Elektronický podpis

Mgr. Pavel Vondruška
ČESKÝ TELECOM, a.s.
e-mail: pavel.vondruska@ct.cz
http://crypto-wolrd.info/

Úvod do klasických a moderních metod šifrování
ALG082
MFF UK Praha, 23.4.2003

Elektronický podpis
Zákon o elektronickém podpisu

- Základní pojmy zákona o elektronickém podpisu
- Typy elektronických podpisů
- Princip elektronického podpisu
- Kvalifikovaný certifikát
- Poskytovatelé certifikačních služeb
- Bezpečnost elektronického podpisu
- (příklad)
- Agendy elektronického podpisu

Použité zkratky

ZoEP - Zákon o elektronickém podpisu
EP - elektronický podpis
ZEP - zaručený elektronický podpis
QP - kvalifikovaný podpis
QC - kvalifikovaný certifikát
PCS - poskytovatel certifikačních služeb
PCS-QC - poskytovatel certifikačních služeb vydávající kvalifikované certifikáty
APCS - akreditovaný poskytovatel certifikačních služeb
PBVP - prostředek pro bezpečné vytváření podpisů
PBOP - prostředek pro bezpečné ověřování podpisů
ÚOOÚ- Úřad pro ochranu osobních údajů
MICR - Ministerstvo informatiky České republiky

Zavedení EP (důvody)

Důvody: nutnost zavedení ekvivalentu ke klasickému podpisu, velký počet dokumentů v elektronické podobě, existence některých dat pouze v digitální podobě, volný pohyb dokumentů, výhody,
(…nutnost zavedení souvisí i se zavedením asymetrické kryptologie.. X symetrické šifrování „nepotřebovalo“ podpis…)

U elektronického podpisu je nutné zajistit
-identifikaci podepisující osoby
-neporušenost doručeného dokumentu (integrita)
-nepopiratelnost
-právní akceptovatelnost

lze klást další požadavky
-…. utajení
-…. zjištění, zda dokument existoval v daném čase

Pojem podpisu I.

- Pojem „podpis“ se v našem právním řádu vyskytuje ve více jak 1000 dokumentech v počtu 2800 výrazů
  (z toho však jen 331 výrazů se nachází ve 101 zákonných předpisech)
  (stav 1.1.2001)
- Žádný zákon či jiný právní předpis pojem „podpis“ nijak nedefinují

Pojem podpisu II.

- Ze (striktně) právního hlediska lze rozlišovat :
  - ***podpis***
  - ***vlastnoruční podpis***
  - ***ověřený podpis***
  - *podpis vlastní rukou (např. čl. 3 odst. 1 sdělení č.* ***179/1996 Sb.)***
  - *podpis na listině, který osoba uznala za vlastní (§ 74 zákona č. 358/1992 Sb.)*

Zákon č.227/2000 Sb.

Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb.

Zdroj:http://www.mvcr.cz/sbirka/2000/sb068-00.pdf
Datum přijetí: 29. června 2000
Datum vyhlášení: 26. července 2000
Datum účinnosti od: 1. října 2000
Sbírka částka: 68
Stránka: 3290 - 3297
Novelizován: č. 226/2002 Sb.
Novelizován: č. 517/2002 Sb.
Aktuální citace: (Zákon c.227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb. a č.517/2002 Sb.)

Evropská Unie

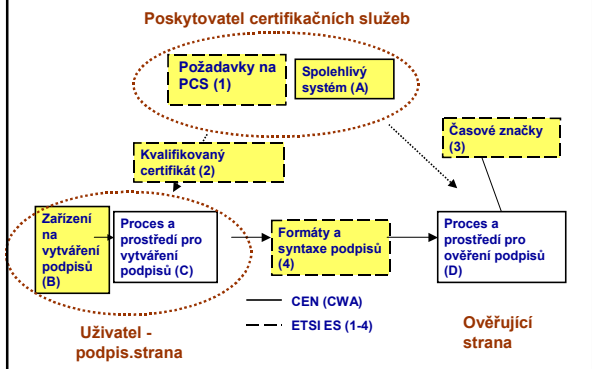
- **Směrnice EU o elektronickém podpisu**
  (schválena Evropskou komisí v prosinci 1999)

Directive 1999/93/EC

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
Zdroj:

http://www.ict.etsi.org/EESSI/Documents/e-sign-directive.pdf
Datum přijetí: 13. 12. 1999
Datum vyhlášení: 19. 1. 2000

EESSI: European Electronic Signature Standardization Initiative



EESSI

(European Electronic Signature Standardization Initiative)

Algorithms and Parameters for Secure Electronic Signatures (4.5.2001 , draft, V 1.44).

V říjnu 2001 byl tento dokument nahrazen verzí 2.1.

Předpokládá se, že pro elektronické podepisování budou zde uvedené algoritmy používány nejméně do konce roku 2005 a pro ověřování elektronického podpisu nejméně do konce roku 2006.

ETSI

Evropský telekomunikační normalizační institut (European Telecommunication Standards Institute)

1) Policy Requirements for CSPs Issuing Qualified Certificates;
2) Qualified Certificates Profile;
3) Time Stamping Profile;
4) Electronic Signature Formats.

CEN

Evropský výbor pro normalizaci (CEN)

CWA 14355 -Guidelines for the implementation of Secure Signature-Creation Devices
CWA14172 - EESSI Conformity Assessment Guidance (1-5 Parts)
CWA 14171 - Procedures for Electronic Signature Verification)
CWA 14170 -Security Requirements for Signature Creation Systems
CWA 14169 - Secure Signature-Creation Devices, version 'EAL 4+'
CWA 14168 - Secure Signature-Creation Devices, version 'EAL 4'
CWA 14167 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
Part 1: System Security Requirements
Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)

Odkazy

EESSI:
http://www.ict.etsi.org/eessi/EESSI-homepage.htm

ETSI:
http://www.etsi.org/sec/el-sign.htm
Sign up from Web-site to open El Sign mailing list

CEN:
http://www.cenorm.be/isss/workshop/e-sign

MICR:
http://www.micr.cz

(ÚOOÚ:
http://www.uoou.cz)

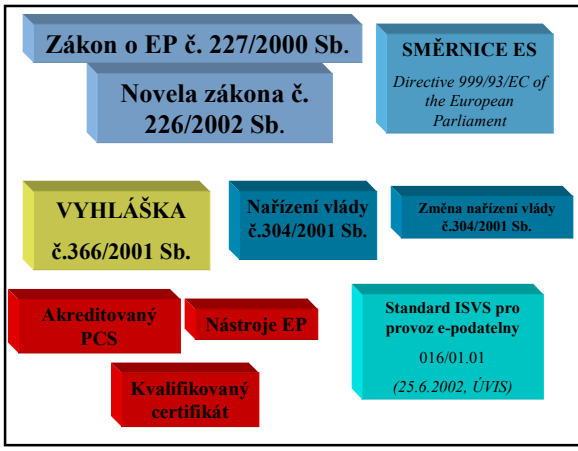
Proposed Classes of Electronic Signatures

Classes of signature:	**General electronic signature** as required in 5.2	**Qualified electronic signature -** as specified in 5.1 (Annex I, II, III)	**Enhanced electronic signature** (applicable to both general and qualified electronic signatures)
Level of legal certainty:	Can not be denied legal effect (art 5.2)	Same legal effect as hand-written signature (art 5.1)	Enhancement of technical evidence
Explanation:	Any electronic signature that is not a qualified electronic signature.	Minimum technical level required for the signer so that his electronic signature can be considered as legally equivalent with a hand-written signature.	Additional technical requirements for a verifier, such as time-stamping, but also for the signer, to enhance technical security and obtain protection against certain threats.

European Electronic Signature Standardisation Initiative

Kryptografické algoritmy a jejich parametry
pro vytváření párových dat poskytovatele
a pro prostředky pro bezpečné vytváření a ověřování
zaručeného elektronického podpisu

001	RSA	MinModLen=1020	rsagen1	pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	rsagen1	emsa	SHA1
003	RSA	MinModLen=1020	rsagen1	emsa	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	dsagen1		SHA1
006	ECDSA-Fp	qMinLen=160 r0Min=104Min Class=200	ecgen1		SHA1
007	ECDSA-F2m	qMinLen=160 r0Min=104 MinClass=200	ecgen1		SHA1



[1] **Zákon o elektronickém podpisu** a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb.
Datum přijetí: 29. června 2000
Datum účinnosti od: 1. října 2000
http://www.mvcr.cz/sbirka/2000/sb068-00.pdf

[2] **Zákon č.226/2002 Sb**. ze dne 9.5.2002, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů, a zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
Datum účinnosti od : 1. července 2002.
http://www.mvcr.cz/sbirka/2002/sb087-02.pdf

[3] **Vyhláška ÚOOÚ 366/2001 Sb.** (k Zákonu o elektronickém podpisu č.227/2000 Sb.) (Vyhláška Úřadu pro ochranu osobních údajů ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu)
Datum účinnosti od: 10. října 2001
http://www.mvcr.cz/sbirka/2001/sb138-01.pdf

[3] **Nařízení vlády č.304/2001** ze dne 25. července 2001
(Nařízení vlády č.304 ze dne 25. července 2001, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu))
Datum účinnosti od: 1. října 2001
http://www.mvcr.cz/sbirka/2001/sb117-01.pdf

[4] **Standard ISVS pro provoz elektronických podatelen** ve vztahu k používání zaručeného elektronického podpisu, 016/01.01
Uveřejněn ve Věstníku ÚVIS, ročník III, částka 1, 2002
Datum schválení: 30. 4. 2002
Datum vyhlášení : 25. června 2002
Datum účinnosti od: 25. června 2002
Počet stran: 14
http://www.micr.cz

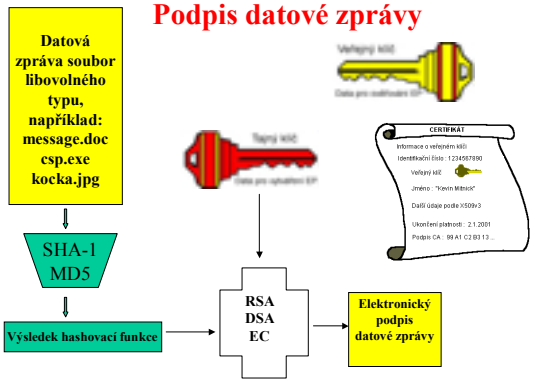
Základní pojmy

Poskytovatel certifikačních služeb (PCS)

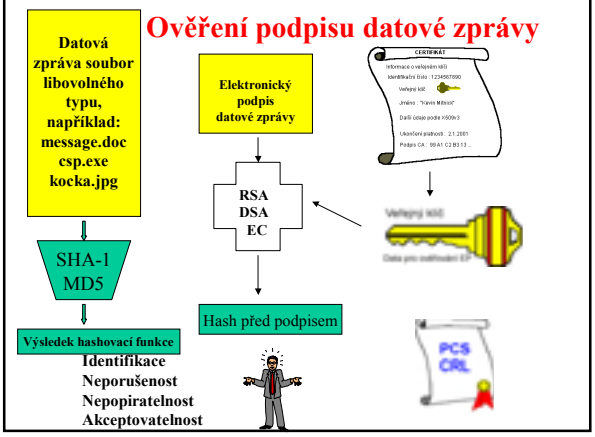
Certifikát

Elektronický podpis

Podpis datové zprávy



Ověření podpisu datové zprávy



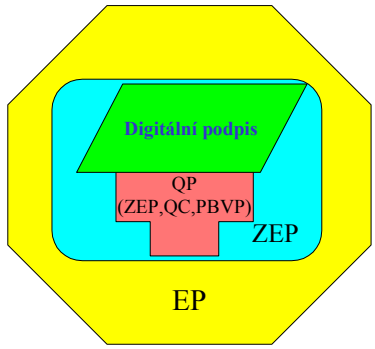
EP : § 2 a) **elektronickým podpisem** údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě,

ZEP : § 2 b) **zaručeným elektronickým podpisem** elektronický podpis, který splňuje následující požadavky:
1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba **může** udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

QP : § 3 (2) Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

PBVP : § 2 k) prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů
§ 2 m) **prostředkem pro bezpečné vytváření elektronických podpisů prostředek** pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem (§ 17)

Typy elektronických podpisů



PCS : § 2 e) poskytovatel certifikačních služeb je subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy

PCS-QC : PCS, který vydává QC (§ 12) a splnil podmínky uvedené v § 6 (Povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty)

APCS : § 2 f) akreditovaným poskytovatelem certifikačních služeb je poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona

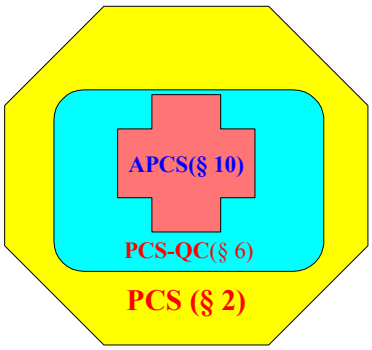
(§ 10) Podmínky udělení akreditace pro PCS
(§ 11) V oblasti veřejné moci je možné používat pouze ZEP a QC od APCS
(§ 13) Povinnosti akreditovaného poskytovatele certifikačních služeb při ukončení činnosti
(§ 14) Opatření k nápravě
(§ 18) Pokuty

Poskytovatel certifikačních služeb

Zákon rozlišuje tyto typy poskytovatelů certifikačních služeb (certifikační autorita):

- poskytovatel certifikačních služeb
- poskytovatel certifikačních služeb vydávajících kvalifikované certifikáty
- poskytovatel certifikačních služeb vydávajících kvalifikované certifikáty, který je pro tuto činnost akreditován ÚOOÚ

Typy poskytovatelů certifikačních služeb



Náležitosti kvalifikovaného certifikátu § 12

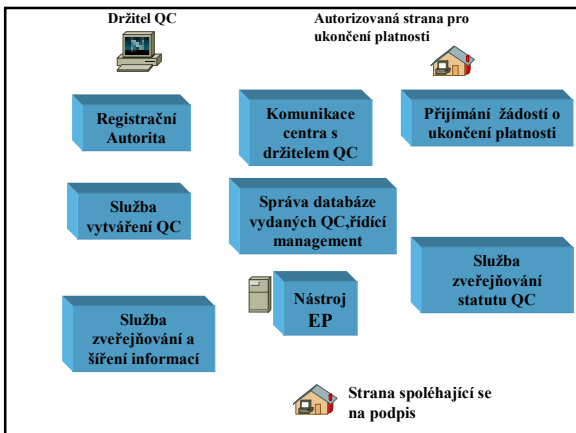
odstavec (1) QC musí obsahovat
a) označení, že je vydán jako QC dle ZoEP 227/2000
b) obchodní jméno PCS, sídlo, údaj, že byl vydán v ČR
c) jméno, příjmení nebo pseudonym podepisující osoby (značení, že jde o pseudonym)
d) zvláštní znaky podepisující osoby, vyžaduje-li to účel QC
e) data pro ověření podpisu …
f) ZEP PCS, který QC vydává
g) unikátní číslo QC (u PCS)
h) počátek a konec platnosti QC
i) omezení QC (podle povahy a rozsahu apod.)
j) omezení hodnot transakcí pro něž je QC použít

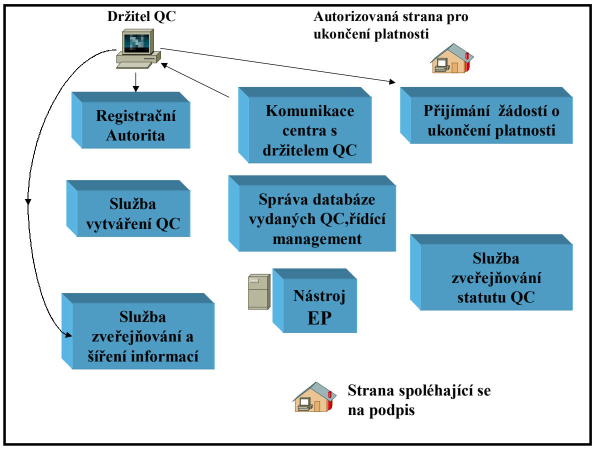
odstavec (2)
Další osobní údaje smí QC obsahovat jen se svolením podepisující osoby

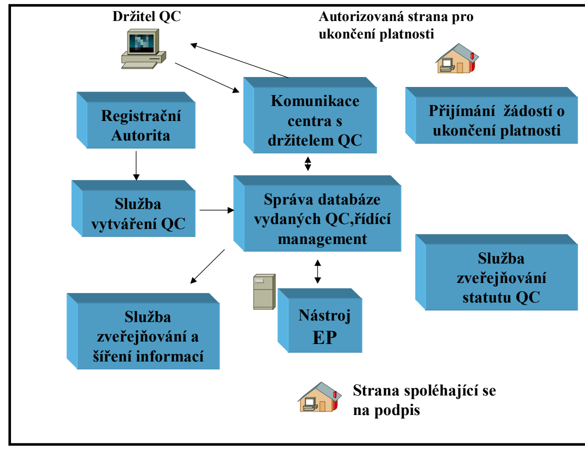
RFC (Request for Comments)

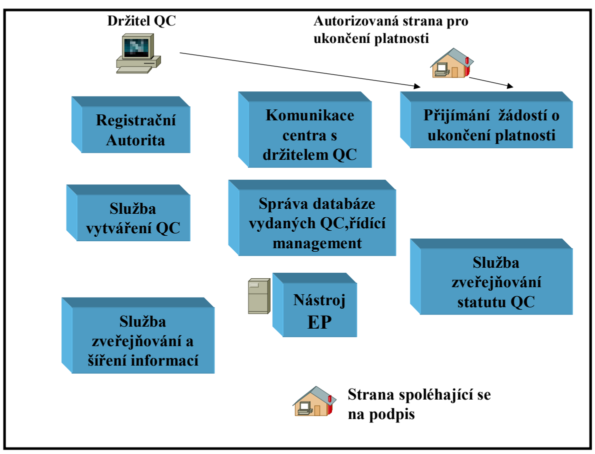
Internet X.509 Public Key Infrastructure :

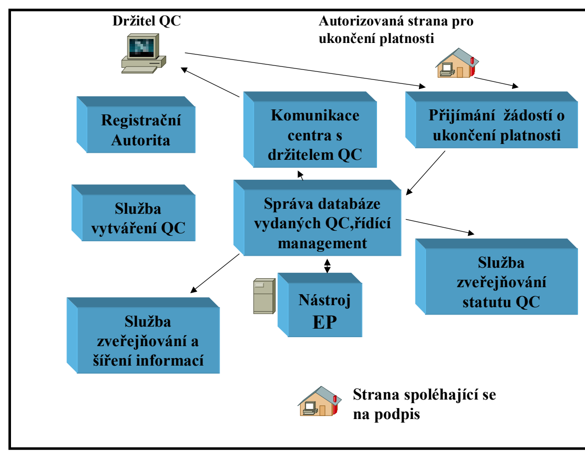
RFC 2459 - Certificate and CRL Profile
RFC 2527 - Certificate Policy and Certification Practices Framework
RFC 2560 - Online Certificate Status Protocol - OCSP
RFC 3039 - Qualified Certificate Profile
RFC 3280 - Certificate and Certificate Revocation List (CRL) Profile

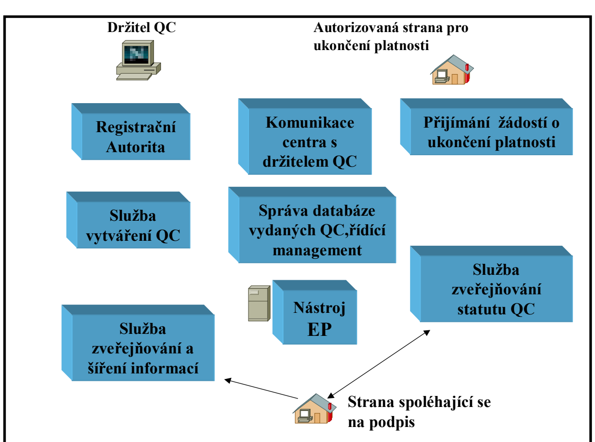












CRL

Většina současných aplikací používá při ověřování certifikátu informace ze seznamu zneplatněných certifikátů (CRL - Certificate Revocation List). Tento protokol byl v době vzniku prvních norem a standardů jediným protokolem, který byl k získání informace o ukončení platnosti (zneplatnění) zvažován. Náš zákon o elektronickém podpisu upravuje ze všech metod přístupu k informaci o ukončení platnosti certifikátu pouze požadavky na tento přístup ke statutu certifikátu.

RFC 2459 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

ETSI : ES 201 456 “Policy requirements for certification authorities issuing qualified certificates”.

Úřad v návrhu vyhlášky prosazoval stanovení periodického vydávání CRL 24 hodin (a to jako doby maximální). V průběhu připomínkového řízení příslušný paragraf vyhlášky 366/2001 získal tuto konečnou podobu:
§ 3, odst. (7)
"Doba mezi ukončením platnosti kvalifikovaného certifikátu a zveřejněním údaje o ukončení této platnosti v seznamu kvalifikovaných certifikátů, které byly zneplatněny, může činit nejvýše 12 hodin".
Formulace je poněkud nešťastná. Při přesném dodržení tohoto paragrafu totiž nemusí být zachována periodicita vydávání CRL. Pokud poskytovatel neobdrží žádnou žádost o ukončení platnosti - není nucen (dle dikce tohoto paragrafu) vydat příslušné CRL. V praxi se periodicita vydávání důsledně zachovává (CRL se číslují) a CRL se vydává i v případě, že k žádné změně nedošlo.

Další důležité informace vztahující se k CRL

CRL Distribution Point (CRL DP) – v certifikátu musí být uveden nejméně jeden distribuční bod. Vzhledem k podmínce vyhlášky 366/2001, §3, odst. 6 plyne, že toto rozšíření musí být u kvalifikovaného certifikátu použito vždy a musí zde být uvedeny alespoň dva distribuční body pro CRL!

CRL DP je definováno v RFC 2459 (1999).
Každý distribuční bod musí být popsán následujícím způsobem:
DistributionPointName :
GeneralNames or RelativeDistinghuishedName
Reason flag : FLAG
CRLIssuer : GeneralNames

Další důležité informace vztahující se k CRL

Pořadová čísla CRL a kódy označující důvod k odvolání. Pořadová čísla musí umožnit uživateli se přesvědčit zda nějaké CRL postrádá nebo ne. Každý certifikát v CRL je také označen kódem, který popisuje důvod odvolání daného certifikátu. Náš zákon ani vyhláška toto nijak dále neupravuje.

Delta-CRL. Vydávání tzv. delta-CRL umožňuje výraznou redukci velikosti rozesílaných a stahovaných CRL. V datové zprávě jsou obsaženy pouze změny oproti poslednímu vydanému CRL. Změnou se myslí nejen informace o nově zneplatněných certifikátech, ale i **vypuštění certifikátů z CRL z důvodu vypršení platnosti**. Certifikáty se po ukončení platnosti totiž v CRL neuvádějí. Náš zákon ani vyhláška vydávání takovýchto seznamů neupravuje.

OCSP

Nově vyvíjené aplikace mohou využít i moderní přístupový protokol k informaci o stavu certifikátů. Takový protokol se nazývá Online Certificate Status Protocol – OCSP. Jedná se o relativně nový protokol, který zatím v aplikacích není příliš rozšířen. Definován je např. v RFC 2560. Tento dokument byl zveřejněn teprve v červnu 1999. V úvodu dokumentu se popisuje hlavní výhoda tohoto protokolu – dostupnost informace o stavu certifikátu v době mezi vydáním dvou CRL.

RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol -OCSP"

(RFC 2559: PKIX Operational Protocols - LDAPv2
RFC 2587: PKIX LDAPv2 Schema)

Žádost podle protokolu OCSP obsahuje následující data:
-- protocol version
-- service request
-- target certificate identifier
-- optional extensions which MAY be processed by the OCSP Responder
Odpovědí na dotaz je indikace stavu certifikátu, na který se žadatel ptá. Odpověď může mít jen následující tři možnosti:
-- **good** (znamená, že nebyla přijata žádost o ukončení platnosti a certifikát není v aktuálním CRL, certifikát však nemusí být platný – tj. doba platnosti již mohla vypršet)
-- **revoked** (certifikát je uveden v CRL nebo byla přijata žádost o ukončení platnosti!)
-- **unknown** (poskytovatel certifikačních služeb není schopen na otázku odpovědět, o certifikátu nic "neví")

Obecný model PKI

V případě kvalifikovaných certifikátů je obsah certifikátu uveden v §12 zákona o elektronickém podpisu č.227/2000 Sb. Certifikát CA podepíše svým soukromým klíčem. Pro ověření elektronického podpisu je nutné, aby příjemce podepsaného elektronického dokumentu **důvěřoval** certifikační autoritě. Certifikační autorita má v tomto modelu dále za úkol poskytovat informace o stavu certifikátu (resp. veřejného klíče). Především jde o důležitou informaci, zda certifikát nebyl zneplatněn. V klasickém PKI se pro zveřejnění této informace používá seznam certifikátů, které byly zneplatněny (CRL, Certificate Revocation List) nebo jiné protokoly (OCSP, LDAP) nebo služby (zasílání, informování).

Obecný model PKI

Důvěra (trust) – entita důvěřuje druhé entitě, pokud se tato entita bude chovat tak, jak první entita očekává.

Navázání vztahu důvěry mezi autoritami – CA vydává certifikát jiné CA buď jako mechanismus potvrzeni (autorizace) jiné CA nebo mechanismus uznání existence jiné CA.

Konstrukce certifikační cesty zahrnuje vytvoření jedné nebo několika cest, které jsou nejenom formálně správně zřetězeny, ale vyhovují i dalším požadavkům, například maximální přípustné délce cesty, omezením jmen nebo certifikační politiky.

Základní metodou konstrukce cesty je zřetězení jmen od důvěryhodné CA až k posuzovanému subjektu. Konkrétně to znamená, že hodnota atributu Subject Name v jednom certifikátu musí být shodná s hodnotou Issuer Name v následujícím certifikátu v cestě.

Oficiální standardy a doporučení pro validaci certifikátu jsou součástí doporučení X.509.4 vydání (ekvivalentní k ISO/IEC 9594-8) a RFC3280.

Alternativní metodou konstrukce cesty je zřetězení identifikátorů AKID a SKID uvedených v extenzích certifikátů. AKID (Authority Key Identifier) je jednoznačný identifikátor veřejného klíče CA, SKID (Subject Key Identifier) je jednoznačný identifikátor certifikátu, obsahující specifický veřejný klíč. Konstrukce cest pomocí zřetězení AKID a SKID je zcela analogická postupu při zřetězení jmen. Existuje několik možností pro výpočet AKID a SKID, například SHA-1 otisk veřejného klíče nebo monotónně rostoucí sekvence čísel.

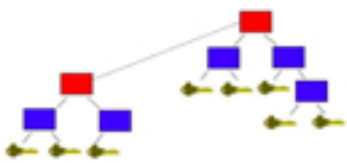
Validace certifikační cesty zahrnuje minimálně ověření, že každý certifikát v cestě je v období své platnosti, nebyl odvolán a má platný podpis.

Hierarchická struktura

(nadřízenost / podřízenost) CA

Poznámka : „Problém při ověřování certifikátů vydaných různými CA by neměl být řešen na úrovni uživatelů, ale na úrovni správců CA.“

Cross-certifikace (jedno a dvoustranná)



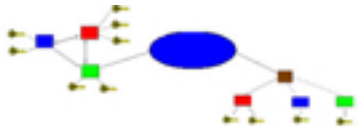
Oproti klasickým strukturám nadřízenosti a podřízenosti je zde jeden zásadní rozdíl. V případě kompromitace klíče kořenové autority „odumřou“ všechny pravé podřízené certifikační autority. Autority, které jsou ve vztahu jednostranné certifikace, nemusí odvolat své vydané certifikáty a existují metody a postupy, jak se tyto autority mají chovat, aby se vyvázaly z tohoto vztahu nepravé podřízenosti.

Propojení hierarchických struktur – síťové PKI (mesh)

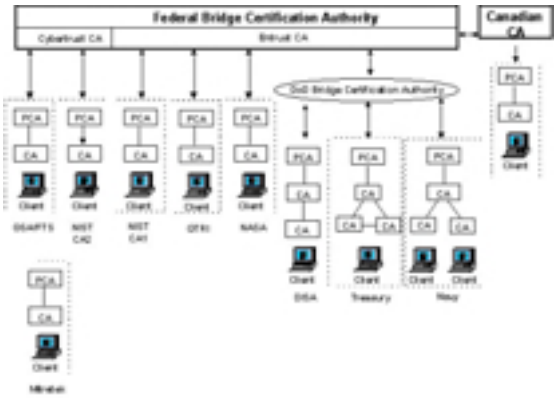
O něco méně známou strukturou, která však má velice zajímavé vlastnosti, je struktura zvaná síťové PKI (mesh PKI). Tato struktura vzniká jednak tehdy, kdy není možné se dohodnout na vztahu podřízenosti a nadřízenosti jednotlivých CA nebo není možné takovýto vztah budovat.

Propojení hierarchických struktur – bridž

(„hub-and-spoke“)



Problémy, které nastávají v případě síťové struktury PKI – především propojení velkého počtu autorit a propojení různých struktur, řeší zatím nejobecnější struktura důvěry mezi autoritami – bridžová autorita



Bezpečné zařízení pro vytváření elektronických podpisů

- Evaluace národními institucemi
- Annex III Směrnice EU
- V rámci EU – instituce akreditované dle akreditačního schématu EU (vzájemné uznávání)
- V ČR dosud neexistuje vhodná instituce

Nástroj elektronického podpisu

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje svým zaručeným elektronickým podpisem kvalifikované certifikáty (uživatele i své další certifikáty) a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Nástroj elektronického podpisu používaný pro toto podepisování nelze použít pro jiné než tyto účely! Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, je povinen používat pouze bezpečné nástroje elektronického podpisu.

Pokud nástroj elektronického podpisu splňuje požadavky stanovené zákonem o elektronickém podpisu a Ministerstvo vysloví shodu, je nástroj považován za bezpečný.

Za podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky se platí správní poplatek 10 000,- Kč.

1.CSA8000; Hardware Revision: G, Firmware Version 1.1,pracující ve FIPS módu Eracom Technologies Australia, Pty. Ltd.Burleigh HeadsQueenslandAustralia

Věstník ÚOOÚ č.15

2. nShield F3 SCSI; Firmware 5.0,Hardware verze nC4032W-150,pracující ve FIPS módu, nCipher Corporation Ltd.Jupiter HouseStation RoadCambridgeCBI 2JDUnited Kingdom

Věstník ÚOOÚ č.15

3. PrivateServer 3.0; Firmware Version 3,Hardware Version 3.0,pracující ve FIPS módu, Algorithmic Research, Ltd.10 Nevatim St., Kiryat MatalonPetah TikvaIsrael

Věstník ÚOOÚ č.16

4. Luna CA^3; Firmware verze 3.2.;hardware ,Chrysalis-ITS, Inc.One Chrysalis WayOttawaK2G6P9 OntarioCanada

Věstník ÚOOÚ č.17

§ 17
Prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů

(1) Prostředek pro bezpečné vytváření podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že
a) data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno,
b) data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie,
c) data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou.

(2) Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

§ 17
Prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů

3) Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby
a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,
b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,
c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,
d) pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,
e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,
f) bylo jasně uvedeno použití pseudonymu,
g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

1) V zákoně o elektronickém podpise není stanovena žádnému subjektu povinnost používat prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů.

2) používáním těchto prostředků se zvyšuje důvěra v tuto komunikaci

3) kvalifikovaný podpis je zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvářený prostředkem pro bezpečné vytváření elektronického podpisu

4) zjednodušeně řečeno - prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů musí splňovat bezpečnostní požadavky podle ISO 15408 , na úroveň záruky EAL 4, v ČR je toto hodnocení uznáváno z libovolné testovací laboratoře, která je schopna tyto testy provádět

Útok na „elektronický podpis“ (metody)

- prolomení kryptografie
  - slabá hashovací funkce
  - slabý algoritmus
  - slabé parametry
- špatná implementace
  - nedodržení doporučených parametrů
  - nedodržení správného postupu
  - možnost narušení (oslabení) implementace
  - vážné nedostatky při realizaci
- využití jiných slabin (systému, prostředí, prostředku)
  - nedůvěryhodný systém / prostředí (výměna CSP)
  - možnost sofistikovaně narušit aplikaci (prostředek) a toto využít
  - slabý generátor náhodných parametrů (klíčů)
- nedodržení bezpečnostních a jiných pravidel
  - nedodržení základních bezpečnostních principů (PO,OSnP, PSC)
  - např. sociální „inženýring“
- využití (zneužití) nedokonalé legislativy
  - odpovědnost za škodu „přenesena“ na PCS (§7)
  - prokázání, že podepisující / resp. osoba spoléhající se na podpis nesplnila požadavky ZoEP (§5)

Zatímco klasický podpis umožňuje v zásadě jen málo druhů "útoků", zavádí elektronický podpis celou škálu nových možností útočníka.
"Klasický podpis" v zásadě umožňuje jen následující situace :

- někdo se snaží napodobit cizí podpis (padělání podpisu)

- někdo nechce uznat podpis, který sám skutečně vytvořil (neodmítnutelnost podpisu)

- někomu se podaří získat podpis na "čistý" papír nebo "vymění několik stran" podepsaného dokumentu (integrita)

- osoba není schopna správně „vyplnit“ podpisový vzor (např. při výběru peněz) (identifikace)

Elektronický podpis však umožňuje nové typy útoků. Nejznámější je samozřejmě případ, kdy útočník získá data pro vytváření elektronického podpisu. Může se pak za tuto osobu podepsat a neexistuje žádná možnost ("elektronický grafolog"), jak takto padělaný podpis rozeznat od originálu.

Zatímco útok na klasický podpis má jen dva subjekty, na které lze útočit - osobu, která se podepisuje a osobu, která se spoléhá na podpis, elektronický podpis, který používá k předání dat pro ověření podpisu služeb nějaké třetí důvěryhodné strany (poskytovatele certifikačních služeb) - umožňuje zcela nový typ útoků - útok na poskytovatele certifikačních služeb.

Útok na „elektronický podpis“ (útočník - cíl)

Pro jednoduchost si označme A (podepisující se osoba), B (osoba spoléhající se na podpis) , PCS (poskytovatel certifikačních služeb), X - útočník (tedy není to ani A,B nebo PCS). V tabulce dále označme : CRL - seznam zneplatněných certifikátů, DVEP - data pro vytvoření elektronického podpisu, EP - elektronický podpis, P - podpis).

platnost právního úkonu
přestupek
trestný čin
odpovědnostní důsledky
(spolu)odpovědnost za škodu

Útok na „elektronický podpis“ (útočník – A,B)

Útočník/podvodník	Stručný popis útoku / pokusu o podvod	EP	P
A	tvrdí, že se nepodepsal	!	*
A	tvrdí, že text byl zaměněn	!	*
A	A zneplatní klíč u PCS a provede transakci, dříve než PCS vydá CRL, A pak odmítne odpovědnost za škodu		
A	tvrdí, že dokument, který podepsal dříve, vznikl až po zneplatnění DVEP , A se chce se zbavit odpovědnosti		
B	tvrdí, že je podepsán A	!	*
B	zamění část podepsaného textu	!	*
B	získá DVEP A po zneplatnění certifikátu, podepíše se za A a tvrdí, že dokument vznikl před zneplatněním		
A,B (domluví se)	A zneplatní klíč, než PCS vytvoří CRL , B provede transakci, škodu chce nahradit od PCS		

Útok na „elektronický podpis“ (útočník - X)

X	podepíše se za A	!	*
X	zamění text	!	*
X	získá DVEP a dále se může vydávat a podepisovat za A !!!		
X	získá DVEP A po zneplatnění certifikátu, podepíše se za A a tvrdí, že dokument vznikl před zneplatněním (chce poškodit A)		
X	zneplatní u PCS certifikát A (poškodí A)		
X	X zachytí podepsanou zprávu (bez časového údaje), X ji odešle B znovu (cíl poškodit původního odesílatele nebo i příjemce)		
X	získá u PCS certifikát za někoho jiného		
X (má k dispozici PCSX)	zamění certifikát PCS za PCSX u B a tím si umožní vydávat se za A (zasláním certifikátu, který si X vydal za A a podepsal jako PCSX) - dočasný útok		
X	získá osobní data zákazníků PCS		

Útok na „elektronický podpis“ (útočník - PCS)

PCS	zneplatní bezdůvodně certifikát A a tím jej poškodí
PCS	vytvoří certifikát pro neexistující osobu
PCS	vytvoří z dat v certifikátu A certifikát pro C (C i A mohou být poškozeny, B se totiž domnívá, že komunikuje s C nikoliv s A)
PCS	při generaci klíčů pro A si PCS ponechá jeho DVEP
PCS	úmyslně neuvede zneplatněný certifikát v CRL
PCS	zneužije osobní data svých zákazníků

Uprostřed března 2001 se přišlo na to, že jedna z největších a nejznámějších certifikačních autorit VeriSign, Inc. vydala dva certifikáty (ve velice důvěryhodné třídě - Class 3) fyzické osobě, která se vydávala za zaměstnance Microsoftu. Jméno, na které byly certifikáty vydány, zní "Microsoft Corporation". Tyto certifikáty byly vydány 29.1. a 30.1.2001.

Agendy I.

Agendy vyplývající z nařízení vlády č. 304/2001 Sb.

Tento právní předpis stanoví povinnost orgánů veřejné moci zřídit elektronické podatelny a zajistit jejich provoz, a to v těch případech, kdy ze zvláštních právních předpisů pro tyto orgány vyplývá

- povinnost přijmout podání učiněná elektronické podobě a elektronicky podepsaná anebo
- právo činit úkony v elektronické podobě a elektronicky podepsané.

Těmito zvláštními právními předpisy jsou:

- zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů
- zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů
- zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů
- zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

Agendy II.

a) Modelovým příkladem komunikace může být otevřená aplikace MPSV. Elektronické formuláře žádostí o jednotlivé dávky státní sociální podpory (SSP) zveřejnilo MPSV na své adrese http://www.mpsv.cz. Žádosti je možné podat podepsané pomocí ZEP založeného na QP od APCS. Jako součást kvalifikovaného certifikátu, vyžaduje MPSV (v souladu s novelou zákona č.227/2000 Sb.) identifikátor klienta MPSV.

b) Dalším příkladem je nově otevřená možnost podávat některá daňová přiznání. Elektronické formuláře daní lze vyplnit pomocí speciální aplikace dostupné na adrese http://www.mfcr.cz. Daňová přiznání je možné podat podepsané pomocí ZEP založeného na QP od APCS. Jako součást kvalifikovaného certifikátu, vyžaduje MFCR stejný bezvýznamový identifikátor MPSV.

Agendy III.

Zákon č. 260/2001 Sb. ze dne 26. června 2001 umožňuje použit EP ve zdravotnictví.

Pokud se vede zdravotnická dokumentace pouze na paměťových médiích výpočetní techniky, lze zápis zdravotnické dokumentace provádět jen za podmínky, že všechny samostatné části zdravotnické dokumentace obsahují ZEP osoby, která zápis provedla, podle zvláštního právního předpisu

Agendy IV.

Vyhláška č.178/2002 ministerstva financí ze dne 19. dubna 2002 o podrobnějších pravidlech pro plnění povinnosti oznámit podíl na hlasovacích právech.

Osoba, které vznikla oznamovací povinnost, odešle oznámení o dosažení, překročení nebo snížení podílu na hlasovacích právech Komisi pro cenné papíry, Středisku cenných papírů a společnosti elektronickou poštou a opatří je ZEP založeným na QC vydaném APCS.

Agendy V.

Hlášení obchodů s investičními instrumenty uzavřených mimo veřejný trh (vyhláška č. 105/2001 ministerstva financí ze dne 9. března 2001).

Povinná osoba může zaslat příslušné hlášení elektronicky, a pokud je opatří ZEP založeným na QC vydaném APCS, má se tato povinnost za splněnou a nemusí toto hlášení zasílat dodatečně v tištěné podobě opatřené podpisem nebo předat elektronicky na nosném médiu.

Agendy VI.

Zákon o podpoře výzkumu a vývoje č. 130/2002 Sb. umožňuje poskytovateli stanovit způsob podání návrhů a předložení projektů elektronicky, podepsaných podle zákona o elektronickém podpisu.

Agendy VII.

Na výrobce zboží, kteří uvádějí na trh výrobky v obalech, a firmy, které obaly vykupují, se vztahuje vyhláška č.117/2002 Sb. ministerstva životního prostředí ze dne 16. března 2002 o rozsahu a způsobu vedení evidence obalů a ohlašování údajů z této evidence. Ta umožňuje výkazy za uplynulý kalendářní měsíc zasílat ministerstvu v elektronické podobě podepsané podle zvláštního právního předpisu.