Digitální a elektronický podpis ve světě a v EU. Legislativní a standardizační aspekty.

Ing. Jaroslav Pinkava, CSc., AEC s.r.o.

Úvod

S nástupem širokého využívání nových informačních technologií se lidská společnost dostává do nové situace. Narůstá množství dokumentů v digitální podobě. V situacích, kdy i klasické papírové dokumenty jsou přenášeny digitálními linkami (např. faxem), riziko padělání podpisu význačně narůstá a obvyklý podpis přestává stačit. Pravost dokumentu je třeba potvrdit jinou cestou.

Digitální versus elektronický podpis

Samotný pojem *digitálního podpisu* se objevuje s nástupem asymetrické kryptografie. Digitální podpis zajišťuje autentizaci (jednotlivce, serveru, služby,…). Je to (obecně řečeno) řetězec znaků, který určitým způsobem spojuje příslušný veřejný klíč a samotnou zprávu. Pouze osoba znající zprávu a odpovídající soukromý klíč mohla vytvořit tento řetězec. Kdokoli, kdo zná zprávu a veřejný klíč, může tento digitální podpis verifikovat.

Pro vytvoření digitálního podpisu je nutné mít příslušný dokument v digitální podobě. To někdy ještě může být nevýhodné. Na druhou stranu procento dokumentů, které jsou zpracovávany už jako digitální, nebo jsou do digitální podoby přetvářeny, stále narůstá. Důležitou (a vlastně základní) vlastností podpisů je jejich odolnost proti zfalšování. Zde lze zkonstatovat neporovnatelné výhody digitálního podpisu oproti klasickému podpisu.

Z technologického hlediska jsou pro realizaci digitálních podpisů východiskem algoritmy kryptografických systémů s veřejným klíčem. Dnes existuje již celá škála takovýchto algoritmů. Pro praktické použití je však vhodné využívat pouze ty algoritmy, které jsou předmětem různých mezinárodních norem a specifikací (DSA, RSA, ECDSA). Důvody jsou zřejmé, prostředky a postupy pro podepisování i prostředky a postupy pro ověření tohoto podpisu musí být široce dostupné a interoperabilní.

Důležitým souvisejícím pojmem je pojem *digitálního certifikátu* příslušného veřejného klíče.Uživatelé musí být schopni získat bezpečnou cestou klíče, které potřebují k zašifrovaní svých dat. Pro systémy s veřejným klíčem zde musí být cesta, jak se podívat, jaký veřejný klíč používá druhá strana. A na druhé straně musí existovat cesta ke zveřejnění vlastního veřejného klíče. To ale nestačí. Uživatel musí mít důvěru v legitimnost takto získaného klíče. V opačném případě by mohl narušitel buď zaměnit veřejný klíč ležící někde v adresáři nebo by se mohl vydávat za někoho jiného. Pro tyto účely slouží certifikáty. Digitální certifikát označuje vlastníka veřejného klíče a asociuje vlastníka a veřejný klíč. Dovoluje verifikaci tvrzení, že daný veřejný klíč patří skutečně danému jedinci. Certifikáty pomáhají chránit se před možností, že někdo falzifikuje klíč s cílem vydávat se za někoho jiného. Další informace k souvisejícím pojmům (např. certifikační autorita, seznam odvolaných certifikátů atd.), lze nalézt např. v [7].

Obecnějším pojmem než digitální podpis je pojem *elektronického podpisu*. Tento pojem v sobě zahrnuje (kromě samotného digitálního podpisu) také aspekty využití celé škály různých biometrických metod. Je pak obvykle precizován tak, aby byl tzv. technologicky nezávislý. Je proto také vhodný pro použití v různých legislativních dokumentech. Zejména v průběhu posledních let se (z hlediska právních a technologických aspektů) dospělo k poznání nezbytnosti používat takto obecný pojem.

Biometrické metody

Existují dva základní typy biometrických technik:

a) *fyziologicky* založené techniky, které měří nějakou fyziologickou charakteristiku dané osoby. Sem patří např.: otisky prstů, charakteristiky duhovky, obličej, geometrie cév, charakteristiky uší, vůně, analýza obrazců DNA, charekteristiky potu atd.
b) *behaviorálně* založené techniky, které se zabývají měřením chování příslušné osoby. Toto zahrnuje např.: verifikaci ručně psaných podpisů, charakterizace úderů do klávesnice, řečová analýza atd.

Zaznamenaná biometrická charakteristika může být různými cestami uložena na záznamové médium a později využita k identifikaci (autentizaci) příslušného jedince. Spolehlivost použitého systému pak spočívá v tom, jakým způsobem je daný systém autentizace chránen proti celé řadě postupů, metod a technik útoků, které mohou být prováděny s cílem zneužít tuto autentizační metodu.

Využití elektronických podpisů

Elektronické podpisy jsou používány:

- pro oficiální komunikaci s veřejnými institucemi (daňová přiznání, přenos dokumentů s právními důsledky,…)
- pro vazby typu smluv v otevřených sítích (např. elektronický obchod, finanční transakce)
- v uzavřených systémech (Intranety)
- pro osobní účely
- pouze pro identifikační a autorizační účely (oprávnění přístupu do výpočetního systému, identifikace webovského serveru,…)

Některé momenty z historie legislativy digitálních podpisů, současná situace ve světě.

Stručně uvedu některé významné informační zdroje:

Mezinárodní dokumenty (UNCITRAL):
První mezinárodní dokument k elektronickým podpisům. Je znám jako Modelový zákon UNCITRAL pro elektronický obchod
http://www.uncitral.org/en-index.htm.
OECD
Různé iniciativy v oblasti elektronického obchodu:
http://www.oecd.org
Evropa
Užitečnou EU webovskou stránkou k iniciativám v oblasti elektronických a digitálních podpisů a příslušných právních aspektů (také elektronický obchod atd. z hlediska EU kontextu) je následující stránka:.
http://www2.echo.lu/legal/en/ecommerc/digsig.html
Direktiva EU k elektronickému podpisu byla Evropskou komisí schválena 30.11. 1999.
Je očekáváno, že vlády jednotlivých zemí EU uvedou tuto direktivu do svého zákonodárství během následujících 18 měsíců (do konce června 2001, to je oficiální termín daný touto direktivou). Text lze získat na adrese:
http://europa.eu.int/comm/dg15/en/media/sign/index.htm

Německo:
Neoficiální znění a komentáře k německému zákonu o digitálním podpisu (z roku 1997) lze získat na adrese:
http://www.kuner.com
Irsko
Text dokumentu, které jsou nazvány „Consultation Paper“ a „Proposed E-Commerce Bill“.
http://www.ecommercegov.ie
Spojené království
The Electronic Communications Act:
http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmbills/004/00004--a.htm
http://www.dti.gov.uk/cii/elec/ecbill.html
http://www.parliament.uk/commons/selcom/t&ipnot.htm
USA
Následující stránka je užitečná z hlediska posouzení zákonodárství v jednotlivých státech:
http://www.mbc.com/ecommerce.html
Byla přijata celá řada dokumentů jak na úrovní jednotlivých států, tak na federální úrovni. Vůbec prvním legislativním dokumentem (i ve světě) je „Utah Digital Signature Act“, který vychází z American Bar Association Digital Signature Guidelines. Stát Utah ho přijal již 27 února 1995.
http://www.le.state.ut.us/~code/TITLE46/46_03.htm
Dokument „The Illinois Act and Final Framework“:
http://www.mbc.com/ecommerce/legis/cecc-fin.html
Americká Sněmovna Reprezentantů přijala „E-Sign Bill (H.R 1714)“ v listopadu 1999.
http://www.cnnfn.com/news/technology/newsbytes/139137.html
Iniciativy Kongresu vzhledem k elektronickým podpisům, elektronickým záznamům a elektronickým smlouvám:
http://civics.com/content/99-legis.htm
Obdobně dokumenty Sněmovny Reprezentantů a Senátu:
http://thomas.loc.gov/
American Bar Association
Příručka „ABA Digital Signature Guidelines“, je použita v řadě přípravných legislativních dokumentů v USA i v zahraničí:
http://www.abanet.org
Kanada
Draft dokumentu „Bill C-54, The Personal Information and E-Document Act“, který je v současné době ve schvalovacím procesu, lze nalézt zde:
http://canada.justice.gc.ca/Commerce/index_en.html
Australie
Dokument „E-Transactions Bill, 1999“, který je základem pro navrhovaný „Isle of Man Electronic Transactions Bill“, lze nalézt na adrese:
http://law.gov.au/ecommerce

Další užitečné adresy:
http://www.bakerinfo.com/itc
http://www.bakerinfo.com/ecommerce
http://www.cybersquirrel.com

Aktivity EU v oblasti elektronických podpisů.

Direktiva EU pro elektronické podpisy

Evropská komise předložila a Evropský Parlament schválil *Direktivu pro elektronické podpisy* (30.11.1999).

Direktiva se zabývá elektronickými podpisy používanými pro autentizační účely jak z hlediska obecného přístupu, tak i z hlediska speciálního typu tzv. kvalifikovaných elektronických podpisů, které mají být právně ekvivalentní klasickým ručně psaným podpisům. Jejím cílem tedy není pokrýt všechny oblasti, ve kterých se používá autentizace, ale zaměřuje se na právní platnost elektronického podpisu, který je připojen k elektronickému dokumentu. Direktiva rovněž stanoví požadavky, které mají být splněny poskytovateli služeb, kteří podporují elektronické podpisy a další požadavky vztahující se k podepisující a ověřující straně. Tyto požadavky nutně vyžadují podporu v detailních normách a veřejných specifikacích, které rovněž splní požadavky evropských obchodních organizací.

Direktiva byla vypracována tak, aby byly dodrženy tři následující principy:

a) technologická neutralita (i když základním smyslem je orientace na technologie digitálních podpisů, je cílem direktivy zůstat neutrální a vyhovět tak i jiným technologickým principům).
b) pro poskytovatele certifikačních služeb není apriori definováno žádné schéma pro autorizaci k provádění těchto služeb, tak aby v budoucnu zde existovala principiální možnost technologických inovací.
c) rozpoznání zákonné platnosti elektronických podpisů, tak aby nemohla být popřena jejich platnost na základě toho, že jsou v elektronické podobě a byla zaručena ekvivalence s ručně napsaným podpisem.

European Electronic Signature Standardization Initiative (EESSI) jako součást Information and Communications Technologies Standards si vzala za cíl analýzu budoucích potřeb v oblasti standardizace na podporu Evropské Direktivy pro elektronický podpis. Tato odborná komise (zástupci průmyslových odborníků z jednotlivých členských zemí EU) zpracovala rozsáhlý a odborně fundovaný zásadní dokument [1], který spatřil světlo světa v červenci 1999. Jeho cílem nebylo ustavení povinných standardů a norem, které by podporovaly Direktivu, ale spíše identifikace požadavků, které by měl napomoci otevřenému trhu produktů a služeb, které splňují požadavky Direktivy.

Nejdůležitější závěry dokumentu:

1) Převzetí resp. vývoj průmyslových norem by mělo maximálně zmenšit potřebu detailizace zákonů a vyhlášek v dané oblasti
2) Normy jsou nezbytně nutné, a všude, kde je to možné, je třeba preferovat odkazy na existující mezinárodní normy před vývojem nových norem.
3) Požadavky v oblasti norem jsou dvojího druhu: kvalitativní a procedurální normy týkající se informační bezpečnosti a technické normy vzhledem k interoperabilitě produktů.
4) Podepisovací prostředky (produkty), pokud vyhovují požadavkům Direktivy, musí projít příslušným hodnocením (shoda produktu) a certifikací akreditovanou institucí pod EN 45000 (Evropské akreditační schéma).
5) Je třeba vytvořit společný referenční bod na základě definice výchozí množiny technologických komponent, který bude tvořit technický rámec pro ověřování kvalifikovaných elektronických podpisů využívajících asymetrickou kryptografii a digitální certifikáty.

6) Vzhledem k poskytovatelům certifikačních služeb je třeba použít vhodné bezpečnostní normy:
   - obecné zásady v oblasti bezpečnosti (např. BS7799 č.1 a č.2)
   - specifikace bezpečnostních požadavků vzhledem k důvěryhodným systémům, které tito poskytovatelé používají. První požadavky v této oblasti se týkají především kryptografických modulů (např. FIPS 140-1) a využití rizikové analýzy.
   - výchozí certifikační politika pro poskytovatele certifikačních služeb – je doporučováno vyjít z materiálu IETF PKIX – rfc.2527
   - obdobně pro poskytovatele služeb v oblasti časových razítek je třeba provést specifikaci požadavků vzhledem k jejich politice
7) Vzhledem k produktům sloužícím pro vytváření podpisů a jejich ověřování je třeba mít k dispozici následující příslušné normy:
   - specifikace bezpečnostních požadavků vzhledem k důvěryhodným hardwarovým zařízením, které jsou použity k jako bezpečná zařízení pro vytváření podpisů (FIPS 140-1, Common Criteria – ISO 15408)
   - specifikace pro vytváření elektronických podpisů (včetně uživatelova interface) a specifikace produktů a postupů k ověřování podpisů
8) Je nezbytná koordinace jednotlivých aktivit v oblasti norem
9) Z hlediska interoperability jsou nezbytné následující normy:
   - technické normy pro syntaxi a kódování elektronických podpisů (včetně vícenásobných podpisů). Je doporučováno vyjít z rfc.2315.
   - operativní protokoly pro řízení PKI (rfc skupiny PKIX)
   - profily kvalifikovaných certifikátů na bázi X.509

Přehled existujících norem v oblasti elektronických (digitálních) podpisů:

Kryptografické algoritmy: hashovací funkce

Následující normy se týkají hashovacích funkcí:

1) ISO/IEC 10118-1 (1994): Hash-functions – Part 1: General. ISO/IEC 10118-1 obsahuje definice a popisuje základní koncepce
2) ISO/IEC 10118-2 (1994): Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm. ISO/IEC 10118-2 popisuje dvě metody konstrukce hashovacích funkcí z blokové šifry
3) ISO/IEC 10118-3 (1997): Hash-functions – Part 3: Dedicated Hash-functions. ISO/IEC 10118-3 specifikuje následující hashovací funkce:
   - SHA-1 (FIPS 180-1)
   - RIPEMD-128
   - RIPEMD-160.
4) ISO/IEC FCD 10118-4: Hash-functions – Part 4: Hash-functions using modular arithmetic. Status: Final Committee Draft; Expected publication date: 1998 ISO/IEC 10118-4 specifikuje jak konstruovat hashovací funkci z modulárního násobení.
5) Internet RFC 1320 (PS 199?): The MD4 Message Digest Algorithm. RFC 1320 specifikuje hashovací funkci MD4. MD4 není již dnes doporučována k používání.
6) Internet RFC 1321 (I 1992): The MD5 Message Digest Algorithm. RFC 1321 (informativně) specifikuje hashovací funkci MD5.
7) FIPS Publication 180-1 (1995): Secure Hash Standard. FIPS 180-1 specifikuje Secure Hash Algorithm (SHA), který je věnován hashovací funkci vyvinuté pro použití v návaznosti na DSA. Původní SHA publikovaná v 1993 byla v roce1995 malinko upravena a přejmenována na SHA-1.

8) ANS X9.30-2 (1997): Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry – Part 2: The Secure Hash Algorithm (SHA-1). X9.30-2 specifikuje ANSI verzi SHA-1.
9) ANS X9.31-2 (draft): Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry – Part 2: Hash Algorithms.

Kryptografické algoritmy: Algoritmy pro digitální podpis

Následující normy se týkají mechanizmů pro digitální podpis:

1) FIPS Publication 186 (1994): Digital Signature Standard. NIST's *Digital Signature Algorithm* (DSA) varianta ElGamalova mechanizmu pro digitální podpis na bázi diskrétního logaritmu. DSA pracuje s 160-bitovou hashovací funkcí (SHA-1).
2) IEEE P1363 - Standard Specifications for Public-Key Cryptography. Status: Draft, Očekávaný rok zveřejnění: 2000. Současný draft obsahuje mechanizmy pro digitální podpis, ustavení klíčů a šifrování na bázi tří rodin schemat s veřejným klíčem:
   - "Klasické" techniky na bázi diskrétního logaritmu (DL) , mj. Diffie-Hellmanovu (DH) dohodu na klíči, Menezes-Qu-Vanstone (MQV) dohodu na klíči , *Digital Signature Algorithm* (DSA), a Nyberg-Rueppelův (NR) digitální podpis.
   - Analogické techniky na bázi eliptického diskrétného logaritmu (EC), tj. EC-DH, EC-MQV, EC-DSA, a EC-NR. Implementace eliptických křivek zahrnují varianty mod p (p je prvočíslo) a varianty v tělesech charakteristiky 2 (reprezentace polynomiální resp. reprezentace pomocí normálních bází).
   - Techniky na bázi složitosti úlohy celočíselné faktorizace (IF – integer factoring), které zahrnují RSA šifrování, RSA digitální podpis, a na RSA založený přenos klíčů.
3) ISO/IEC 9796 (1991): Digital signature scheme giving message recovery. ISO/IEC 9796 specifikuje mechanizmus digitálního podpisu na bázi RSA.
4) ISO/IEC 9796-2 (1997): Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash-function. ISO/IEC 9796-2 specifikuje mechanizmus digitálního podpisu na bázi RSA s využitím hashovací funkce.
5) ISO/IEC CD 9796-4: Digital signature schemes giving message recovery – Part 4: Discrete logarithm based mechanisms. Status: Draft; Očekávaný rok zveřejnění: 2000. ISO/IEC 9796-4 specifikuje mechanizmus digitálního podpisu s částečným rozkrytím zprávy, který je založen na technikách diskrétního logaritmu.Tento draft v sobě obsahuje také schéma Nyberg-Rueppela.
6) ISO/IEC FCD 14888-1: Digital signatures with appendix – Part 1: General. Status: Draft; Očekávaný rok zveřejnění: 2000. ISO/IEC 14888-1 obsahuje definice a popisuje základní koncepty digitálního podpisu s přívěškem.
7) ISO/IEC FCD 14888-2: Digital signatures with appendix –
   Part 2: Identity-based mechanisms. Status: Final Committee Draft; Expected publication date: 1999. ISO/IEC 14888-2 specifikuje mechanizmy digitálního podpisu s přívěškem využívající identifikační klíčový materiál.tento draft obsahuje techniky zero-knowledge (Fiat-Shamir a Guillou-Quisquater).
8) ISO/IEC FCD 14888-3: Digital signatures with appendix –
   Part 3: Certificate-based mechanisms. Status: Final Committee Draft; Expected publication date: 1999. ISO/IEC 14888-3 specifikuje mechanizmy digitálního podpisu s přívěškem využívající klíčový materiál odvozený z certifikátů. Tento draft obsahuje následujících pět schémat:
   - DSA,
   - EC-DSA, eliptický analog NIST DSA (Digital Signature Algorithm),
   - Pointcheval-Vaudeney podpis,

- RSA podpisy,
- ESIGN.

9) ISO/IEC WD 15946-2: Cryptographic techniques based on elliptic curves - Part 2: Digital signatures. Status: Working Draft; Expected publication date: 2000. ISO/IEC 15946-3 specifies digital signature schemes with appendix using elliptic curves. The current draft includes two schemes:
   - EC-DSA, an elliptic curve based analog of NIST's Digital Signature Algorithm,
   - EC-AMV, an elliptic curve based analog of the Agnew-Muller-Vanstone signature algorithm.
10) ANS X9.31-1 (draft): Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry – Part 1: The RSA Signature Algorithm. ANSI X9.31-1 specifies a digital signature mechanism with appendix using the RSA public-key technique.
11) ANS X9.30-1 (1997): Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry – Part 1: The Digital Signature Algorithm (DSA). ANSI X9.30-1 specifies the DSA, NIST's *Digital Signature Algorithm*.
12) ANS X9.62 (draft): Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA). The ANSI X9.62 draft standard specifies the *Elliptic Curve Digital Signature Algorithm*, an analog of NIST's *Digital Signature Algorithm* (DSA) using elliptic curves. The appendices provide tutorial information on the underlying mathematics for elliptic curve cryptography and many examples.

Podpora infrastruktury TSP

V této oblasti existují následující práce:

1) ISO/IEC 14516 (WD): Guidelines on the use and management of Trusted Third Party services. Status: Draft; Očekávaní datum zveřejnění: 2000. ISO/IEC 14516 obsahuje příručku k používání a řízení služeb Důvěryhodné Třetí Strany (TTP-Trusted Third Party).
2) ISO/IEC 15945 (WD): Specification of TTP services to support the application of digital signatures. Status: Draft; Očekávaní datum zveřejnění: 2000. ISO/IEC 15945 specifikuje služby TTP, které se týkají podpory digitálních podpisů.
3) ANS X9.31-3 (draft): Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry – Part 3: Certificate Management for RSA.
4) ANS X9.30-3 (draft): Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry – Part 3: Certificate Management for DSA.
5) ANS X9.57 (1997): Public Key Cryptography for the Financial Services Industry – Certificate Management. Tato norma specifikuje obsah certifikátů veřejných klíčů a techniky pro generování, verifikaci a odvolání certifikátů (zejména certifikáty pro DSA a tzv. "attribute certificates").
6) ANS X9.55 (1997): Public Key Cryptography for the Financial Services Industry – Extensions to Public Key Certificates and Certificate Revocation Lists. Ve spojení s X9.57, X9.55 rozšiřuje a zabezpečuje větší flexibilitu pro použití certifikátů využitím dalších polí obsahujících dodatečné informace o veřejných klíčích, alternativních jménech certifikovaného subjektu a omezující specifikace (např. zamýšlené použití).

Poznámka 1.: Přehled těchto vybraných norem je zde dán zejména proto, aby ukázal, jaký typ norem je třeba převzít do české normativní sféry, čeho se tyto normy týkají a jak široké je jejich spektrum.
Poznámka 2.: Důležitost těchto norem nespočívá např. jenom v možnostech vybrat si z nich ty, které budu třeba jako jejich konkrétní uživatel potřebovat (např. pro využití ve vlastní práci), ale také je třeba si uvědomit, že se s realizacemi těchto norem budeme setkávat při komunikacích s ostatními evropskými partnery. A např. byla by rozhodně škoda, kdybychom potom (třeba v rámci elektronického obchodu) zjistili, že danou transakci nemohu uskutečnit, vzhledem k tomu, že české normy neumožňují spolupráci např.na bázi eliptických křivek a potenciální partner používá právě ty normy, které daná schémata popisují.

Závěr

Cílem materiálu je seznámit širší veřejnost se současnými aspekty problematiky digitálních podpisů v návaznosti na legislativní dokumenty (zejména EU). Jádro odpovídajícího řešení v rámci České republiky vidí autor v následujících bodech:

1. Je třeba postupovat v návaznosti na příslušné dokumenty EU (direktiva EU k elektronickým podpisům, závěrečná zpráva EESSI) a v součinnosti s evropskými odborníky v dané oblasti (včetně např. časových aspektů – Direktiva EU má být uvedena do legislativní praxe jednotlivých členských zemí do 30.6.2001).
2. Těžiště řešení spočívá kromě oblasti legislativní především v oblasti normativní. Je nezbytné kvalifikovaně vytvořit postup k převedení celé řady mezinárodních norem na normy platící i pro Českou republiku (a to včetně návazných norem týkajících se např. certifikace prostředků pro podepisování a ověřování podpisu – dle FIPS 140-1 nebo analogických dokumentů, atd.).
3. S tím souvisí i funkční činnost vhodného akreditačního orgánu. Je nezbytné, aby konkrétní prostředky určené k vytváření a ověřování digitálních podpisů prošly příslušnou validací.

Literatura:

[1] Final Report of the EESSI Expert Team 20th July 1999, http://www.ict.etsi.org/eessi/Final-Report.doc
[2] http://europa.eu.int/comm/dg15/en/media/sign/index.htm Direktiva EU
[3] http://www.ict.etsi.org/eessi/EESSI-homepage.htm evropské dokumenty
[4] http://www.spis.cz/ZEP/zep.htm návrh zákona o el.podpisu (SPIS)
[5] http://www.usiscr.cz/cz/archiv/dokumenty/diskuse/dig_podpis.html návrh zákona o el.podpisu (USIS – stará verze)
[6] http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm přehled existujících legislativních iniciativ v oblasti digitálních (a elektronických) podpisů v celém světě.
[7] Jaroslav Pinkava: Úvod do kryptologie, květen 1998, http://www.aec.cz