Evropská Unie a elektronický podpis. Legislativa a normy.

Ing. Jaroslav Pinkava, CSc.,

AEC spol. s r.o. & Norman Data Defense Systems

jaroslav.pinkava@normancz.cz

Klíčová slova:

Elektronický podpis, Směrnice EU, kvalifikované certifikáty, časové značky, bezpečný podpisový prostředek, poskytovatelé certifikačních služeb, ETSI, CEN/ISSS

Anotace:

V návaznosti na Směrnici Evropské Unie o elektronickém podpisu probíhá v jednotlivých členských zemích příprava národních legislativ. Období těchto legislativních příprav bude uzavřeno v polovině roku 2001 (nové zákony, vyhlášky, atd...). Některé návrhy zákonů jednotlivých zemí zpracované dle požadavků Směrnice EU jsou již k dispozici. Souběžně s tím připravují dvě instituce Evropské unie (ETSI a CEN ISSS) základní normy pro činnost poskytovatelů certifikačních služeb. Týkají se např. časových značek, formátů elektronických podpisů v návaznosti na tyto časové značky, profilů kvalifikovaných certifikátů, politik poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty, důvěryhodné systémy používané takovýmito poskytovateli, požadavků na bezpečný podpisový prostředek, atd. Cílem přednášky bude seznámit posluchače s těmito současnými evropskými trendy.

Úvod:

Aktuálnost problematiky elektronického podpisu není třeba zvláště zdůrazňovat. Vytváření prostředí, ve kterém by tento důležitý nástroj elektronického obchodu, e-governmentu mohl smysluplně, bezpečně a dostatečně efektivně fungovat není jednoduchou záležitostí. Kromě momentů ryze technologických a organizačních zde nastupují i otázky právního charakteru vztahující se k právnímu uznávání a závaznosti vytvářených elektronických podpisů. Potřeba unifikovaného přístupu v dané oblasti i z mezinárodního hlediska je dána objektivními skutečnostmi. Elektronické podpisy snadno překračují hranice a je tudíž nezbytné, aby se jejich praxe opírala o prostředky takto široce rozpoznatelné a uznávané. To je základním východiskem při formování současných trendů v legislativní a normativní oblasti. Evropská Unie v této

oblasti stojí v čele těchto světových aktuálních trendů a prosazuje velice moderní ucelenou a obsahově rozmanitou koncepci praxe elektronických podpisů.

V rámci předložené stati bude poukázáno na odpovídající základní dokumenty EU k problematice elektronických podpisů a to jak v oblasti legislativní, tak především v oblasti zpracovaných resp. připravovaných evropských norem pro tuto problematiku.

Závěrečná zpráva EESSI a Směrnice EU o elektronickém podpisu

Výchozím dokumentem zpracovaným EU pro problematiku elektronických podpisů je Závěrečná zpáva EESSI (lit. [1]). Tento dokument byl zpracován skupinou odborníků z různých zemí EU a byl zveřejněn (v definitivní podobě) v červenci 1999.

V návaznosti na tuto závěrečnou zprávu byla Evropskou komisí předložena a Evropským parlamentem přijata (30.11.1999) Směrnice Evropské Unie pro elektronické podpisy [2].

Toto jsou dva základní dokumenty, ze kterých potom vychází další postupy. První z nich komplexně vytyčuje celkovou strategii Evropské Unie při řešení problematiky elektronických podpisů. Ukazuje nezbytné směry v legislativě, v normotvorné činnosti (především) resp. se dotýká i dalších nezbytných aktivit. Jeho základní závěry jsou formulovány následovně:

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 - evaluace) 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, dnes ISO-17799),

- 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 k vytváření podpisů a jejich ověřování je třeba mít k dispozici následující příslušné normy:

- specifikace bezpečnostních požadavků vzhledem k důvěryhodným hardwarovým zařízením, která jsou použita 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.

Směrnice Evropské Unie pro elektronický podpis byla vyvíjena několik let – existovala v podobě draftu, který byl velice široce diskutován. Nakonec ji 30.11.1999 schválil Evropský parlament. Přitom členské země EU jsou povinovány uvést své zákony, vyhlášky a administrativní postupy v platnost do souladu s touto Směrnicí do 19. července 2001. Směrnice byla formulována tak, aby byly naplněny následující tři základní principy:

I. *Technologická neutralita*

II. Vydávání oprávnění pro poskytovatele certtifikačních služeb není direktivně omezeno žádným schématem

III. Nezbytnost rozpoznání zákonné platnosti elektronických podpisů

Podrobnější diskusi jednotlivých bodů Směrnice EU lze nalézt např. v [5].

Normy pro oblast elektronických podpisů připravované v EU

Na základě strategie zformulované v Závěrečná zprávě EESSI se rozeběhly práce pro přípravu norem pro oblast elektronických podpisů. Tyto práce probíhají ve dvou nezávislých pracovních skupinách: ETSI a CEN/ISSS.

Dokumenty skupiny ETSI

(ETSI Electronic Signatures and Infrastructures - EESSI Program)

V první fázi prací byl zpracován dokument určující osnovu dalších prací Electronic Signature Report (http://docbox.etsi.org/tech-org/security/open/el-sign/ESRep042.pdf) . Druhá fáze prací započala na počátku roku 2000 a zahrnuje (dokument Workplan) následující okruhy problémů:

a) problematika časových značek je řesena v rámci těchto okruhů:

Electronic Signature Formats.

Time Stamping Profile;

b) problematika kvalifikovaných certifikátů je řesena v rámci těchto okruhů:

Qualified Certificates Profile;

Policy Requirements for CSPs Issuing Qualified Certificates;

První ze série norem „ETSI standard ES 201 733 (**Electronic Signature Formats**)" byla původně schválena již v květnu 2000. V současné době byla zpracována rozšířená verze tohoto dokumentu, která nese označení TS 101 733, tato verze byla schválena ETSI SEC v listopadu 2000 a opublikována následně v prosinci 2000. Obsahuje zejména definice různých formátů elektronických podpisů v návaznosti na používání časových značek (podrobněji např. v článku [9]).

Samotnému procesu vytváření časových značek je věnována norma **Time Stamping Profile**, která se opírá především o dokument Internet X.509 Public Key Infrastructure Time Stamp Protocols (v současné době je nejnovější draft-ietf-pkix-time-stamp-13.txt). Dokument byl již také schválen, dostal označení TS 101 861 a bude opublikován jakmile se příslušný draft stane dokumentem RFC.

V normě **Qualified Certificates Profile** jsou na podobu kvalifikovaného certifikátu kladeny některé základní doplňkové nároky. Např. v poli, kde je označen vydavatel certifikátu musí být obsaženo i jméno vydávající země (vpříslušném atributu). V profilu musí být obsaženy následující údaje:

- formulace, že certifikát je vydán jako kvalifikovaný certifikát;
- formulace omezující hodnotu transakce, pro kterou lze certifikát využít;
- formulace ukazující časový interval, po který je archivována informace poskytnutá uživatelem při registraci.

Dokument byl již schválen, dostal označení TS 101 862 a byl opublikován v prosinci 2000.

Posledním z těchto dokumentů je norma zabývající se požadavky na politiku poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty - **Policy Requirements for CSPs Issuing Qualified Certificates.** Toto je samostatný dokument upřesňující požadavky na CP (certifikační politiku) a CPS (certifikační prováděcí směrnici) poskytovatelů certifikačních služeb - životnost klíčů, certifikátů, management certifikátů, bezpečnostní aspekty, atd. Svojí filosofií vychází dokument z RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Tento dokument je pro praxi poskytovatelů certifikačních služeb stěžejní. Hlavní rozdíly pro praxi poskytovatelů certifikačních služeb spočívají totiž především v oblasti kvality práce CA a toto formulují právě dokumenty CP A CPS. Také česká vyhláška formulující požadavky pro činnost poskytovatelů, kteří chtějí vydávat kvalifikovaní certifikáty, z dokumentu Policy Requirements for CSPs Issuing Qualified Certificates vychází jako z jednoho z hlavních materiálů. Dokument byl již schválen, dostal označení TS 101 456 a byl opublikován v prosinci 2000. S aktuálním stavem se lze seznámit v [3].

Třetí fáze prací skupiny ETSI bude probíhat v roce 2001. ETSI oznámila, že v roce 2001 chystá vydání zhruba pěti nových dokumentů. K jejich obsahu jsou v současné době známy pouze následující informace.

Policy requirements for CSPs issuing trusted time stamps

Dokument bude vycházet z požadavků na politiku, které již byly v dokumentech ETSI zpracovány. Na službě časových značek je velice zainteresována komerční sféra a stávají se důležitou složkou problematiky elektronických podpisů (dokumentES 201733). Zde zformulovaná minima pro požadavky v oblasti bezpečnosti a kvality jsou nezbytná k zabezpečení důvěryhodného ověření dlouhodobých (long-term) elektronických podpisů.

Policy requirements for CSPs, according to Art. 5.2 of the Directive

Obsahem tohoto materiálu budou otázky řízení bezpečnosti a certifikační politika těch poskytovatelů certifikačních služeb, kteří fungují na bázi principů odlišných od principů pro poskytovatele certifikačních služeb (PCS), kteří vydávají kvalifikované certifikáty. Potřeba existence těchto PCS vyplývá z potřeb trhu (transakce elektronického obchodu střední úrovně – jako například mobilní elektronický obchod). Na základě analýzy provedené STF pro alternativní třídy certifikátů (dle článku 5.2 Směrnice EU o elektronických podpisech) budou stanoveny příslušné specifikace, které se mimo jiné budou odkazovat např. na dokument RFC 2527 a doplní zde potřebné specifické detaily.

XML electronic signatures

Norma se bude zabývat syntaxí a formáty kódování elektronických podpisů v XML na základě dokumentu ES 201733. První studie pro verzi XML je připravována v rámci STF 155 (Specialist Task Force). Současný formát XML podpisů dle W3C bude použit k převzetí formátů vyšších úrovní elektronických podpisů dle ETSI do světa XML. Tato aktivita vznikla v návaznosti na mezinárodní aktivity v dané oblasti, zejména W3C/IETF a práce v EDI. Hlavním důvodem pro toto spojení je uvedení specifikací XML na mezinárodní scénu.

Technical aspects of signature policies

Koncepce podpisové politiky je zde zvažována ve vztahu k ustavení společné základny elektronických podpisů. Dokument ETSI ES 201 733 již sice obsahuje určité specifické nástroje pro definice podpisových politik, avšak neobsahuje všechny takovéto aspekty (např. vícenásobné podpisy). Dokument bude navržen jako experimentální RFC pro IETF a posléze připraven jako norma.

Infrastructure and interoperability requirements for on-line validation of Certification Service Providers

Cílem těchto prací je stanovit doporučení pro podporu akcí spoléhajíci se strany ve směru ověření, že vydavatel došlého certifikátu je v dané době důvěryhodnou stranou transakce. Na základě existujících dokumentů EESSI lze zajistit, že strana spoléhající se na certifikát (například příjemce podepsané smlouvy či objednávky) získá dostatek informací potřebných pro kontrolu platnosti certifikátu. Existují tedy normy podporující takovouto kontrolu. Avšak podstatně obtížnější je ověřit, zda vydávající CSP je v době transakce v pořádku (např. CSP mohla ukončit svoji činnost nebo neprošla posledním auditem atd.). Tento typ informací je dodáván třetí stranou nezávislou jak na straně, která transakci podepsala, tak i na straně vydavatele certifikátu. Důležitost této informace je stěžejní zejména v transakcích překračujících hranice domén a států.

Existující národní schémata pro tuto problematiku nejsou harmonizována, totéž se týká odpovídajících protokolů a formátů dat. Dokument zohlední jak technické tak i akreditační aspekty problematiky a jeho cílem bude identifikace potřebných procedurálních a technických vlastností.

Dokumenty skupiny CEN ESSI

V současné době jsou prováděny práce na zpracování následujících pěti dokumentů:

Security Requirements For Trustworthy Systems and Products
Security Requirements for Signature Creation Devices
Signature Creation Environment
Signature Verification Process nad Environment
Conformity Assessment of Products and Services for Electronic Signatures

Aktuální informace lze nalézt v [4]. Zde došlo na posledním jednání (E-SIGn Workshop, 20-21.11.2000) k posuvu obsahu jednotlivých dokumentů, odsud pramení i změna jejich názvů.

První z dokumentů: původní název zněl **Security Requirements for Trustworthy Systems and Products** - se zabývá bezpečnostními požadavky na důvěryhodné systémy poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty. Jedním ze závěrů projednaných v listopadu je rozhodnutí, že bude zpracován nový dokument - pracovní název „*Security Requirements for Cryptograhic Modules Suitable for trustworthy Systems*". První draft měl být k dispozici v lednu 2001 a v březnu 2001 má být tento materiál projednán. Bylo zde konstatováno, že je problém odkazovat se v Evropě na dokument (FIPS 140-1), který není uznáván jako evropská norma. Současně s tím vzniká i problém evaluace produktu dle dokumentu FIPS. Z hlediska obsahu FIPS 140-1 je otázkou nakolik lze požadavky v něm formulované vztáhnout i na specifika certifikačních autorit. Nový dokument bude vycházet z formátu a obsahu ISO 15408 (Barcelona, říjen 2000) a měl by tvořit celosvětový základ pro evaluace. Byly stanoveny oblasti, kterých se bude chystaný dokument týkat. Přestože tak bylo původně ohlášeno (N115), v pořadu únorového jednání (a ani v rámci zveřejněných dokumentů) se zatím neobjevila žádná informace ohledně chystaného draftu „*Security Requirements for Cryptograhic Modules Suitable for trustworthy Systems*" Draft však existuje, ale zatím nebyl zveřejněn – nelze se tedy vyjádřit k jeho konkrétnímu obsahu.

Po rozdělení problematiky v této oblasti se v lednu objevila také nová verze základního dokumentu (**Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures, N129).** Oproti předešlým verzím (kromě zapracování některých připomínek) byly odstraněny původní přílohy A. a B, jejichž obsah se stane zřejmě základem chystaného nového dokumentu – výše zmíněného *Security Requirements for Cryptograhic Modules Suitable for trustworthy Systems.*

Velice důležitou je norma **Security Requirements for Signature Creation Devices**, tj. norma stanovující požadavky na bezpečný podpisový nástroj (v duchu terminologie Směrnice EU o

elektronickém podpisu a i našeho zákona o elektronickém podpisu). Momentálně existují dvě verze tohoto dokumentu – EAL 4 a EAL4+, které se tudíž (jak ukazuje název verze) liší v nárocích na bezpečné podpisové zařízení. Názvy těchto dvou verzí jsou:

Secure Signatur-Creation Devices, version 'EAL 4', 2001-02-01 (N131);

Secure Signatur-Creation Devices, version 'EAL 4+', 2001-02-01 (N132).

Při jednání k tomuto dokumentu došlo totiž k rozporným stanoviskům při formulaci požadavku vzhledem k zranitelnosti evaluovaného podpisového prostředku. Podle EAL 4 (Common Criteria) stačí požadovat, aby objekt evaluace byl rezistentní vůči útokům narušitele „s nízkou schopností útočit". Oproti tomu zpracovatelé dokumentu přišli s návrhem, aby zde byla použit požadavek, aby objekt evaluace byl rezistentní vůči útokům narušitele „s vysokou schopností útočit". Na jednání nedošlo k dohodě a nakonec bylo rozhodnuto, že vedení EESSI má přijít před Evropskou komisi paralelně s oběma návrhy.

Problematika **Signature Creation Environment** - zde je k dispozici zatím pouze materiál „*Security Requirements for Signature Creation Systems*" (říjen 2000) a shrnuty komentáře k tomuto materiálu, nová verze zatím není k dispozici.

V dokumentu je mimo jiné řečeno: Systém na vytváření podpisů (SCS) bude obsahovat specifické komponenty ve vztahu k důvěryhodnému prostředí a k vlastním aplikacím. Důvěryhodnými komponentami (a současně závaznými) jsou tyto komponenty:

· **SDV** - (Signer´s Document Viewer) používano pro prohlížení podepsaných dokumentů;

· **SAV** - (Signature Attributes Viewer) používano pro prohlížení atributů podpisu;

· **SIC** - (Signer Interaction Component) pomocí této komponenty probíhá interakce podpisující strany s SCS, tak, aby bylo vytváření podpisu pod kontrolou uživatele;

· **SAC** - (Signer´s Authentication Component) - to je např. čipová karta s PINem, která je používána k autentizaci podepisující strany na základě autentizujících dat anebo biometrických vlastností takovou cestou, že výsledek lze porovnat s hodnotou uloženou v SSCD.

· **DHC** - (Data Hashing Component) – připravi pro vstupní data příslušný otisk;

· **SSC** - (SSCD/SCS Communicator) řídí interakce mezi SCS a SSCD;

· **SSA** - (SSCD/SCS Authenticator) ustavuje důvěryhodnou cestu mezi SSCD a SCS.

Poznámka : SSCD = Secure Signature Creation Device.

Aplikačními specifickými komponentami jsou:

· **SDC** - (Signer's Document Composer) - např. textový editor, sloužící pro vytváření, výběr dokumentu podepisující osoby a jejích atributů.

· **CCV** - (Certificate Content Viewer) - ten dokáže zobrazit úplný obsah certifikátu podepisující osoby.

· **SDOC** - (Signed Data Object Composer) - přetváří složky podepisovaného objektu do bitového řetězcea jeho výstupem je určitý normalizovaný formát (ETSI Electronic Signature Formats Document);

· **CSPC** - (Certification Service Provider Interaction Component) používán pro získání certifikátu podepisující strany či získání časové značky;
· **SHI** - (SSCD Holder Indicator) zobrazuje jméno majitele SSCD.

Požadavky na ověřování elektronického podpisu stanoví problematika **Signature Verification Process nad Environment**. Jsou zde analyzovány různé aspekty verifikačního procesu (časové značky, kvalifikované certifikáty), popis jednotlivých komponent verifikačního systému, příklady různých prostředí a zformulovány požadavky na systém verifikující podpisy z řady hledisek (právní aspekty, atd.). Jsou zde také analýzovány otázky vícenásobných podpisů a otázky dlouhodobé archivace podpisů. Také tato problematika byla v současné době rozdělena do dvou dokumentů:

Security Requirements for Signature Creation Systems; Version 3.0, 2000-10-08 (N91);

Procedures for Electronic Signature Verification; V 1.0.3, 2001-01-25 (N129).

Druhý dokument popisuje různé stránky verifikačního procesu. Draft nahrazuje starší verzi N102. Struktura dokumentu zůstala shodná, bylo reflektováno na některé připomínky (N113, N127).

Poslední materiál **Conformity Assessment Products and Services for Electronic Signature** je věnován otázkám harmonizace implementací norem pro elektronické podpisy – slouží zejména jako příručka certifikujícím a testujícícm laboratořím.

Týká se čtyř základních oblastí:

A.: služeb CA a procesů navazujících na řízení PKI, informační bezpečnosti, organizační spolehlivosti ve vztahu ke kvalifikovaným certifikátům;

B.: systémů pro vytváření elektronických podpisů ;

C.: procedur pro verifikaci podpisu;

D.: bezpečných podpisových prostředků.

Poslední diskutovaný dokument k této problematice je **EESSI Conformity Assessment Guidance; Version 2.0; 2001-01-22 (N130).** Draft nahrazuje starší verzi N120. Oproti předešlé verzi došlo pouze k některým dílčím úpravám.

Zatím ještě neexistují definitivní verze těchto dokumentů.

Shrnutí:

V současné době (únor 2001) je většina členských zemí EU v etapě legislativních příprav pro problematiku elektronického podpisu. Např. v Německu byl parlamentem schválen nový zákon formulující rámcové podmínky pro elektronický podpis 15. 2. 2001, v Rakousku byla projednána novela zákona (v návaznosti na podmínky Směrnice EU). V obou zemích se pracuje na vyhláškách k tomuto zákonu. Také v dalších zemích probíhají analogické práce. Formulace Směrnice stanoví sice podmínku

pro členské země EU uvést svoje zákonodárství do souladu s touto Směrnicí do poloviny roku 2001, avšak sama předpokládá určité postupné fáze celého procesu uvedení problematiky elektronického podpisu do praxe jednotlivých zemí EU. V roce 2003 (nejpozději do 19.7) má být Evropskou komisí provedena analýza funkčnosti Směrnice a podány návrhy na její potenciální úpravy. Příslušná zpráva bude dle potřeby obsahovat i patřičná legislativní doporučení.

V České republice byl přijat Zákon o elektronickém podpisu v létě roku 2000. Jeho formulace v zásadě vychází ze Směrnice EU i když jsou zde určité dílčí odlišnosti (problémy dnes činí formulace paragrafu 11 a výklad tohoto paragrafu). V současné době probíhají také intenzivní práce na přípravě vyhlášky k tomuto zákonu [7].

Literatura:

[1] Final Report ICTSB European Electronic Signature Standardization
http://www.ict.etsi.org/eessi/Final-Report.pdf

[2] Směrnice EU o elektronickém podpisu – Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures
http://www.ict.etsi.org/eessi/e-sign-directive.pdf

[3] webovské stránky ETSI : http://www.etsi.org/sec/el-sign.htm.

[4] webovské stránky CEN/ISSS: http://www.cenorm.be/isss/workshop/e-sign/
http://www.ni.din.de/index.php3

[5] J. Pinkava : Elektronický podpis a EU, DSM 2/2000

[6] Český zákon č. 227/2000 Sb. o elektronickém podpisu.

[7] Návrh české vyhlášky k ZoEP (ÚOOU), http://www.epodpis.cz

[8] Crypto-World (vychází 1x mesíčně v elektronické podobě), http://www.mujweb.cz/veda/gcucmp

[9] J. Pinkava: Moderní kryptografické algoritmy pro elektronický podpis, Seminář ČAČK, březen 2000