Certifikační autorita a uživatel. Bezpečné prostředí.

Ing. Jaroslav Pinkava, CSc.

AEC spol. s r.o. & Norman Data Defense System CZ

Úvod

Při zavádění problematiky elektronických podpisů do praxe ve vztahu k poskytovatelům certifikačních služeb (certifikačním autoritám) vydávajícím tzv. kvalifikované certifikáty vyvstává celá řada otázek, které je třeba vyřešit při přípravě praktických řešení. To souvisí především s uváděním do života požadavků Směrnice Evropské Unie o elektronickém podpisu (a tedy i požadavků českého zákona o elektronickém podpisu). Předložený přehledový článek si klade za cíl seznámit veřejnost zejména se stavem prací v oblasti norem pro elektronický podpis, které jsou připravovány v rámci Evropské Unie. Přitom ohnisko pozornosti je zaměřeno do oblasti norem, které zpracovává pracovní skupina CEN/ISSS a které se týkají v návaznosti na problematiku elektronického podpisu především bezpečnostních okruhů otázek jako jsou bezpečné prostředky pro vytváření elektronických podpisů, důvěryhodné prostředí, problematika evaluace atd.

Bezpečné prostředí

Pro reálné implementace elektronických podpisů je nezbytné se zabývat souvisejícími otázkami bezpečnostního charakteru. Týká se to jednotlivých uživatelů, kde to souvisí jednak s *bezpečným uložením* soukromého klíče uživatel, ale také s jeho *bezpečným použitím*. Ale týká se to i poskytovatelů certifikačních služeb (PCS) , které vydávají odpovídající digitální certifikáty. Také zde bezpečnostní otázky souvisí s bezpečným uložením a použitím soukromého klíče PCS. Přitom otázka bezpečnosti stojí pro CA podstatně vyhraněněji. Pokud dojde ke kompromitaci soukromého klíče jednoho konkrétního uživatel, může na to doplatit v zásadě právě pouze tento uživatel. Pokud však dojde ke kompromitaci soukromého klíče CA, může být tímto klíčem podepsáno nepřehledné množství nových digitálních certifikátů, odvolány jiné, dosud platné certifikáty a škody takto způsobené mohou být značné.

Legislativa a normy EU jsou připravovány především pro využití v rámci gesce PCS, kteří vydávají kvalifikované certifikáty. Obsahem příslušných dokumentů jsou samozřejmě i bezpečnostní aspekty problematiky elektronických podpisů.

Normy Evropské Unie

Na základě pověření EESSI (European Electronic Signature Standardization) dvě instituce Evropské unie (ETSI a CEN ISSS) připravují 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.

Dokumenty zpracované ETSI v roce 2000 se týkají dvou základních oblastí, problematiky časových značek a problematiky kvalifikovaných certifikátů:

a) problematika časových značek je řešena 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;

Další 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 úvodní vstupní informace (viz [5], [7]) – mají se týkat některých dalších oblastí, jako jsou např. podmínky na činnost poskytovatele certifikačních služeb, který funguje ve smyslu znění odstavce 5.2 Směrnice EU (tím je v zásadě míněna činnost CA pro elektronický obchod). Dále jsou to požadavky na politiku PCS, který vydává časové značky; syntaxe a formáty XML podpisů; podpisové politiky a on-line validace PCS.

Normy skupiny CEN/ISSS

V současné době již běží práce na zpracování následujících pěti okruhů:

D: Security Requirements For Trustworthy Systems and Products (N142)

F: Security Requirements for Signature Creation Devices (N136, N137)

G1: Signature Creation Environment (N141)

G2: Signature Verification Process nad Environment (N140)

V: Conformity Assessment of Products and Services for Electronic Signatures (N143, N144)

(v závorkách jsou uvedena čísla posledních draftů, které lze získat na adrese: http://www.ni.din.de/index.php3). Vznikající dokumenty mají statut CWA (CEN Workshop Agreement).
Následující dva okruhy problematik byly v současné době otevřeny a příslušné dokumenty budou zpracovány ještě během letošního roku.

AA: Extension of SSCD requirements towards specific applications/environments and towards e-commerce applications – Art.5.2

K: Requirements for smart cards used as SSCD

Následuje stručný obsahový přehled jednotlivých okruhů problematik.

Skupina D: Bezpečnostní požadavky na důvěryhodné systémy a produkty

V nedávné době došlo k rozdělení prací této skupiny na dva směry. Souvisí to s tím, že jako oddělenou se ukázalo řešit problematiku vyhodnocování shody (evaluace) kryptografických prostředků – to je obsahem práce nově vzniklé skupiny D2.

Skupina D1: Bezpečnostní požadavky na důvěryhodné systémy a produkty

(Security requirements for trustworthy systems and products)

Dokument je určen pro práci poskytovatelů certifikačních služeb, opírá se o požadavky vznesené v příloze II Směnice EU. V odstavci f. se zde říká:
PCS musí používat důvěryhodné systémy a výrobky, které jsou chráněny proti pozměňování a a zajistit technickou a kryptografickou bezpečnost postupů, které tyto systémy a výrobky podporují;
Dle článku 3.3 Směrnice zveřejní komise odkazy na příslušné normy. Dokument specifikuje bezpečnostní požadavky na výrobky a technologické komponenty, které používají PCS při vytváření kvalifikovaných certifikátů pro zaručené podpisy (dle ETS STF 115TI).
Dokument formuluje obecné bezpečností požadavky a předpoklady, detaily ponechává na konkrétních implementacích.. Předpokládá se rovněž, že bude provedeno vyhodnocení shody jako nezbytná součást pro demostranci toho, že jsou dodrženy tyto požadavky.

Skupina D2: Bezpečnostní požadavky na důvěryhodné systémy a produkty

(Security requirements for trustworthy systems and products)

Materiál vzniklý v rámci této skupiny bude definovat požadavky na kryptografické moduly použitelné v důvěryhodných systémech (pro PCS vydávající kvalifikované certifikáty), bude napsán dle formátu ochranných profilů, který je definován v ISO 15408. 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.Takovýto formát a obsah vytvoří celosvětovou bázi pro možná vyhodnocování shody (evaluaci) výrobků, i když takováto formální evaluace není dle Evropské směrnice povinná. Připravovaný dokument ponese název *Security requirements for a cryptographic module usable in trustworthy systems* a měl by být zpracován do června 2001.

Skupina F: Bezpečnostní požadavky na zařízení pro vytváření podpisů

(Security requirements for secure signature creation devices)

Materiál vychází z požadavků přílohy III Směrnice EU. A jeho cíl je příprava normy pro bezpečná zařízení pro vytváření elektronických podpisů. 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. Verze ALE 4+ obsahuje oproti EAL 4 dva doplňující požadavky.

Skupina G1. Bezpečnostní požadavky na systémy pro vytváření podpisů

(Area G1 - Security Requirements for Signature Creation Systems)

Dokument formuluje bezpečnostní požadavky na systém pro vytváření podpisu (SCS – Secure Creation System), který vytváří zaručené elektronické podpisy pomocí bezpečného zařízení na vytváření podpisů a dat pro vytváření podpisu podepisující strany na základě kvalifikovaného certifikátu následujícími prostředky:

- model prostředí pro vytváření podpisu a funkční model systému pro vytváření podpisu
- celkové požadavky aplikované na všechny funkce identifikované ve funkčním modelu
- bezpečnostní požadavky pro každou z funkcí identifikovanou v systému pro vytváření podpisu včetně bezpečného zařízení pro vytváření podpisu

Dalším cílem je vytvoření takových specifikací, aby použití elektronického podpisu bylo stejně snadné a bezchybné jako užití vlastnoručního podpisu. Mělo by být možné pro všechny lidi, včetně těch, kteří mají speciální požadavky vzhledem k elektronickým podpisům. Dosažení těchto cílů má vést k větší důvěře uživatelů v elektronické podpisy. Specifikace je zamýšlená takovou cestou, aby byla nezávislá na konkrétní technologii a využívané implementaci.
Součástí zprávy není:

- generování a distribuce dat pro vytváření podpisu (soukromý klíč) a volba a použití kryptografických algoritmů
- legislativní interpretace jakekoliv podoby podpisu

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.

Skupina G2: Postupy pro verifikaci podpisů

(Procedures for electronic signature verification)

Dokument specifikuje doporučovanou (ve smyslu přílohy IV. Směrnice EU a v zájmu uživatelů) funkcionalitu a důvěryhodnost pro verifikaci elektronického podpisu. Jeho primárním účelem je být příručkou na cestě k verifikyci kvalifikovaných elektronických podpisů, které jsou ekvivalentní vlastnoručním podpisům (ve smyslu odstvce 5.1. Směrnice EU) a objasnit důležitost používaní časových značek.

Je však použiteklný i v situacích, kdy certifikát podepisující strany není kvalifikovaný. Definuje procesy a požadavky, které jsou využitelné v různorodých systémech.

Skupina V: Vyhodnocení shody výrobků a služeb pro elektronické podpisy

V nedávné době zde došlo rovněž k rozdělení základního zaměření na dva okruhy otázek.

Skupina V1: Vyhodnocení shody výrobků a alužeb pro elektronické podpisy

(Conformity assessment of products and services for electronic signatures)

Práce skupiny je věnována otázkám harmonizace implementací norem pro elektronické podpisy – slouží zejména jako příručka certifikujícím a testujícím 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.

Skupina V2: Vyhodnocení shody výrobků a alužeb pro elektronické podpisy

(Conformity assessment oftrustworthy systems and products – Area D1 and D2)

V rámci materiálu zpracovávaného touto skupinou bude provedena revize dokumentu, který již byl připraven v rámci V1 a tio tak, aby bylo možné ověřovat i bezpečnostní požadavky formulované v D1 a D2

Skupina AA: Rozšíření požadavků na bezpečný prostředek pro elektronický podpis ve vztahu k aplikacím pro elektronický obchod

(Extension of SSCD requirements towards specific applications/environments and towards e-commerce applications - Art5.2)

Jak již název napovídá, tento (připravovaný – práce se rozeběhly teprve v letošním roce) dokument se bude zabývat doplňujícími požadavky na bezpečné zařízení pro vytváření elektronického podpisu. Tyto požadavky budou zaměřeny na využití v oblasti *elektronického obchodu.* Bude se mj. zabývat i využitím mobilních telefonů a veřejných terminálových stanic. Dokument má být připraven do konce roku 2001.

Skupina K: Požadavky na čipové katy používané jako bezpečné zařízení pro vytváření elektronických podpisů

(Requirements for smart cards used as SSCD)

Také tento dokument je teprve připravován. Jeho cílem je stanovit požadavky na čipové karty, tak, aby vyhověly úrovni EAL4+ (dle závěrů skupiny F). Jako výchozí příklad bude analyzované použití pro WAP v mobilních telefonech. Předpokládá se spolupráce s fórem WAP a jím připravovaným PKI (Public Key Infrastructure). Výsledné PKI by mělo být kompatibilní s dokumenty IETF-pkix. Dokument má být zpracován do podzimu 2001.

Shrnutí.

Bezpečné prostředí, bezpečné prostředky pro vytváření elektronických podpisů, čipové karty, bezpečný elektronický obchod – to jsou témata, která jsou dnes v centru pozornosti zpracovatelů norem pro elektronický poodpis v Evropské Unii. Nejedná se o nějakou čistou teorii, Evropa dokazuje, že to se svojí přípravou na e-government myslí vážně.

Literatura

[1] Business Plan for the CEN/ISSS Workshop on Electronic Signatures, CEN/ISS WS/E-Sign N 125, leden 2001

[2] J. Pinkava: Elektronický podpis a Evropská Unie, DSM 2/2000

[3] J. Pinkava: Certifikace kryptografických prostředků a prostředků pro elektronický podpis, DSM 6/2000

[4] J. Pinkava: Normy pro kryptografii a návazné aplikace, DSM 2+3 /2001

[5] J. Pinkava: Evropská Unie a elektronický podpis. Legislativa a normy. Konference Bezpečnost informacií vo finančnom sektore, 21.-23.3.2001, Tatranská Lomnica.

[6] P. Vondruška: Typy elektronických podpisů, Crypto-World 3/2001, http://www.mujweb.cz/veda/gcucmp

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

[8] webovské stránky CEN/ISSS: http://www.cenorm.be/isss/workshop/e-sign/

http://www.ni.din.de/index.php3