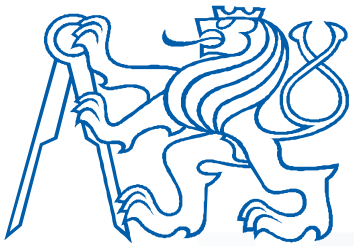
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

A7B32KBE – 13.přednáška

Certifikáty, CA, PKI

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz



Obsah

- Certifikační autorita
- Certifikát
- Časová razítka
- Atributové certifikáty
- DV certifikáty
- X.509
- DER,BER, ASN.1

Certifikační autorita - CA

- Základní části:
  - registrační autorita (RA)
    - Komunikace s žadatelem
    - Ověřování totožnosti
  - certifikační autorita (CA)
    - Generování (podepisování) certifikátů
  - správní autorita (SA)
    - Udržuje adresář vydaných certifikátů.
    - Zodpovídá za publikované údaje.
    - Zajišťuje dostupnost certifikátů přes Internet (LDAP).
- musí ručit za jednoznačnost vydaných certifikátů
  - pole subject a sériové číslo certifikátu
- může ručit za totožnost uživatele, vlastnícího dvojici veřejný/soukromý klíč

Certifikační autorita - CA

Třídy CA:

- Třída 1 – CA ručí pouze za jednoznačnost certifikátu
  - Registrační autoritu takové CA je možné zjednodušit na program. Žadatel vyplní formulář WWW-serveru a protokolem HTTPS jej odešle (stačí autentizace serveru - klient je anonymní).
- Třída 2 - jako třída 1 + CA kontroluje totožnost uživatele
  - je vybudována síť registračních autorit kam osobně dochází uživatelé se svými žádostmi
  - RA ověří totožnost uživatele a odesílá žádost k vyřízení CA.
  - CA třídy 2 uchovává svůj soukromý klíč v bezpečném hardware.
- Třída 3 – jako třída 2, ale vydané certifikáty jsou určeny výhradně pro konkrétní aplikaci - pro nic jiného se nepoužívají.
  - Příklad: certifikát vydaný bankou lze použít k přihlašování k Internet bankingu, ale nelze ho použít pro podepisování emailu.
  - CA třídy 3 uchovává svůj soukromý klíč v bezpečném hardware.

Certifikační autorita - CA

Třídy CA:

- Třída 1 – CA ručí pouze za jednoznačnost certifikátu
  - Registrační autoritu takové CA je možné zjednodušit na program. Žadatel vyplní formulář WWW-serveru a protokolem HTTPS jej odešle (stačí autentizace serveru - klient je anonymní).
- Třída 2 - jako třída 1 + CA kontroluje totožnost uživatele
  - je vybudována síť registračních autorit kam osobně dochází uživatelé se svými žádostmi
  - RA ověří totožnost uživatele a odesílá žádost k vyřízení CA.
  - CA třídy 2 uchovává svůj soukromý klíč v bezpečném hardware.
- Třída 3 – jako třída 2, ale vydané certifikáty jsou určeny výhradně pro konkrétní aplikaci - pro nic jiného se nepoužívají.
  - Příklad: certifikát vydaný bankou lze použít k přihlašování k Internet bankingu, ale nelze ho použít pro podepisování emailu.
  - CA třídy 3 uchovává svůj soukromý klíč v bezpečném hardware.

Certifikační autorita - CA

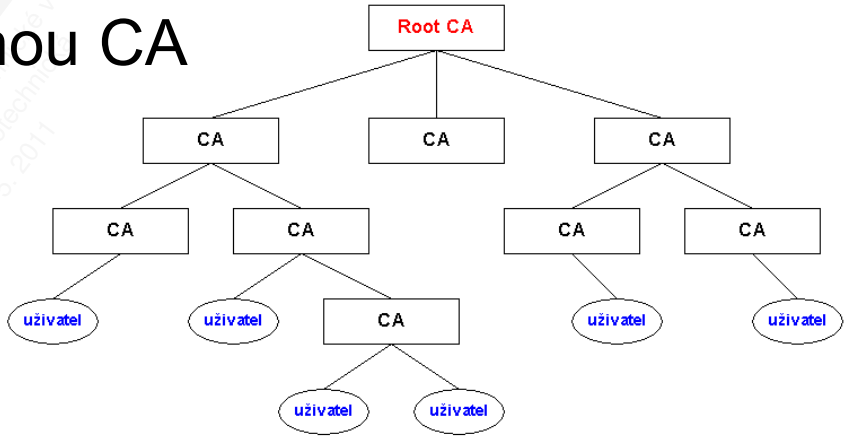
Jak zajistit, vzájemné důvěřování dvou různých CA ?

- nadklíč – ověřuje obě CA
- křížový certifikát (cross certificate) – certifikát, který znají obě CA a důvěřují mu
- prostředník (bridge), třetí entita, která je s jednou CA spojena jedním křížovým certifikátem a s druhou CA druhým křížovým certifikátem
- ruční (fyzická) výměna klíčů jednotlivých CA jejími zástupci

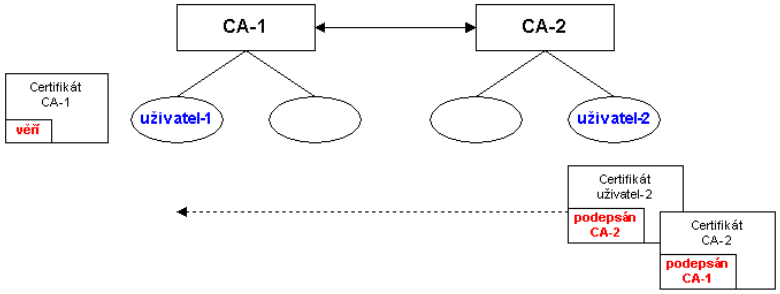
Certifikační autorita - CA

Certifikát certifikační autority:

1) kořenový (root)
   - pole issuer a subject jsou (téměř) identické
   - certifikát je podepsán samotnou CA
2) certifikát je podepsán nadřazenou CA



3) křížová certifikace



- datová zpráva, která je vydána poskytovatelem certifikačních služeb (PCS)

- řeší problém slouží důvěryhodného předání veřejného klíče podepisující osoby

- certifikát spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost

- tato vazba je stvrzena elektronickou značkou nezávislé důvěryhodné třetí strany - Certifikační Autority (v ZoEP se místo pojmu CA používá PCS)

Certifikát X.509v3

- využívají je technologie S/MIME, SSL/TLS, IPsec, SSH,
- součást série doporučení ITU-T X.500 definujících globální adresářovou službu
- adresářová služba je systém spravující informace o uživatelích
- certifikát spojuje entitu s veřejným klíčem
- entita je jednoznačně identifikována pomocí význačného jména (DN - distinguished name)
- dnes se používá nejvíce verze X.509v3
- nejčastější typ certifikátů (existují i jiné formáty certifikátů EDI, PGP,…), ale příliš se nepoužívají

Certifikát – X.509v3

- adresářová struktura (ve smyslu „telefonní seznam“ ne adresář souborů)
- jedinečné jméno *(Distinguished Name, DN)* je tvořeno posloupností relativních dílčích jmen *(Relative Distinguished Name)*
- relativní jedinečné jméno = dílčí informace o subjektu stát, město, název společnosti, divize, oddělení, adresa, jméno, příjmení)
- relativní jedinečná jména se v jedinečném jméně mohou opakovat (např. s jinou hodnotou)
- nejvyšší adresářovou úrovní byla definice země (C – Country), následována organizací (O – Organization), organizační jednotkou (OU – Organization Unit) a konče jednotlivými osobami (CN – Common Name)

Certifikát X.509v3 - příklad

Common Name (CN) = Tomáš Vaněk
Surname (SN) = Vaněk
DNQualifier = *prázdné*
(Karel IV by zde měl „IV“, v PKI slouží k rozlišení certifikátů osob se stejným předmětem)
Serial Number = 1
(rozlišení certifikátů téhož subjektu - !neplést si s pořadovým číslem certifikátu)
E-mail (E) = tomas.vanek@fel.cvut.cz (podle RFC 822)
Organization Unit (OU) = K13132
Organization Unit (OU) = FEL
Organization (O) = ČVUT
Locality (L) = Praha
Country (C) = CZ (dvoupísmenný kód podle ISO 3166)

Certifikát – X.509v3

- **Verze** – X.509v3 obsahuje hodnotu 2
- **Pořadové číslo certifikátu** - celé kladné číslo, jedinečné v rámci CA. Dvojice pořadové číslo + vydavatel jednoznačně identifikuje jakýkoliv certifikát.
- **Doba platnosti** - skládá se ze dvou časových údajů určujících od kdy do kdy je certifikát platný. Životnost certifikátu by měla být výrazně nižší než je doba nutná k prolomení certifikovaného veřejného klíče.
- **Algoritmus podpisu** - vždy dvojice (hash funkce + asymetrický šifrovací algoritmus)

  - specifikuje jakým způsobem CA podepsala daný certifikát
- **Vydavatel (Issuer)** -jméno CA, která vytvořila a podepsala daný certifikát.
- **Předmět (Subject)**–specifikuje držitele certifikátu. CA nesmí vydat různým osobám různé certifikáty se stejným předmětem.

- **Identifikátor veřejného klíče**- obsahuje veřejný klíč včetně informací o algoritmu a parametrech použitých k jeho vytvoření. Neplést s polem „Algoritmus podpisu“

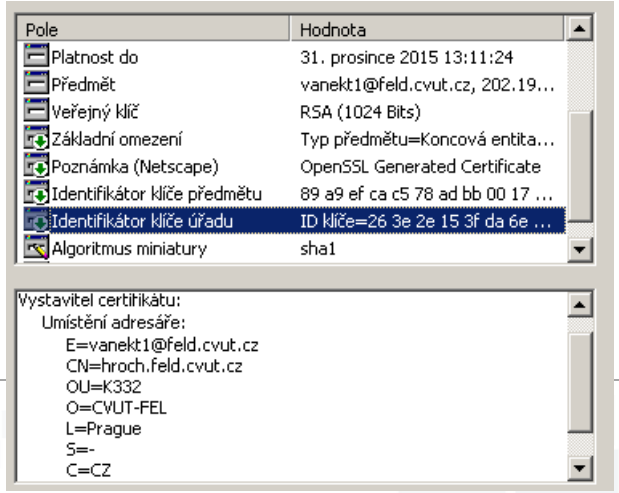
Certifikát – X.509v3

- **Rozšíření**-obsahuje různé dodatečné informace o předmětu certifikátu
  - závažné (critical) (v IE – zelená šipka); aplikace jim **musí** rozmět, jinak je certifikát odmítnut
  - Nezávažné (non-critical)

Např.: **základní omezení** (basic contraints) - u certfikátů CA musí být použito a je závažné

- **certifikační politiky (**Certificate Policies - u MS se jmenuje Zásady certifikátu) - volitelné

- **Podpis** - elektronický podpis všech ostatních položek certifikátu. Kromě samotného zašifrovaného hash kódu, obsahuje informace o algoritmu a parametrech použitých k jeho vytvoření.



Certifikát – X.509v3

- Použití klíče
  - Digitální podpis (Digital Signature) – podepisování zpráv
  - Neodvolatelnost (Non Repudation)- ověřování podpisu
  - Šifrování klíče (Key Encipherment)
  - Šifrování dat (Data Encipherment) – jiných než jsou klíče
  - Výměna klíčů (Key Agreement)
  - Podepisování certifikátů (Key Certificate Sign) – umožní podepisovat certifikáty – tzn.vytvořit si vlastní CA
  - Podepisování CRL (CRL Sign)
- toto rozšíření je závažné
- omezí použití certifikátu na vymezené účely (např. zamezí uživatelům vydávat další certifikáty)

Formáty ukládání certifikátů X.509

PEM - Privacy Enhanced Mail
- původ ve standardu pro zabezpečení elektronické pošty
- ASCII formát
- kódování Base64 (3B dat se převedou na 4B ASCII)
- před takto zakódovaná data je přidána hlavička obalen hlavička
- může obsahovat soukromé i veřejné klíče (kromě certifikátu)

DER/BER (Distinguished Encoding Rules, Basic Encoding Rules)
- Binární formát pro klíče i certifikáty
- překódováním do Base64 a obalením hlavičkami vznikne formát PEM
- DER je zjednodušená podmnožina BER

ASN.1
- standard ASN.1 (Abstract Syntax Notation) se věnuje popisu dat a standard DER pak jejich uložení a transportu.
- dobře čitelný pro lidi (textový formát, struktura podobná prg. jazykům)

Certifikát v PEM formátu

-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIEQrLqHzANBgkqhkiG9w0BAQUFADBDMRIwEAYKCZImiZPyLGQBGRYCY3oxGTAXBgoJkiaJk
/IsZAEZFgljZXNuZXQtY2ExEjAQBgNVBAMTCUNFU05FVCBDQTAeFw0wNTA2MTcxNDUwMTdaFw0yNTA2MTcxNTI
wMTdaMEMxEjAQBgoJkiaJk/IsZAEZFgJjejEZMBcGCgmSJomT8ixkARkWCWNlc25ldC1jYTESMBAGA1UEAxMJQ0VT
TkVUIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8RVNQRNqWLs6fn9L34J/kg+jHUL6mKltRX8EC
JPGuokGm5XD+7CzrZ7sCebIiZQrhe0h350bDeeeoOH2kI1Y2f9EGorW16ReUieWS7Xt6TxmkLPX/9aMtRJEBhmuisq2z
FaTmfqj8cJTWVrqPKoWMEt36voF5wzqfIBEAzP0U8z+jxrhs2roVl+Vr3g02h3RDVG1usZGsoSJpdSewZQboyA0/y2tMu0
onIt9dyov27PE8CYnbDKmcWD7XOMR/sVczkWqNju3F2S+EpCUchfFkkPxk0Q+ElDhyC9XUWqD+XdHbTht5zwVEq7R
O6APbiEh16qcwYWQ0RG1XKC5djYnHwIDAQABo4IB0DCCAcwwEQYJYIZIAYb4QgEBBAQDAgAHMIIBDgYDVR0fBII
BBTCCAQEwgf6ggfuggfikVDBSMRIwEAYKCZImiZPyLGQBGRYCY3oxGTAXBgoJkiaJk/IsZAEZFgljZXNuZXQtY2ExEj
AQBgNVBAMTCUNFU05FVCBDQTENMAsGA1UEAxMEQ1JMMYZEaHR0cDovL3d3dy5jZXNuZXQuY3ovcGtpL2NybC
9jbj1DRVNORVQlMjBDQSxkYz1jZXNuZXQtY2EsZGM9Y3phMS5jcmyGWmxkYXA6Ly9sZGFwLmNlc25ldC1jYS5jei9jbj
1DUkwxLGNuPUNFU05FVCUyMENBLGRjPWNlc25ldC1jYSxkYz1jej9hdXRob3JpdHlSZXZvY2F0aW9uTGlzdDArBgNV
HRAEJDAigA8yMDA1MDYxNzE0NTAxN1qBDzIwMjUwNjE3MTUyMDE3WjALBgNVHQ8EBAMCAQYwHwYDVR0jBBg
wFoAUL2wFw1EmrK85nD44Nd1SKSeAxfUwHQYDVR0OBBYEFC9sBcNRJqyvOZw+ODXdUikngMX1MAwGA1UdEwQ
FMAMBAf8wHQYJKoZIhvZ9B0EABBAwDhsIVjcuMTo0LjADAgSQMA0GCSqGSIb3DQEBBQUAA4IBAQA5NzubuXmgx
Ni38eBENiuHdPrPtHh9puLkZTPvEGyJaqmWkXBR6HhX68VRF9NlCpdxGqbjYB1gbh62nHQSpWf4fKuU3LONwSZvn6+
lpUckxubcQyf6oERlh0uJS4vqa4UNl3WZmCzsM1OgvNvuPnqqeW2i36KIafooTVG8m+ywMgfiwf1s38y+zisWTjmExcQF1
/4F/JX1fhu7JrFkLDVYoYSSewL937sD7cyq89xmb+TAgI8nTZNNZsyYAbFOqTzWqe4KmC9Q2j6Ic0ImuPsqIqO5qk52rx
MUzHP+j3GPg8zHGBlLI1HH6FeOWpNobs4cceQ7NBTNre8SNrvWfSax--
---END CERTIFICATE-----

Ověření certifikátu

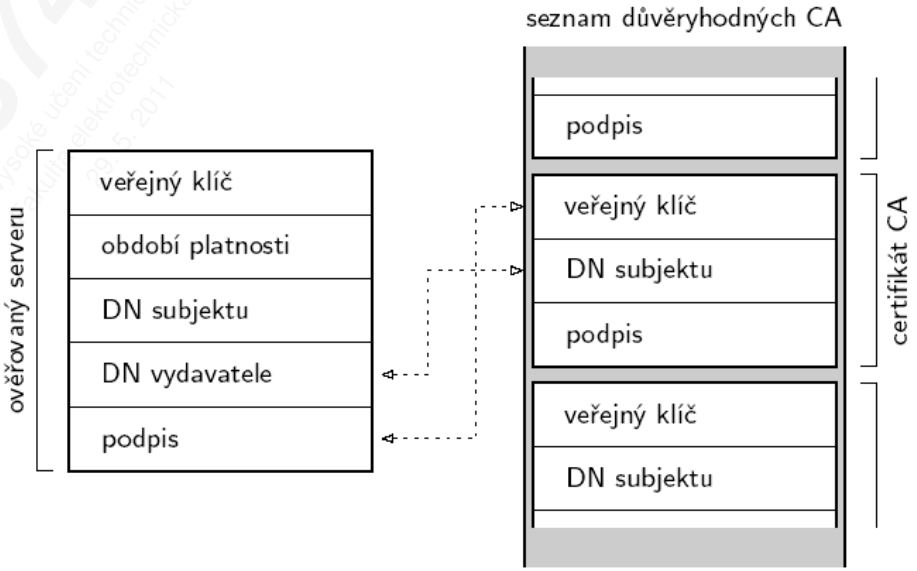
- zjišťování, zda je certifikát:
  - platný (aktuální datum je mezi *notBefore* a *notAfer)*
  - řádně podepsaný
  - není na seznamu CRL
  - vydán důvěryhodnou CA
  - byl klíčový pár vygenerován na příslušném zařízení a zda-li je příslušný soukromý klíč odpovídajícím způsobem chráněn

Přímé ověření certifikátu

- nejjednodušší forma ověření
- certifikát musí být uložen v databázi ověřujícího
- porovnává se certifikát ověřovaného s certifikátem v databázi ověřujícího
- stačí ověřit období platnosti certifikátu s aktuálním datem a časem

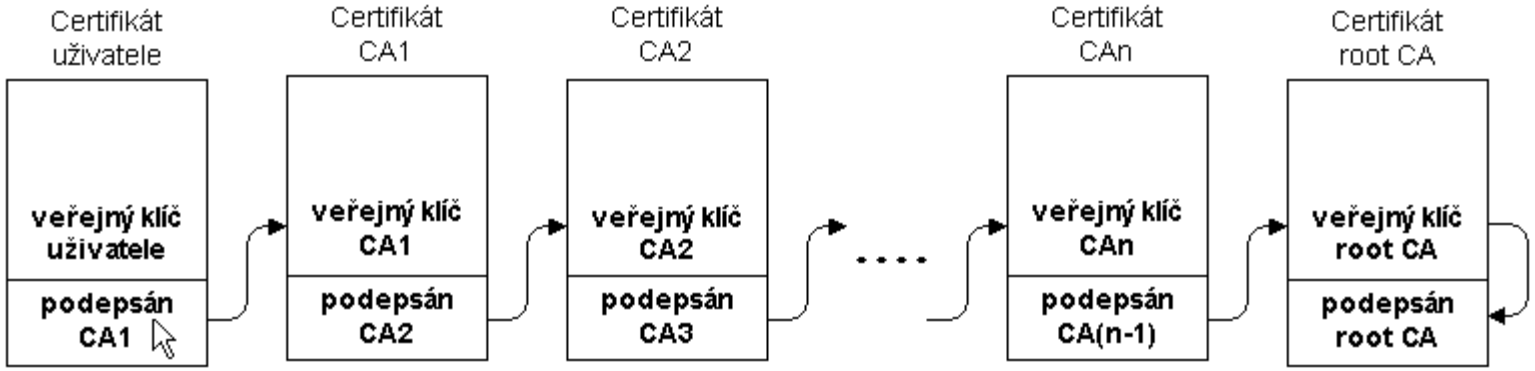
Ověření certifikátu pomocí certifikátu CA

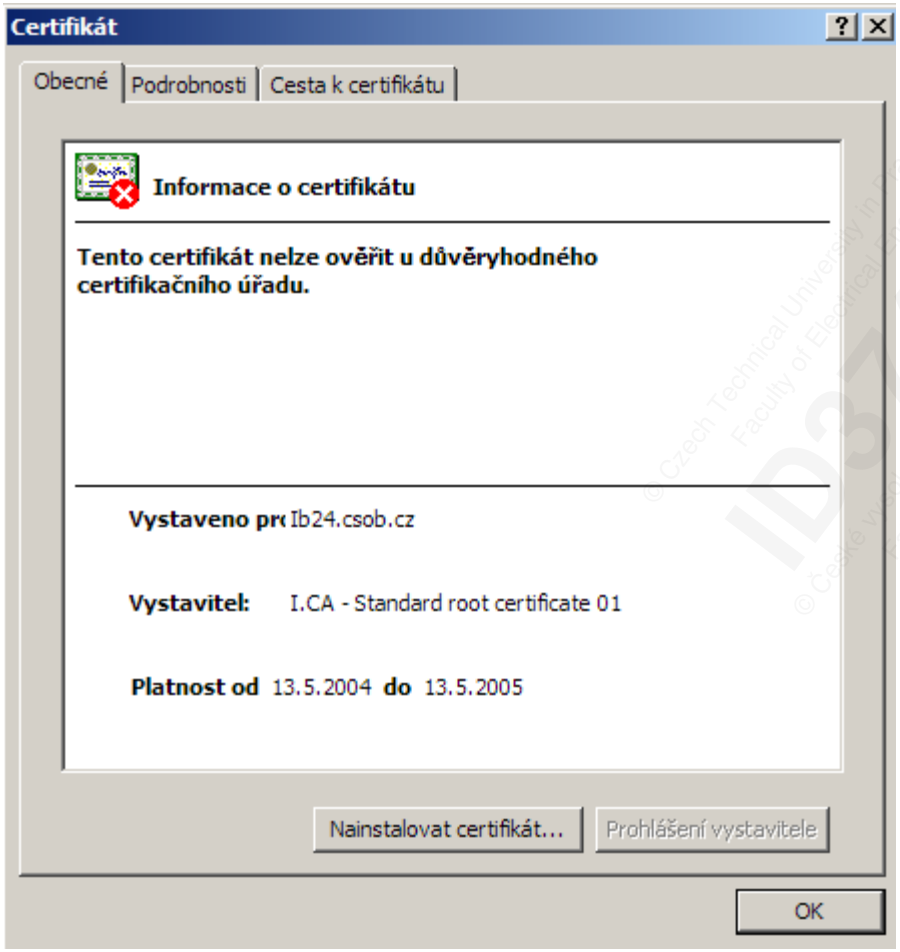
1. ověření platnosti certifikátu (datum, čas, CRL)
2. ověření, zda byl certifikát vydán CA reprezentovanou certifikátem CA uloženým v databázi ověřujícího
3. ověření pravdivosti podpisu ověřovaného certifikátu (ověření popisu certifikátu pomocí veřejného klíče certifikátu CA)

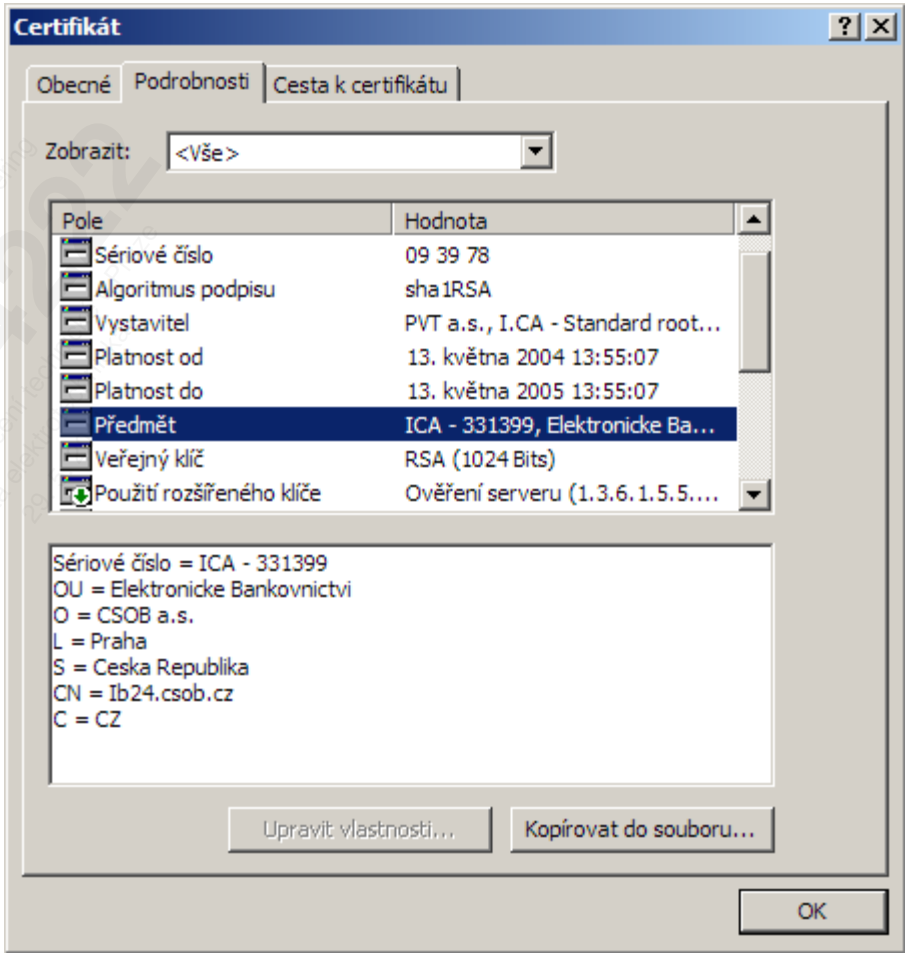


Konstrukce a validace certifikační cesty

- validace certifikátu X.509.4 (ISO/IEC 9594-8) a RFC3280
- Konstrukce certifikační cesty zahrnuje vytvoření jedné (nebo více cest) , které jsou:
  1) formálně správně zřetězeny
  2) vyhovují i dalším požadavkům (např. maximální přípustné délce cesty, omezením jmen nebo certifikační politiky)
- zřetězení jmen od důvěryhodné CA až k posuzovanému subjektu.
- hodnota atributu Subject Name v jednom certifikátu musí být shodná s hodnotou Issuer Name v následujícím certifikátu v cestě.
- Kořenový certifikát - hodnoty obou atributů jsou stejné




Certifikát
Obecné
Podrobnosti
Cesta k certifikátu
Informace o certifikátu
Tento certifikát nelze ověřit u důvěryhodného certifikačního úřadu.
Vystaveno pr(Ib24.csob.cz
Vystavitel: I.CA - Standard root certificate 01
Platnost od 13.5.2004 do 13.5.2005
Nainstalovat certifikát...
Prohlášení vystavitele
OK


Certifikát
Obecné
Podrobnosti
Cesta k certifikátu
Zobrazit:
<Vše>
Pole
Hodnota
Sériové číslo
09 39 78
Algoritmus podpisu
sha1RSA
Vystavitel
PVT a.s., I.CA - Standard root...
Platnost od
13. května 2004 13:55:07
Platnost do
13. května 2005 13:55:07
Předmět
ICA - 331399, Elektronicke Ba...
Veřejný klíč
RSA (1024 Bits)
Použití rozšířeného klíče
Ověření serveru (1.3.6.1.5.5....
Sériové číslo = ICA - 331399
OU = Elektronicke Bankovnictvi
O = CSOB a.s.
L = Praha
S = Ceska Republika
CN = Ib24.csob.cz
C = CZ
Upravit vlastnosti...
Kopírovat do souboru...
OK

Životní cyklus certifikátu

- Vygenerování párových dat (klíčů)
  - PEM
  - PKCS#10 (převzato jako RFC 2986)
  - CRMF (Certificate Request Message Format – RFC 2511, 4211)
- Vytvoření žádosti o certifikát
  - Identifikační údaje žadatele
  - Veřejný klíč
  - Důkaz vlastnictví soukromého klíče
  - Údaje pro fakturaci
  - Heslo pro komunikaci s CA
- Vydání certifikátu
- Možné „konce“
  - Obnovení certifikátu (Renew vs. Rekey)
  - Vypršení platnosti certifikátu (pole *notAfter*)
  - Odvolání certifikátu (CRL, OCSP)

Zneplatňování certifikátů

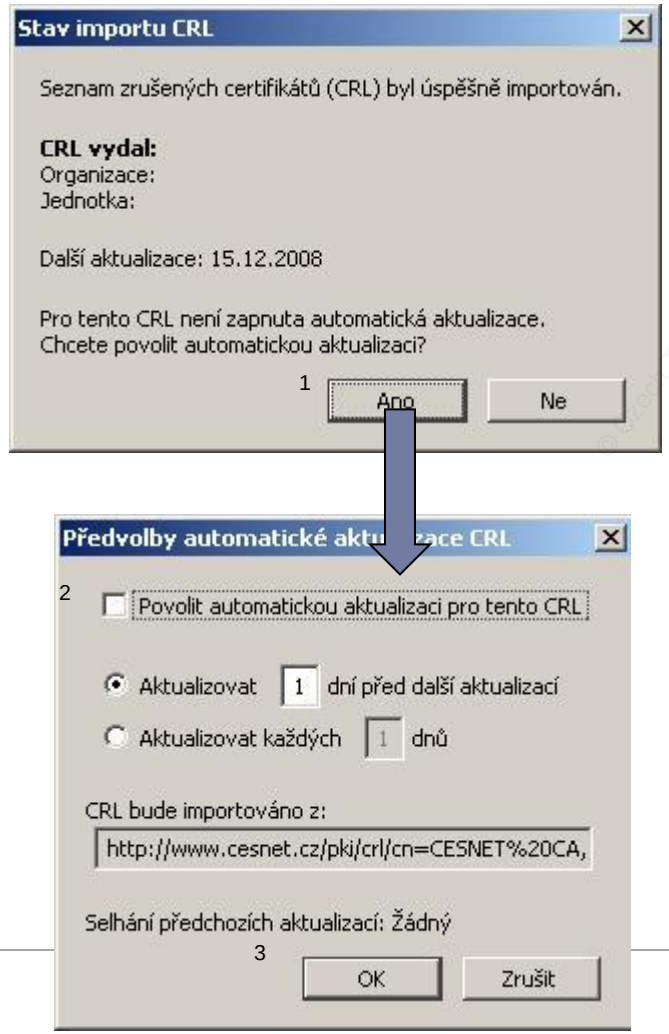
- Z nejrůznějších důvodů se může stát, že certifikát ztratí důvěryhodnost. Typicky to jsou situace, kdy vlastník certifikátu zjistí narušení bezpečnosti, nebo dojde ke změně jména vlastníka certifikátu.
- certifikát je třeba zneplatnit
- způsob tohoto procesu definuje CA ve své certifikační politice.

Seznam zneplatněných certifikátů (CRL)

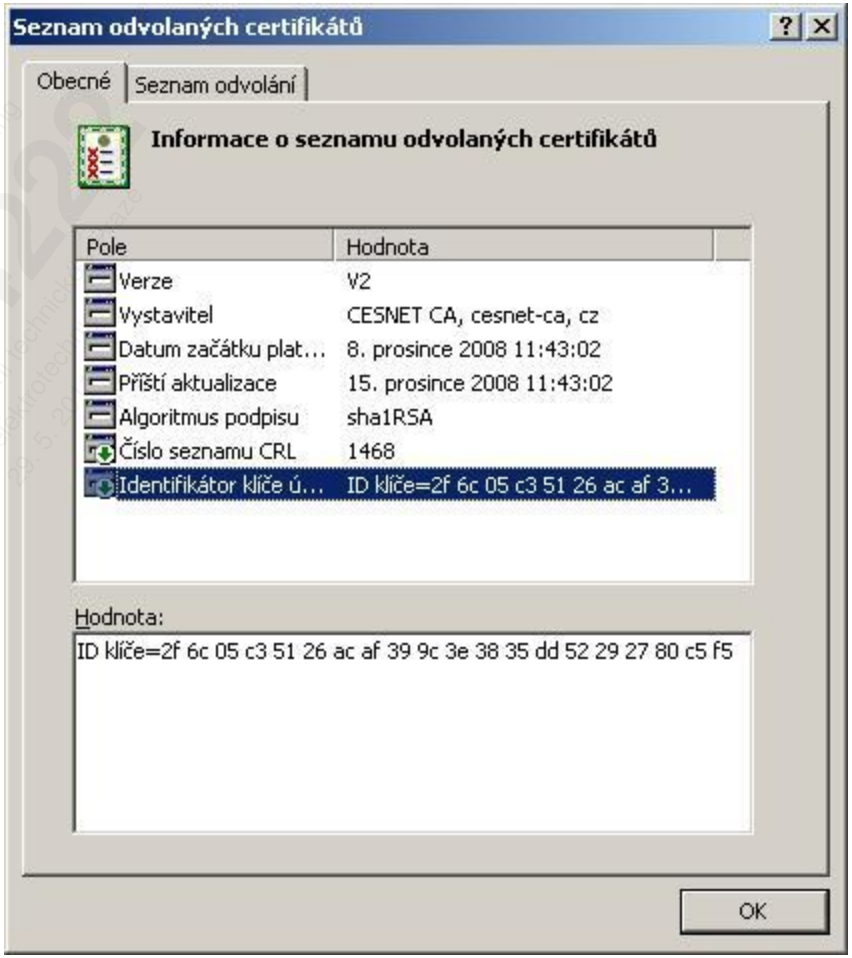
- umístění sériového čísla certifikátu na seznam zneplatněných certifikátů (Certificate Revocation List)
- tento seznam je pravidelně zveřejňován a aktualizován
- odkaz na umístění CRL je součástí certifikátu
- seznam je číslovaný, obsahuje datum vydání, datum vydání příštího seznamu a je podepsán CA

CRL

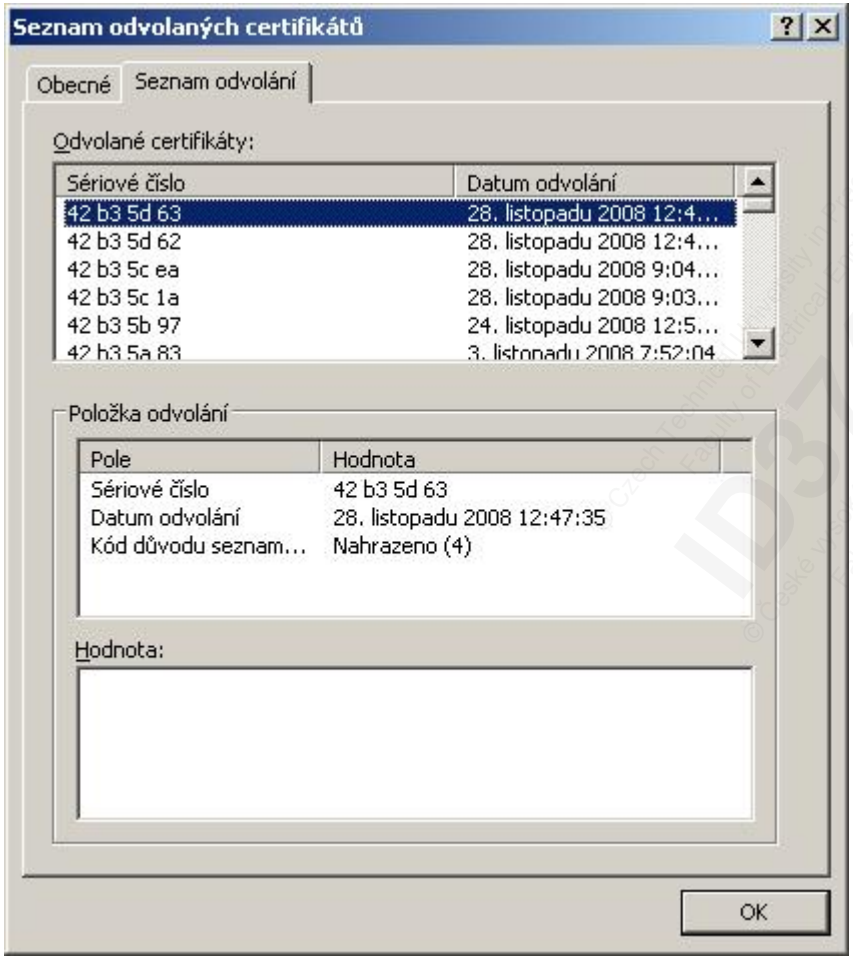
Firefox 3.0 – import CRL

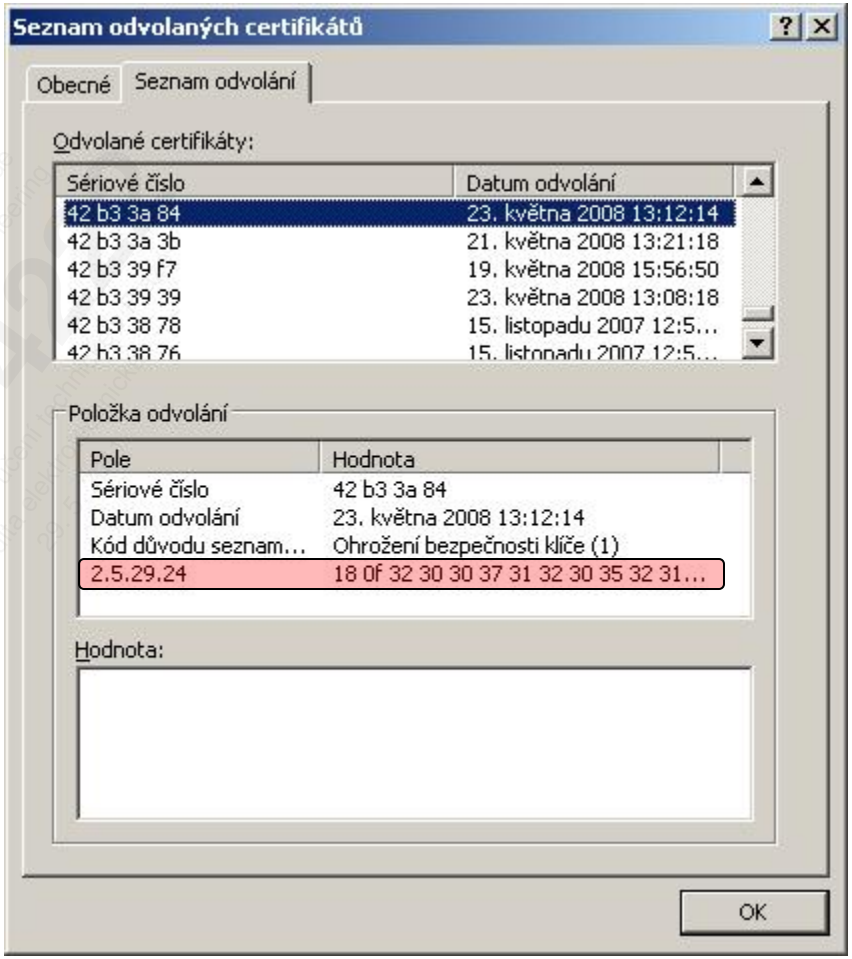


IE - ukázka CRL



CRL

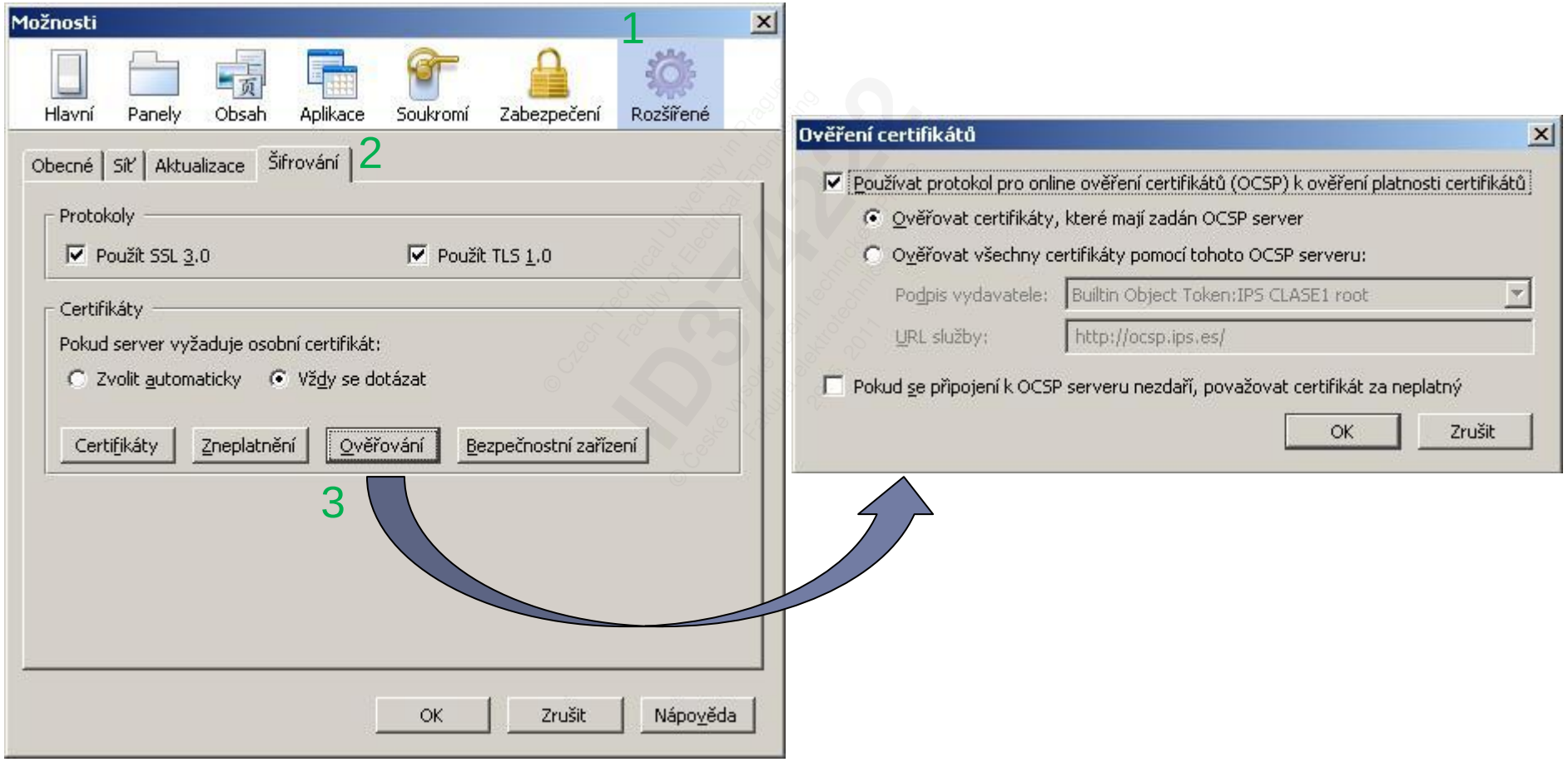

Seznam odvolaných certifikátů
Obecné
Seznam odvolání
Odvolané certifikáty:
Sériové číslo
Datum odvolání
42 b3 5d 63
28. listopadu 2008 12:4...
42 b3 5d 62
28. listopadu 2008 12:4...
42 b3 5c ea
28. listopadu 2008 9:04...
42 b3 5c 1a
28. listopadu 2008 9:03...
42 b3 5b 97
24. listopadu 2008 12:5...
Položka odvolání
Pole
Hodnota
Sériové číslo
42 b3 5d 63
Datum odvolání
28. listopadu 2008 12:47:35
Kód důvodu seznam...
Nahrazeno (4)
Hodnota:
OK


Seznam odvolaných certifikátů
Obecné
Seznam odvolání
Odvolané certifikáty:
Sériové číslo
Datum odvolání
42 b3 3a 84
23. května 2008 13:12:14
42 b3 3a 3b
21. května 2008 13:21:18
42 b3 39 f7
19. května 2008 15:56:50
42 b3 39 39
23. května 2008 13:08:18
42 b3 38 78
15. listopadu 2007 12:5...
Položka odvolání
Pole
Hodnota
Sériové číslo
42 b3 3a 84
Datum odvolání
23. května 2008 13:12:14
Kód důvodu seznam...
Ohrožení bezpečnosti klíče (1)
2.5.29.24
18 0f 32 30 30 37 31 32 30 35 32 31...
Hodnota:
OK

Zneplatňování certifikátů - OCSP

- **Online Certificate Status Protocol**
- jiný mechanismus pro zjištění platnosti certifikátu
- RFC 2560, klient/server architektura
- Klient pošle OCSP serveru žádost obsahující identifikaci certifikátu, OCSP server vrátí podepsanou informaci o tom, zda je certifikát platný či nikoliv, nebo chybové hlášení, že certifikát nemá v databázi.
- Výhody OCSP oproti CRL :
  - Informaci o zneplatnění lze distribuovat prakticky všem okamžitě.
  - řeší problém velkých PKI, kde je velký objem dat v CRL
  - šetří se objem dat přenášených v síti
- OCSP může být provozován samotnou CA nebo může být tato pravomoc delegována na jiný server.
- Informace o OCSP serverech může být také přímo součástí certifikátu.

OCSP - Firefox



Kvalifikovaný certifikát (QC)

- speciální případ certifikátu
- QC je certifikát, který má náležitosti stanovené v 12 ZoEP a byl vydán PCS splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty

QC musí obsahovat - 12 odst.1 ZoEP

a) označení, že je vydán jako QC dle ZoEP 227/2000 Sb. (v poli rozšíření)

b) obchodní jméno PCS, sídlo, údaj, že byl vydán v ČR

c) jméno, příjmení nebo pseudonym podepisující osoby (+ označení, 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

Kvalifikovaný certifikát (QC)

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 použit

odst. 2)
- další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby

Poskytovatelé certifikačních služeb (PCS)

Základní rozdělení: PCS – Poskytovatel certifikačních služeb
KPCS – Kvalifikovaný poskytovatel certifikačních služeb
APCS – Akreditovaný poskytovatel certifikačních služeb

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

KPCS - 2 i) PCS, který vydává QC (12) nebo QSC (12a) a splnil podmínky uvedené v 6a (Povinnosti poskytovatele certifikačních služeb vydávajícího QC a QSC)

Poskytovatelé certifikačních služeb (PCS)

APCS je podle 2f) poskytovatel certifikačních služeb, který získal akreditaci ve smyslu zákona č.227/2000 Sb. o elektronickém podpisu.

Přehled udělených akreditací je zveřejňován na stránkách Ministerstva Informatiky – www.micr.cz

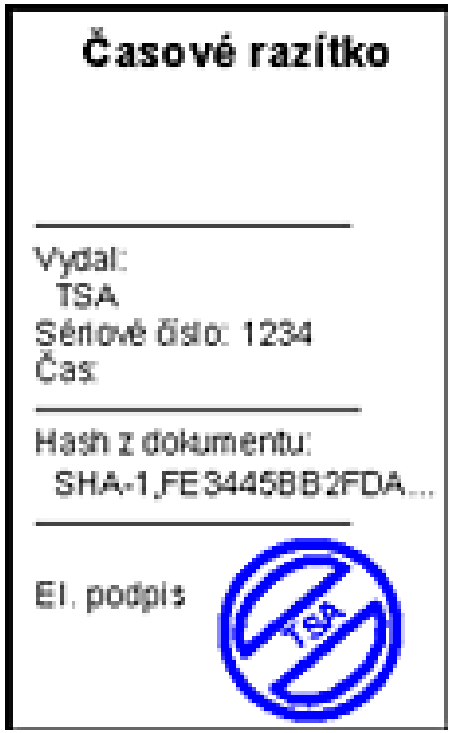
Podle 11 je v oblasti komunikace s veřejnou mocí možné používat pouze ZEP a QC vydané APCS

V ČR dnes existuje tři akreditovaní PCS

1. CA www.ica.cz
E-identity www.eidentity.cz
Česká pošta www.postsignum.cz

Časové razítko

- též časová značka, časová známka, Time Stamp (TS)
- dokazuje, že dokument v daném čase a podobě existoval
- datová struktura obdobná certifikátu
- časové razítko je elektronicky podepsáno autoritou pro vydávání časových razítek (Time Stamping Authority - TSA)



Elektronicky podepsaná struktura časového razítka mj. obsahuje: jméno vydavatele jedinečné sériové číslo razítka, kontrolní součet (hash) z dokumentu a čas.

Časová razítka

Časová autorita prokazuje synchronizaci svého časového zdroje s celosvětovým časovým standardem UTC (Universal Time Coordinated).

Nejčastější způsoby využití:

- práce s dokumenty – jednoznačné doložení času, ve kterém dokument v daném tvaru existoval
- ochrana logovaných záznamů - časové razítko jednoznačně definuje čas, ve kterém v dané podobě soubor existoval
- elektronické podatelny
- notářské služby
- on-line obchody

Časová razítka

Kvalifikované časové razítko musí obsahovat (12b ZoEP):

a) unikátní číslo kvalifikovaného časového razítka (v rámci daného kvalifikovaného PCS)
b) označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,
c) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno a stát, ve kterém je kvalifikovaný poskytovatel usazen,
d) hodnotu času, která odpovídá UTC při vytváření kvalifikovaného časového razítka
e) data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno
f) elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

Atributový certifikát

- struktura podobná certifikátu
- používá se v kombinaci s certifikátem
- místo veřejného klíče obsahuje jiné identifikační údaje např. přístupová práva do aplikace, role uživatele,…
- vydává je atributová autorita (AA)

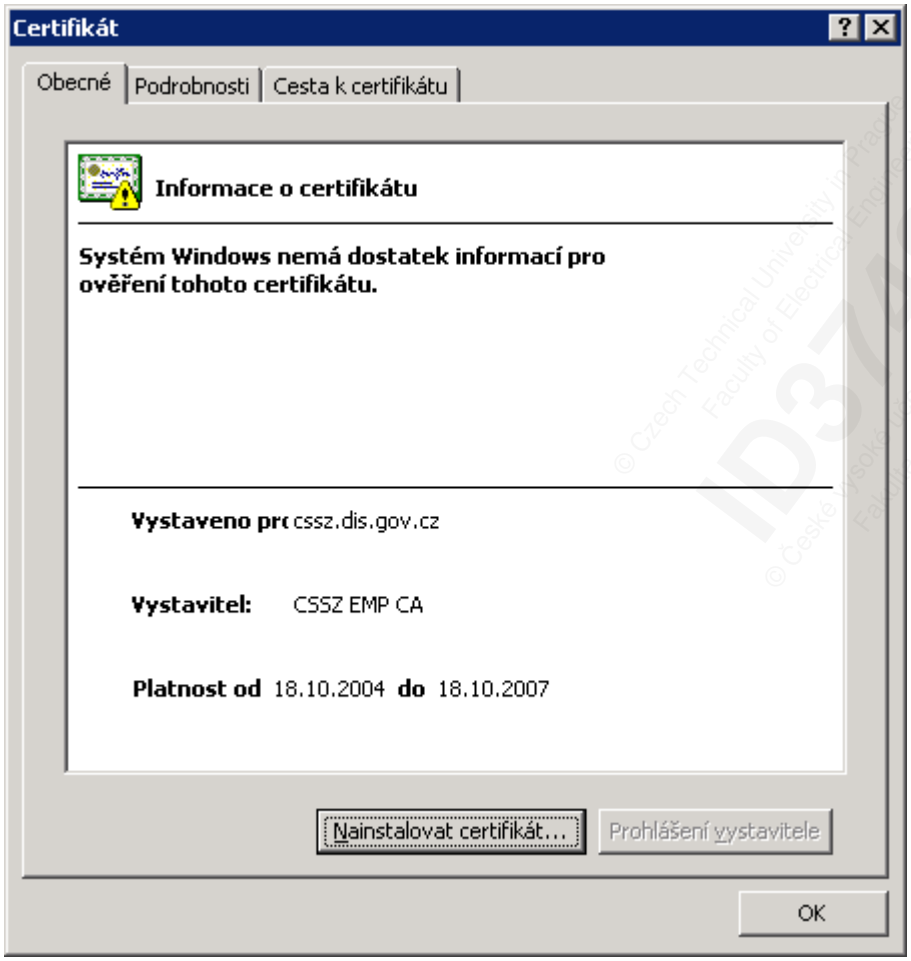
DV certifikát

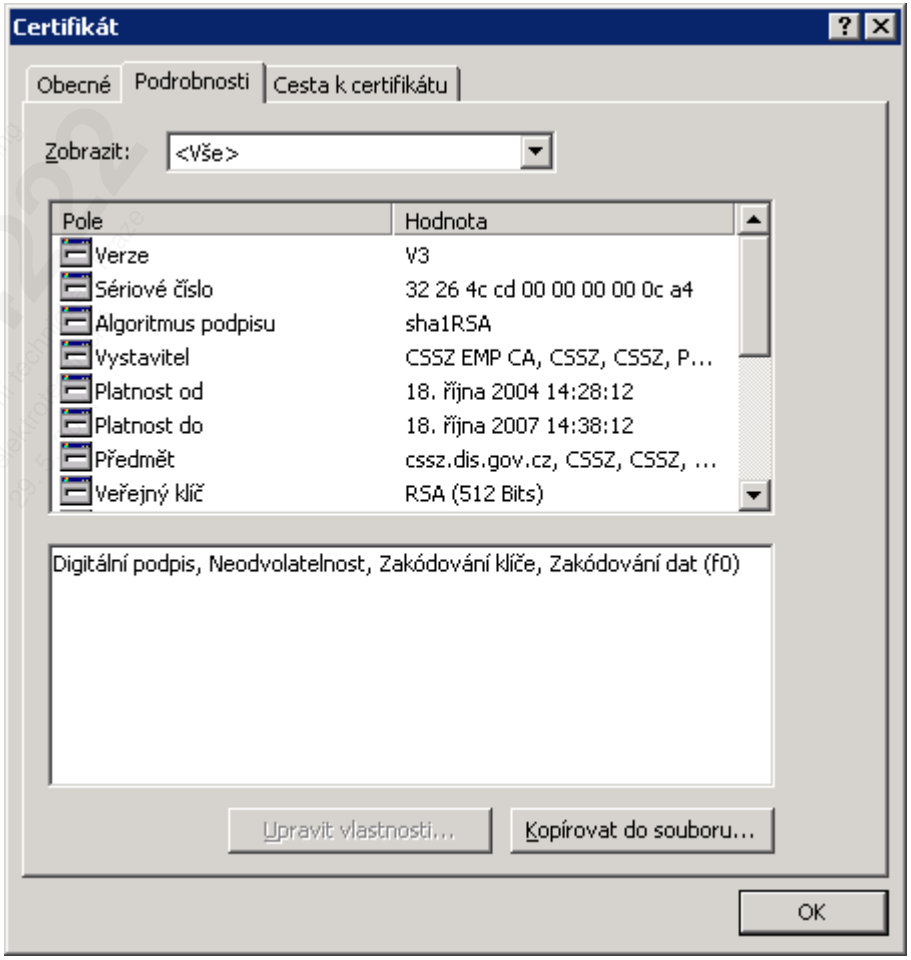
- dokazuje, že dokument v daném čase a byl v držení nějakého subjektu
- datová struktura obdobná certifikátu
- DV certifikát je elektronicky podepsán serverem pro vydávání DV certifikátů (DVCS)

PKI – Public Key Infrastructure

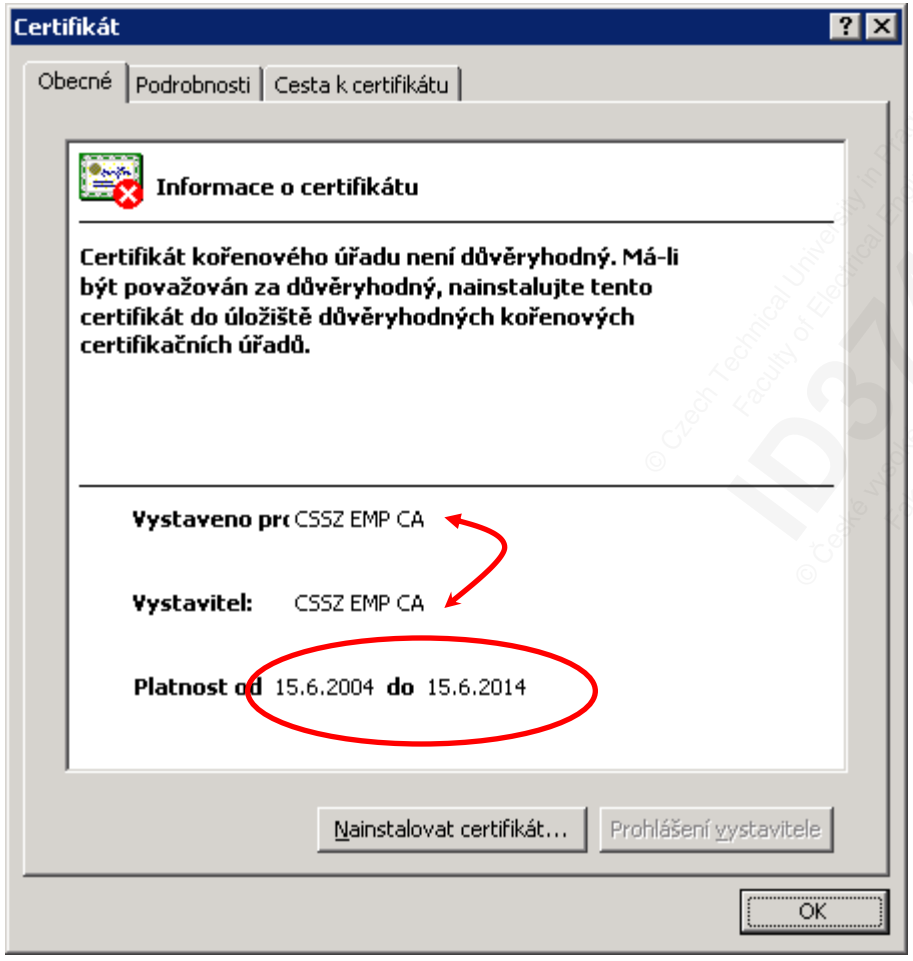
- PKI je souhrn znalostí, dohod, konvencí, technických postupů, organizačních principů, speciálního hardware a software, aplikací, standardů, norem, prováděcích směrnic, legislativy, osob a subjektů, které používají nebo se spoléhají na příslušné technologie (certifikáty, kryptografické klíče) ….
- Český ekvivalent je „ Infrastruktura veřejných klíčů“
- pojem PKI se často používá právě v souvislosti s elektronickým podpisem

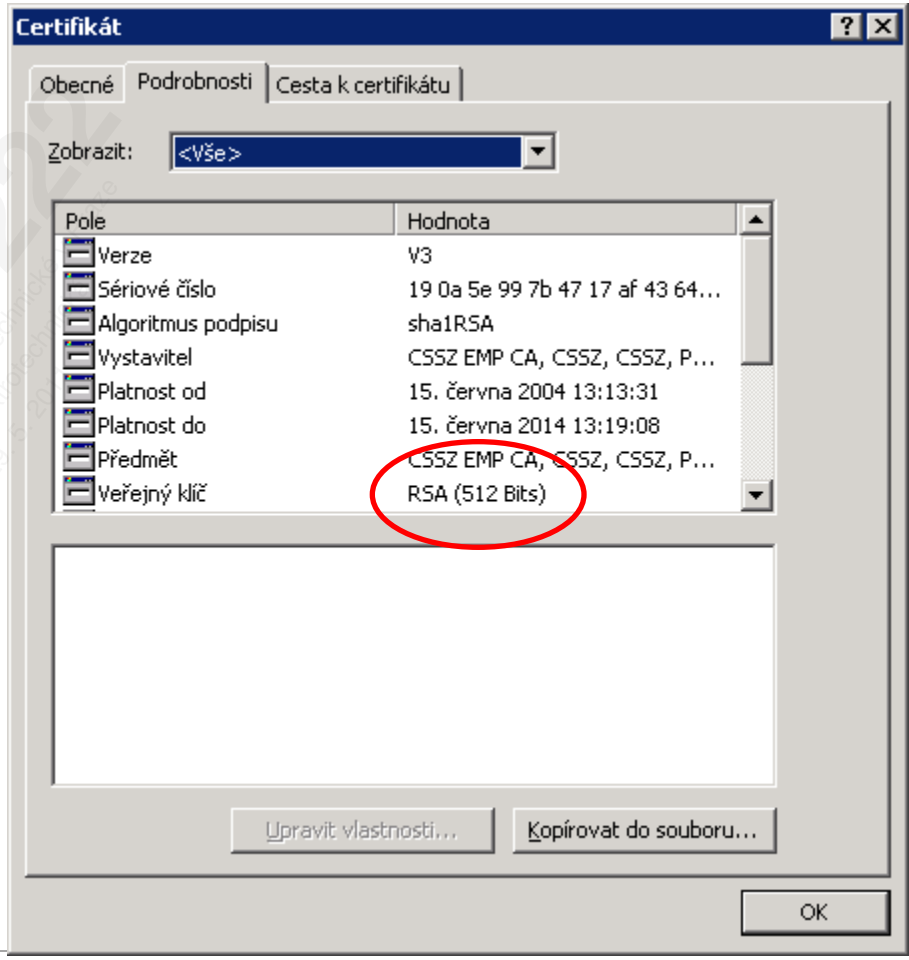
Certifikát vydaný ČSSZ pro šifrování komunikace mezi firmami a ČSSZ





Kořenový certifikát CA ČSSZ – dnes již neplatí





Dotazy