, jenž by popisoval tvar vytvořených či předávaných dat. Navíc není použit certifikát ani jiný způsob zveřejnění pomocných dat (dat pro ověřování podpisu, osobních dat podepisující osoby, informace o systému použitém při podpisu atp.), tato data nejsou definována. Nejsou kladeny žádné konkrétní požadavky na použitý podpisový systém či na prostředek pro vytváření elektronického podpisu a jeho ověřování [1, s. 103, 104].

Tento typ podpisu tedy nemá pro příjemce dostatečnou vypovídací hodnotu, důvěra v něj je minimální. Slouží hlavně pro informaci příjemce. Proto je důležitější spíše **zaručený elektronický podpis** [1, s. 104].

Dva základní typy elektronických podpisů: zaručený a uznávaný

Zaručený elektronický podpis [5, § 2, písm. b]

- zaručeným elektronickým podpisem se rozumí (pro účely tohoto zákona) elektronický podpis, který splňuje tyto požadavky:
  - je jednoznačně spojen s podepisující osobou,
  - umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
  - byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

- k datové zprávě, ke které se vztahuje, je připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Uznávaný elektronický podpis

- „uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby“ [5, § 11, ods. 3a, s. 11]
- takový elektronický podpis nám uzná úřad (orgán veřejné moci)

Legislativní ukotvení

V členských zemích Evropské unie je problematika nahrazení elektronického podpisu za rukou psaný podpis řešena pomocí Směrnice Evropského parlamentu a Rady 1999/93/ES z 13. prosince 1999. Do české legislativy byla zapracována zákonem o elektronickém podpisu č. 227/2000 Sb.[1] Tento zákon byl několikrát novelizován [2, s. 30].

Stát užití elektronického podpisu v mnoha situacích nařizuje – v souvislosti s celkovou elektronizací veřejné správy a jejích agend. Praktické využití nachází elektronický podpis v řadě oblastí [2, s. 125, 126]:

- **e-government**: jedná se o náhradu rukou psaného podpisu ve styku občanů se státní správou a samosprávou a také mezi jednotlivými orgány státní správy a samosprávy mezi sebou
- **e-business**: EU vydala „Směrnici o elektronickém obchodu“ - cílem je přispěk k řádnému fungování vnitřního trhu EU tak, že podpoří volný pohyb služeb společnosti mezi členskými státy; jedná se zejména o elektronické sjednávání obchodních smluv
- **e-faktura**: daňový doklad může být vystaven i v elektronické podobě, pokud jej plátce opatří elektronickým podpisem založeným na kvalifikovaném certifikátu nebo elektronickou značkou
- **e-procurement**: elektronické zadávání veřejných zakázek
- **e-health**
- **e-banking**

Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace fyzických osob

1 Zákon je možné stáhnout na webových stránkách Ministerstva vnitra České republiky v sekci eGovernment: <http://www.mvcr.cz/clanek/elektronicky-podpis-archiv-pravidla-pro-vyrizovani-elektronicke-posty.aspx>.

v prostředí Internetu [3].

Elektronický podpis je v podstatě hodně velkým číslem. Tak velkým, že by nebylo šikovné psát ho jako binární číslo (tedy posloupností jedniček a nul). Jako s číslem pracují s elektronickým podpisem počítačové programy, které jej ověřují. Výsledek takového ověření zobrazí uživateli v uživatelsky přívětivé podobě [4, s. 9].

Elektronický podpis je pro každou podepsanou zprávu jiný a odvozuje se od této zprávy (jakým způsobem – uvedeno níže v sekci **Modelový příklad**.) [1, s. 94, 95]. To znamená, že je vždy pevně spjat s posílanou zprávou a je jedinečný.

Základní principy

V souvislosti s otázkami počítačové bezpečnosti jsou důležité čtyři základní principy:

- důvěrnost (utajení),
- autenticita (identifikace),
- integrita,
- nepopiratelnost.

Elektronický podpis zajišťuje:

- **nepopiratelnost** (neodmítnutelnost) – každý je zodpovědný za to, co podepsal, autor se nemůže vzdát zodpovědnosti za sdělení opatřené jeho podpisem (např. u výhružných dopisů), je nepopiratelné, že právě on je autorem, když zprávu (dokument) opatřil elektronickým podpisem, který je vytvořen na základě jeho soukromého klíče – zná ho jen on (je povinen svůj soukromý klíč pečlivě střežit)
- **autenticitu = identifikaci** – tzn. je možné ověřit identitu autora, protože pouze autor vlastní jedinečný soukromý klíč
- **integritu** (neporušenost ve smyslu neměnnosti) – obsah sdělení nebude pozměněn, pokud ano, příjemce to pozná, pokud bude dokument změněn „na cestě“, nebude k němu sedět jeho elektronický podpis [4, s. 9]

Elektronický podpis ale nezajišťuje důvěrnost – zprávu si může přečíst kdokoliv, protože veřejný klíč je dostupný všem. Důvěrnost může být zaručena použitím jiné kryptografické metody.

Elektronický podpis z hlediska matematiky

Elektronický podpis funguje na základě matematických principů asymetrické kryptografie, kterou si

stručně představíme. Kromě asymetrické kryptografie existuje také kryptografie symetrická, která je pro pochopení problematiky jednodušší a přirozenější.

Symetrická kryptografie

Používá jeden klíč pro zašifrování obsahu i pro jeho dešifrování. Tento způsob je tak možné přirovnat k zamknutí dat do trezoru – klíč od něj můžeme dát jen povolané osobě. Při manipulaci s daty pak pracujeme s celým trezorem, čili nám nemusí vadit, když někdo trezor po cestě zachytí či zkopíruje, když jej bez klíče nedokáže otevřít [4, s. 392].

Klíč nesmí jít uhodnout, proto je generován **náhodně** (ona náhodnost je poměrně problematický pojem, protože je obtížné počítačem vygenerovat skutečně náhodné – tedy nepředvídatelné číslo; využívá se k tomu fyzikálních jevů, jako jsou měření aktivity pevného disku, ale také lze využít časových parametrů získaných sledováním stisků kláves) počítačem. Výpočetně je symetrické šifrování mnohem méně náročné než asymetrické, nepotřebuje tedy velkou výpočetní kapacitu počítače [4, s.392].

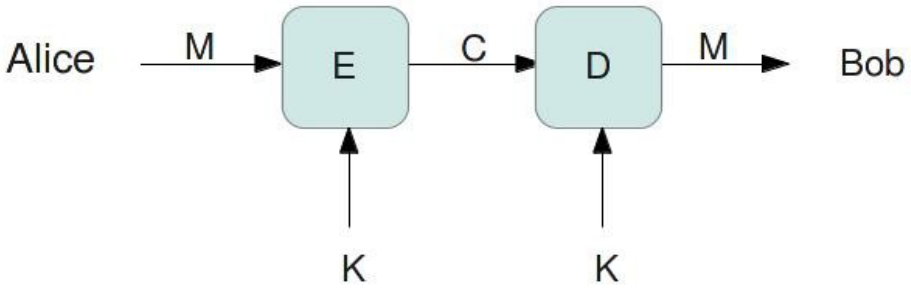
Pro bezpečnou distribuci klíče je samozřejmě lepší, když se obě strany znají a mohou si klíč předat osobně. Složitější případ nastává, pokud se dva lidé, kteří spolu musí komunikovat pomocí symetrické kryptografie, vůbec neznají. [4, s. 392, 393].

Symetrická kryptografie zajišťuje:

- **důvěrnost**: klíč není nikde zveřejněn (někdy se mu říká také tajný), znají ho jen dva lidé, pouze ti mohou zašifrované zprávy dešifrovat
- **autenticitu**: příjemce je schopen ověřit, že zprávu napsal ten druhý z dvojice, nikdo jiný nezná klíč
- **integritu**: pokud si odesilatel a příjemce zvolí nějaký formát zprávy (např. HTML), potom lze ověřit, zda došlo ke změně zašifrovaných dat; při (neoprávněné) změně zašifrované zprávy bude po dešifrování zřejmé, že je formát porušen.

- nezajišťuje nepopiratelnost – zprávu mohla vytvořit Alice, ale stejně tak i Bob, tj. skutečný autor může popřít, že zprávu napsal

Alice posílá Bobovi zprávu. Už dříve mu předala tajný klíč, kterým A zprávu zašifruje a B ji následně rozšifruje.



M = message: zpráva

K = key: klíč

E = enryption: zašifrování

C = cryptotext: zašifrovaná zpráva

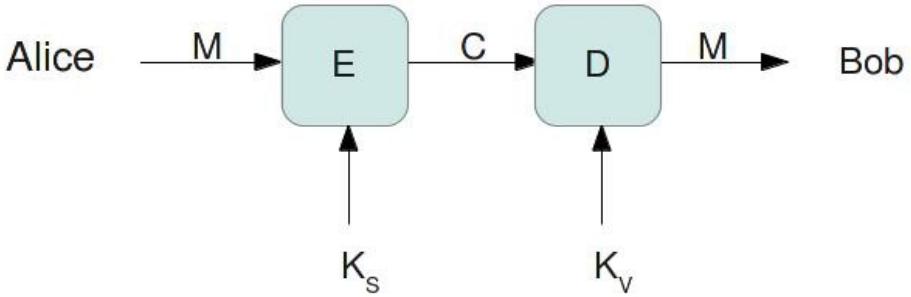
D = decryption: dešifrování

Za bezpečné se v symetrické kryptografii považují klíče už o délce 80 bitů (10 Bytů).

Asymetrická kryptografie

Používá dva různé klíče: jeden soukromý a jeden veřejný. Osoba, která disponuje soukromým klíčem, musí zajistit, aby byl řádně utajen a nedostal se nikomu do rukou.

- veřejný se vystaví na veřejné místo, např. na webové stránky; může být přiložen přímo k podepsanému dokumentu



K_S = private key: soukromý klíč

K_V= public key: veřejný klíč

K_S a K_V spolu tvoří pár.

Soukromý klíč – je nutné si ho pečlivě hlídat, nikomu ho nesdělovat; používá se při procesu vytváření podpisu (podepisování)

Veřejný klíč – je určen k poskytnutí komukoli, kdo si chce ověřit platnost podpisu; používá se při ověřování podpisu

V současné době se v případě asymetrické kryptografie používají klíče o délce 1024 bitů, 2048 bitů a 4096 bitů. Klíče o délce 1024 bitů jsou však již považovány za příliš krátké, tedy jen málo bezpečné, standardní délka je 2048; a je-li požadováno, aby klíč vydržel delší dobu, je vhodné použít 4096 bitů.

Podle toho, zda se k šifrování použije klíč soukromý, anebo veřejný, rozlišujeme **podepsání zprávy**, anebo **utajení zprávy**. Při šifrování soukromým klíčem lze zprávu dešifrovat pouze klíčem veřejným – může tak učinit kdokoliv, čímž se ověří, že zpráva byla zašifrována právě párovým klíčem soukromým (a žádným jiným). V opačném případě může zprávu zašifrovat kdokoliv (použije se klíč, který je veřejný), ale dešifruje ji pouze majitel soukromého klíče, zpráva tak byla utajena.

Algoritmy pro asymetrickou kryptografii

- **RSA** – umožňuje jak podepsat, tak utajit; je postaveno na situaci, kdy se vygenrují dvě velká prvočísla a vynásobí se, útočník potom není schopen z tohoto velkého čísla získat zpět obě prvočísla (trvalo by mu to příliš dlouho)
- **DSA/DSS** – umí pouze podepisovat, ne utajovat; používá se v USA jako algoritmus pro uznávaný elektronický podpis
- **DH** – umí pouze utajovat, ne podepisovat

Podepisující osoba

Podepisující osobou může být dle zákona č. 227/2000 Sb. pouze fyzická osoba (stejně jako v případě vlastnoručního podpisu). V organizacích (firmách apod.) jsou vždy určeni pracovníci s pravomocí zastupovat ji, kteří jsou oprávněni opatřovat listiny svým podpisem, a tak jednat jménem právnické osoby – analogicky se postupuje i v případě elektronického podepisování [1, s. 134].

Pokud by soukromý klíč sdílelo více osob, byla by tím porušena jeho podstata. Totiž, přestal by být klíčem soukromým a nebylo by možné jej využít pro zajištění požadovaných bezpečnostních

funkcí (např. nepopiratelnost).

Certifikát

Certifikát veřejného klíče je datová struktura, jež spojuje identifikaci žadatele s jeho veřejným klíčem. Vazba je potvrzena digitálním podpisem nezávislé třetí strany – tzv. **certifikační autority** [2, s. 345]. Právě touto certifikací se uznávaný elektronický podpis liší od zaručeného.

Certifikát je tedy potvrzením o tom, že veřejný klíč je skutečně klíčem konkrétní osoby, jejíž identita je v certifikátu popsána. Rovněž stvrzuje, že příslušná osoba je držitelem odpovídajícího soukromého klíče (s nímž je veřejný klíč do páru), který má ve své (výlučné) moci. Certifikát může být vydán pouze fyzické osobě [4, s. 37, 38], stejně jako může být podepisující osobou pouze osoba fyzická. Kvalifikovaný certifikát musí obsahovat náležitosti dané zákonem podle § 12.

Certifikační autority

Ten, kdo vydává certifikáty, je běžně označován jako **certifikační autorita**, v terminologii zákonů a vyhlášek jako **poskytovatel certifikačních služeb**. Takovou certifikační autoritou může být například banka, která vydává certifikát pro zabezpečení svého internet bankingu [4, s. 42].

Certifikační autorita má také za úkol sledovat, aby nevydala více certifikátů pro stejný veřejný klíč. To je sice málo pravděpodobné, ale ne nemožné; pak by více osob mělo stejný veřejný klíč – a tím pádem i soukromý. Generování shodných párových dat se však zamezuje užíváním kvalitních generátorů náhodných čísel při generování dvojice veřejný/soukromý klíč, jsou to tzv. pravé generátory náhodných čísel (true random). Díky tomu je pak nepravděpodobné, že by si dva různí uživatelé vygenerovali stejná párová data. Je však třeba myslet i na možné útoky postranními kanály. Jak bylo uvedeno výše, certifikační autorita musí sledovat možnou duplicitu a zamezit jí (nevydáním více certifikátů pro shodný veřejný klíč) [2, s. 58].

Kvalifikované certifikační autority

Důležitějším pojmem jsou však **kvalifikované certifikační autority**. Ty jsou oprávněny vydávat kvalifikované certifikáty přesně definované zákonem (§ 6) a splňují všechny další požadavky na jejich fungování vyplývající ze zákona (§ 6a, 6b) [4, s. 42].

Stát na základě splnění všech požadavků vyplývajících ze zákona může kvalifikované certifikační autoritě udělit **akreditaci**[2]. Pokud nemá kvalifikovaná certifikační autorita udělenou akreditaci, neznamená to, že není důvěryhodná. Akreditace je spíše nutný – zákonem stanovený –

2 Aktuální přehled akreditací lze nalézt na webových stránkách MV ČR: <http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx>.

předpoklad, který souvisí s požadavkem, kdy chce fyzická osoba komunikovat s orgány veřejné moci – v takovém případě musí používat uznávaný elektronický podpis. Ten je založen na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb [4, s. 43]. Z toho vyplývá, že třeba živnostníci musí mít certifikován svůj elektronický podpis u kvalifikované certifikační autority, která má od státu udělenou akreditaci, aby mohli podat například daňové přiznání.

Časové razítko

V **časovém razítku** je uveden údaj o vzniku elektronického podpisu, který osobě poskytla důvěryhodná třetí strana. Principem je, že se důvěryhodnýčasový údaj nebude vkládat do samotného podpisu podepisující osoby, ale je vložen do dalšího podpisu vytvořený tím, kdo tento časový údaj poskytuje [4, s. 77].

Stejně jako je certifikát veřejného klíče datovou strukturou, která spojuje identifikaci žadatele s jeho veřejným klíčem, přičemž je tato vazba stvrzena elektronickým podpisem nezávislé třetí strany, je i časové razítko podobná datová struktura, jež ale svazuje dokument s určitým časem. Časové razítko slouží jako **důkaz, že dokument existoval v daném čase** [2, s. 345].

Časové razítko obsahuje čas, hash dokumentu, jméno vydavatele razítka a pořadové číslo. Vše je stvrzeno nezávislou třetí stranou – Autoritou pro vydávání časových razítek. V české legislativě se takové autority nazývají: kvalifikovaní poskytovatelé certifikačních služeb, vydávající kvalifikovaná časová razítka [2, s. 345].

Hashovací funkce

Zpráva (e-mail, dokument v PDF, obrázek, video...) je posloupnost Bytů, často velmi dlouhá.
Z libovolně dlouhé posloupnosti Bytů lze vypočítat tzv. **hash** pomocí **hashovací funkce**[3]:

- vstupem je libovolně dlouhá posloupnost Bytů
- výstupem je fixní posloupnost Bytů, nejčastěji 128 bitů (16 Bytů), 160 bitů (20 Bytů), 256 bitů (32 Bytů) nebo 512 bitů (64 Bytů); výstup se nazývá *hash* nebo také *otisk* – zprávu jednoznačně charakterizuje
- není výpočetně náročná

Podmínky hashovací funkce

1. Hashovací funkce je **jednocestná** => z výsledku nelze získat zpět vstup (je výpočetně

3 Někdy se označuje počeštěně jako hašovací či hešovací funkce.

náročné až nemožné[4] z výstupu hashovací funkce získat původní vstup).

2. Je výpočetně náročné až nemožné nalézt dvě různé zprávy, které mají stejnou hash (otisk), říkáme, že je funkce **bezkolizní**[5].

Hashovací algoritmy

- MD5 – zjistilo se, že není odolná proti kolizím, a proto se nedá použít pro elektronické podepisování; nahrazuje se jinými algoritmy
- SHA1 – použitelný, prozatím nekolizní, do budoucna však nedoporučovaný
- SHA2 – vylepšený, málo rozšířený

Kvalitní hashovací agoritmy dávají výrazně odlišný výsledek při drobné změně původního textu (aby mohla být tato změna snadno nalezena). Pokud se například počítá hash pro digitální podpis z textu nesoucího platební příkaz, nebylo by žádoucí, kdyby se po připsání nuly k převáděné částce hash nezměnil [2, s. 21].

Modelový příklad

Bob dostal zprávu (M) od Alice a chce:

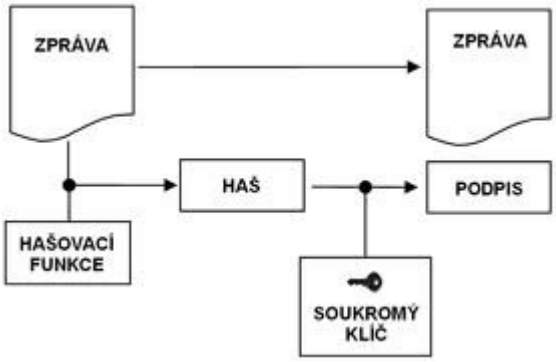
- ověřit, že zpráva je skutečně od Alice => autenticita (identifikace)
- ověřit, že zprávu nikdo po cestě nezměnil => integrita
- být schopný prokázat, že zpráva je od Alice => nepopiratelnost

Alice posílá zprávu (M) společně s podpisem zprávy (S) Bobovi.

$$E(h(M)) = Sign(M) = S$$
$$\Uparrow$$
$$K_S$$

Postup A: Podpis (S) získá Alice tak, že vypočítá hash zprávy h(M) o délce 256 bitů (délka závisí na zvoleném algoritmu) a tento hash zašifruje (E) asymetrickou kryptografií pomocí svého soukromého klíče (K_S).

4 Trvalo by to např. několik milionů let.
5 Kolize = dvě různé zprávy se stejnou hashí.

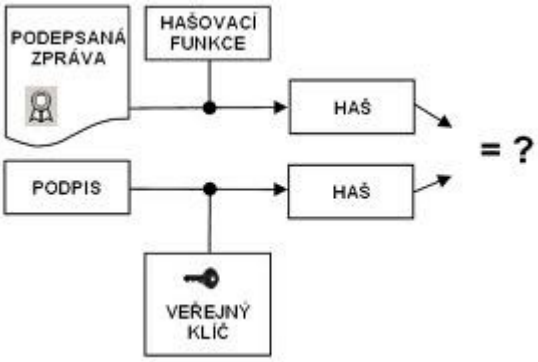


(Obrázek převzat z [5, s. 7].)

Zpráva spolu s podpisem přijde Bobovi, který chce ověřit tři výše uvedené body:

$$D\,(E\,(h\,(M))) = h\,(M)$$
$$\Uparrow \quad \Uparrow$$
$$K_V \; K_S$$

Postup B: Bob dešifruje podpis (S) pomocí veřejného klíče (K_V), který získal od Alice, čímž získá hash zprávy. Dále spočítá hash ze zprávy samotné a obě hodnoty porovná. Pokud se rovnají, je elektronický podpis ověřen a uznán za platný.



(Obrázek převzat z [5, s. 7].)

Elektronický podpis se stal jedním ze zájmů (nejen) české společnosti. Stalo se to vlivem vývoje technologií, především Internetu, který nabízí velké množství aplikací. Již není tolik běžné pracovat s daty „na papíře“, tisknout každý dokument – tato agenda se přenesla do elektronického prostředí. Toto prostředí je však nutné opatřit postupem, který zajistí možnost identifikace konkrétní osoby. Elektronický podpis je jedním z těchto postupů. Zatím se nachází v začátcích, jak o tom svědčí i stále vydávané novely zákony č. 227/2000 Sb. Nakolik uspěje, ukáže čas a praxe.

Použité zdroje

1. BOSÁKOVÁ, Dagmar a kol. *Elektronický podpis: Přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů.* Olomouc: Anag, 2002. ISBN 80-7263-125-X.
2. DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. Brno, 542 s. ISBN 978-80-251-2619-6.
3. Ministerstvo vnitra české republiky [online]. *Informace k používání elektronického podpisu*. 2010 [cit. 2012-10-20]. Dostupné z: <http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx>.
4. PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ.NIC, c2011, 430 s. ISBN 978-80-904248-3-8.
5. SVOBODA, Petr. *Systémy elektronických podpisů*. Brno: Masarykova univerzita. Fakulta informatiky. Katedra počítačových systémů a komunikací, 2006. Vedoucí diplomové práce doc. Ing. Jan Staudek, CSc.
6. *Zákon č. 227/2000 Sb. o elektronickém podpisu*. 2012 [cit. 2012-10-21]. Dostupné z: <http://www.mvcr.cz/e-podpis-legislativa.aspx>.