MFF UK
Praha, 22. duben 2008

Elektronický podpis / CA / PKI – část 2

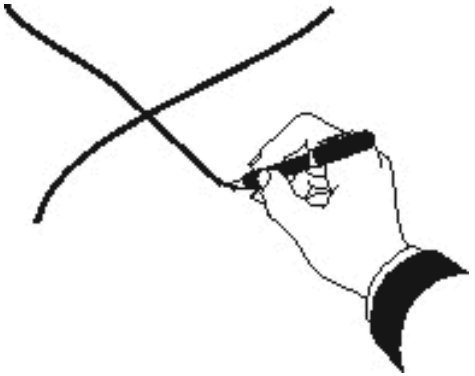
http://crypto-world.info/mff/mff_03.pdf

P.Vondruška

Telefónica

O2

MOTIVACE



PODPIS * VLASTNORUČNÍ PODPIS * OVĚŘENÝ PODPIS
(RAZÍTKO, SVĚDCI,
ÚŘEDNÍ OSOBA, NOTÁŘ)

EP * ZEP * ZEP+QC (PCS-QC)* ZEP+QC (APCS)*QP
+ další služby TS (časové razítko), elektronický notář, …

Základní pojmy

Poskytovatel certifikačních služeb (PCS)

Certifikát

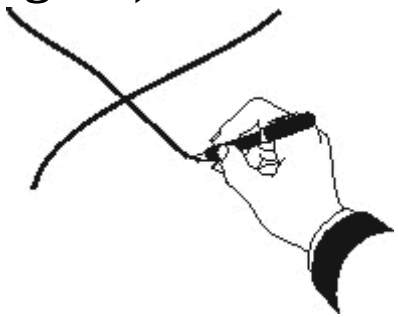
Elektronický podpis

ZoEP č.227/2000

Důvodem : nutnost zavedení ekvivalentu ke klasickému podpisu, velký počet dokumentů v elektronické podobě, existence některých dat pouze v digitální podobě, volný pohyb dokumentů, výhody…

U elektronického podpisu je nutné zajistit

- **-identifikaci podepisující osoby**
- **-neporušenost doručeného dokumentu (integrita)**
- **-nepopiratelnost**
- **-právní akceptovatelnost**



lze klást další požadavky

- **-…. důvěrnost obsahu**
- **-…. zjištění, zda dokument existoval v daném čase**

Pojem podpisu

1. 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)
2. Žádný zákon či jiný právní předpis pojem „podpis“ nijak nedefinují (Např. občanský soudní řád, právní předpis upravující mimo jiné způsob podávání soudní žaloby a její náležitosti, jakož i náležitosti soudního rozhodnutí, neupravuje výslovně podepisování žaloby či rozsudku, pouze v komentáři k zákonu je vysloven názor, že uvedené písemnosti musí být podepsány)

Působnost zákona o elektronickém podpisu a výklad hlavních pojmů

- Účinnost a požadavky na jednotlivé subjekty a jejich odpovědnost (podepisující se osoba, osoba spoléhající se na elektronický podpis, organizace, veřejná moc, poskytovatel certifikačních služeb)
- Typy elektronických podpisů (elektronický podpis, zaručený a kvalifikovaný elektronický podpis)
- Typy poskytovatelů certifikačních služeb a certifikátů (PCS, kvalifikovaný certifikát, PCS vydávající kvalifikované certifikáty, akreditace PCS)
- Některé problémy spojené s aplikací zákona v praxi

§ 2 Vymezení některých pojmů

Pro účely tohoto zákona se rozumí :

datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,

podepisující osobou fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické či právnické osoby

§ 2 Vymezení některých pojmů

daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,

daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,

prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů

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 : Kvalifikovaný podpis : vzniká použitím zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu.

UP : Uznávaný podpis : vzniká použitím zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu, který vydal akreditovaný poskytovatel certifikačních služeb.

Novela zákona č. 227/2000 Sb., o elektronickém podpisu

Dne 26. července 2004 nabyla účinnosti novela zákona o elektronickém podpisu (č. 440/2004 Sb.). Tento předpis nově zavádí pojem "**kvalifikované časové razítko**", které prokazuje existence elektronického dokumentu v čase. Další novinkou je možnost používat „**elektronické značky**“. Elektronickou značkou může označovat data právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy. Elektronické značky jsou podmínkou pro připravované zavedení výpisů ze stáních rejstříků na poštách a matrikách. Novela dále upravuje používání elektronických podatelen na orgánech veřejné moci. http://www.micr.cz/scripts/detail.php?id=1540

Zákon o elektronickém podpisu č.227/2000 Sb., rozlišuje tyto typy podpisů :

1) Elektronický podpis
2) Zaručený elektronický podpis
3) Zaručený elektronický podpis založený na certifikátu (nepřímo)
4) Zaručený elektronický podpis založený na kvalifikovaném certifikátu
5) Uznávaný podpis
6) Kvalifikovaný podpis (nepřímo)
7) Elektronická značka (po novele)

- Kvalifikované časové razítko (služba pro zvýšení důvěry v el.podpisy)
- (Digitální podpis – technologie, která umožňuje realizovat předchozí typy podpisů)

Zákon o elektronickém podpisu č.227/2000 Sb., rozlišuje tyto typy certifikátů :

1) certifikát
2) kvalifikovaný certifikát
3) kvalifikovaný systémový certifikát
4) kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb

Náležitosti kvalifikovaného certifikátu

odstavec (1) QC musí obsahovat

a) označení, že je vydán jako QC dle ZoEP č. 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 použit

odstavec (2)

Další osobní údaje smí QC obsahovat jen se svolením podepisující osoby

Zákon o elektronickém podpisu č.227/2000 Sb., rozlišuje tyto typy poskytovatelů :

1) poskytovatel certifikačních služeb
2) poskytovatel certifikačních služeb vydávající kvalifikované certifikáty
3) poskytovatel certifikačních služeb vydávající kvalifikovaná časová razítka
4) akreditovaný poskytovatel certifikačních služeb

Přehled akreditovaných poskytovatelů v ČR:

(Ministerstvo informatiky zveřejňuje v souladu s § 9 odst. 2 písm. e) zákona č. 227/2000 Sb. přehled udělených akreditací):
http://www.micr.cz/scripts/detail.php?id=603

1. První certifikační autorita, a. s.,
http://www.ica.cz/home_cs/
Podvinný mlýn 2178/6,
PSČ 190 00 Praha 9

2.Česká pošta, s. p.
http://qca.postsignum.cz/
Olšanská 38/9,
PSČ 225 99 Praha 3

3.eIdentity a. s.,
https://www.eidentity.cz/app
Vinohradská 184/2396,
PSČ 130 00 Praha 3

Přehled akreditovaných poskytovatelů na Slovensku (NBÚ SR):

http://www.nbusr.sk/sk/elektronicky-podpis/zoznam-aca/index.html

1. CA EVPÚ
www.caevpu.sk
Trenčianska 19,
018 51 Nová Dubnica

2. Prvá slovenská certifikačná autorita (PSCA)
www.psca.sk
Borská 6,
841 04 Bratislava

3.The Slovak National Certification Authority (SNCA)
ep.nbusr.sk/snca
Budatínska 30,
850 07 Bratislava 57

4. První certifikační autorita, a.s.
www.ica.cz
Podvinný mlýn 2178/6
190 00 Praha 9

5. Certifikačná autorita Ministerstva obrany SR (CAMOSR)
www.pki.mil.sk
Olbrachtova 5,
911 01 Trenčín

Přehled poskytovatelů certifikačních služeb v EU :

Aktualizovaný seznam akreditovaných poskytovatelů, poskytovatelů certifikačních služeb, kteří vydávají kvalifikované certifikáty, atd. je udržován v rámci projektu eEurope :

http://ec.europa.eu/information_society/eeurope/2005/all_about/security/esignatures/index_en.htm

§ 5 Povinnosti podepisující osoby

(1) Podepisující osoba je povinna

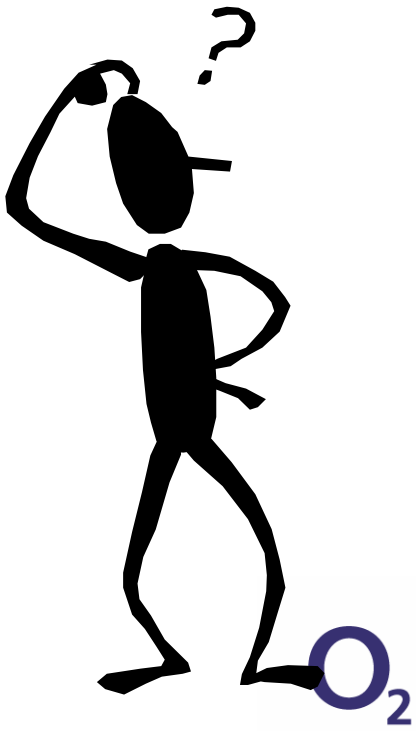
a) zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který jí vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu,

c) podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu.

§ 5 Povinnosti podepisující osoby

(2) Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle zvláštních právních předpisů. Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.
(Zákon č.40/1964 Sb., občanský zákoník)



§ 11

(1) V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen „uznávaný elektronický podpis“). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, stanoví ministerstvo prováděcím právním předpisem.

(2) Písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.

(3) Orgán veřejné moci přijímá a odesílá datové zprávy podle odstavce 1 prostřednictvím elektronické podatelny.

Legislativa a důvěra / EU

Směrnice EU o elektronickém podpisu

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

Legislativa a důvěra / ČR

Zákon č.227/2000 Sb.

Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), jak vyplývá z pozdějších změn.

Vyhláška č. 378/2006 Sb.

Vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb

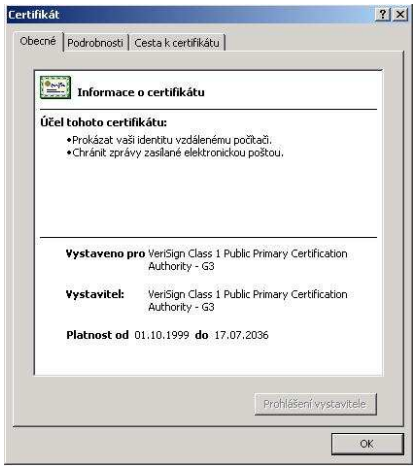
Vyhláška č. 496/2004 Sb.

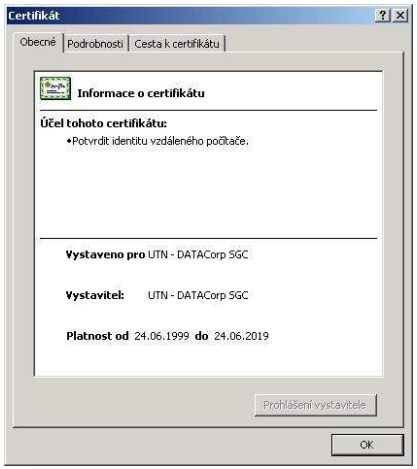
Vyhláška o elektronických podatelnách

NV 495/2004 Sb.

Nařízení vlády, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů

Kterému certifikátu důvěřujete ?





1. **VeriSign Class 1 (v úložišti MS, Mozilla)**
2. **UTN (v úložišti MS, Mozilla)**
3. **I.CA (kvalifikový systémový certifikát akreditovaného poskytovatele)**
4. **SelfSigned (http://adreu.eurid.eu , rozhodování o doménách)**
5. **CA Telefónica O2 CZ**

Různé přístupy k důvěře a ověření digitálních certifikátů resp. elektronických podpisů:

- Legislativní pohled
- Technický pohled / IT pohled
- Laická představa

Definice…

1. **PKI (Public Key Infrastructure)** je kombinace znalostí, soubor představ, dohod, konvencí, speciálního hardware a software, aplikací, které PKI využívají, standardů, norem, prováděcích směrnic, legislativy, osob a subjektů, které používají nebo se spoléhají na příslušné technologie

2. **CA** (Certifiaction Authority) – Certifikační autorita (poskytovatel certifikačních služeb) Poskytovatel certifikačních služeb je subjekt, který vydává certifikáty a vede jejich následnou správu. Zejména zveřejňuje seznamy vydaných certifikátů a seznamy certifikátů, které byly zneplatněny - CRL (Certificate Revocation List).

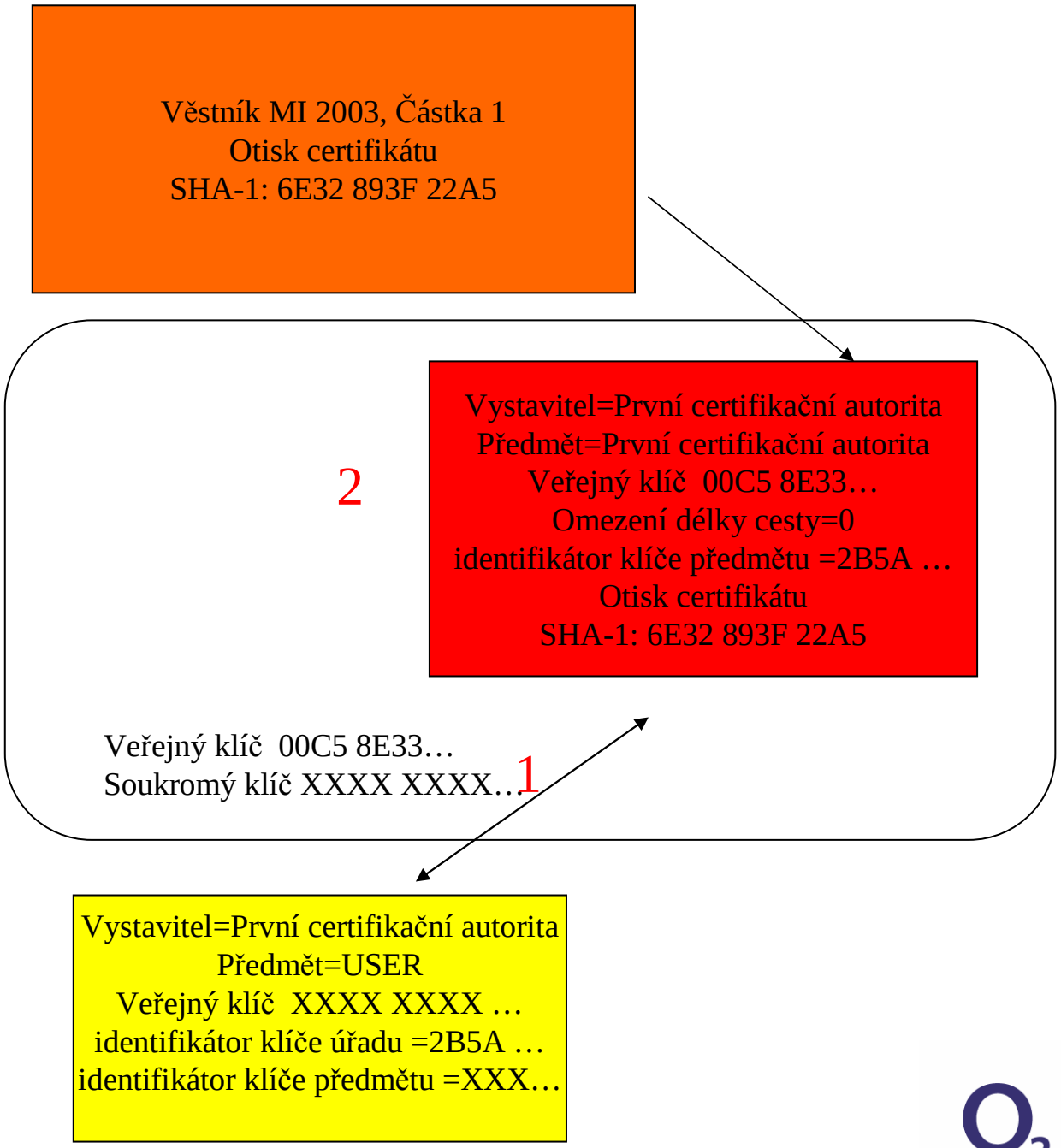
Konstrukce a validace certifikační cesty

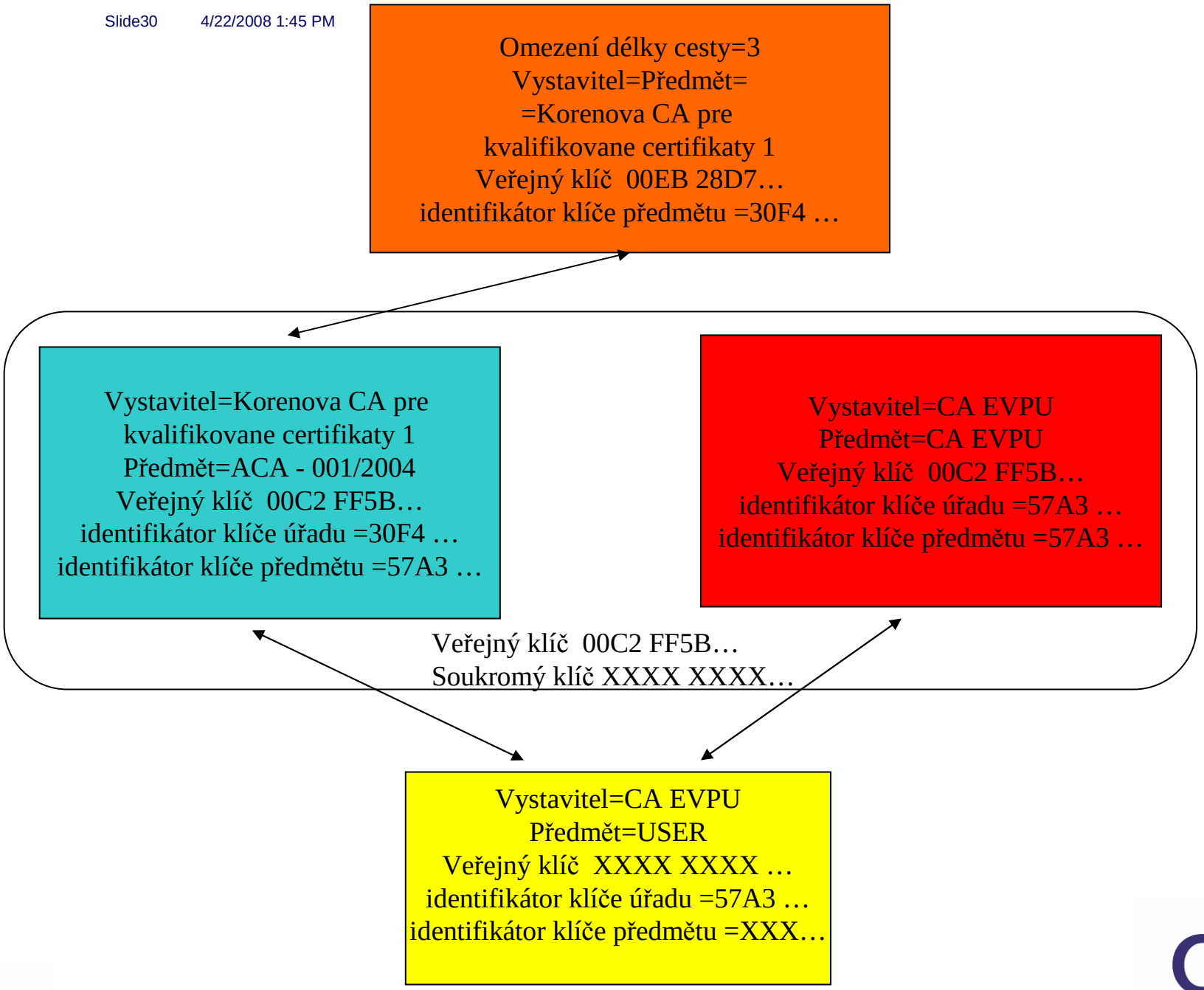
- Konstrukce certifikační cesty mezi ověřovaným certifikátem a důvěryhodným certifikátem CA (singulární bod důvěry) a ověření každého certifikátu v této cestě.
- Oficiální standardy a doporučení pro validaci certifikátu jsou součástí doporučení X.509.4 vydání (ekvivalentní k ISO/IEC 9594-8) a RFC3280.
- 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.

Konstrukce a validace certifikační cesty

- Zřetězení jmen je vyhovující v případě, kdy je zaručena jedinečnost páru veřejného a privátního klíče CA. (☺)
- V budoucnu je nutné počítat s procesy výměny klíčů CA (key rollover), kdy jedinečnost klíčů nebude zaručena a zřetězení jmen nevyhoví.
- Alternativní metodou konstrukce cesty je zřetězení identifikátorů AKID a SKID uvedených v extenzích certifikátů
- AKID (Authority Key Identifier) je jednoznačný identifikátor veřejného klíče CA (vystavitele certifikátu)
- SKID (Subject Key Identifier) je jednoznačný identifikátor certifikátu, obsahující veřejný klíč vlastníka certifikátu.
- 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).

1) Subject=Issuer
2) Root certifikát
   (Subject=Issuer)
3) Otisk certifikátu

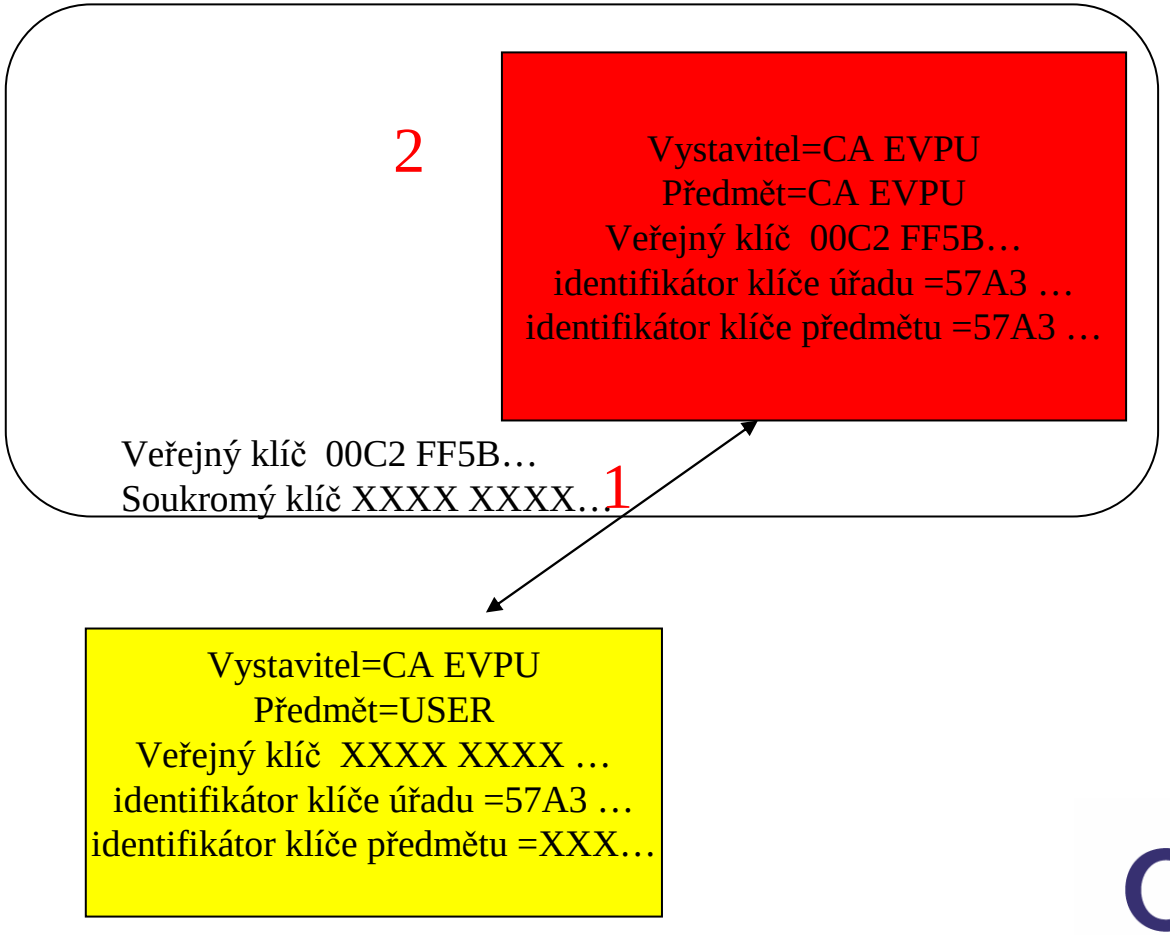


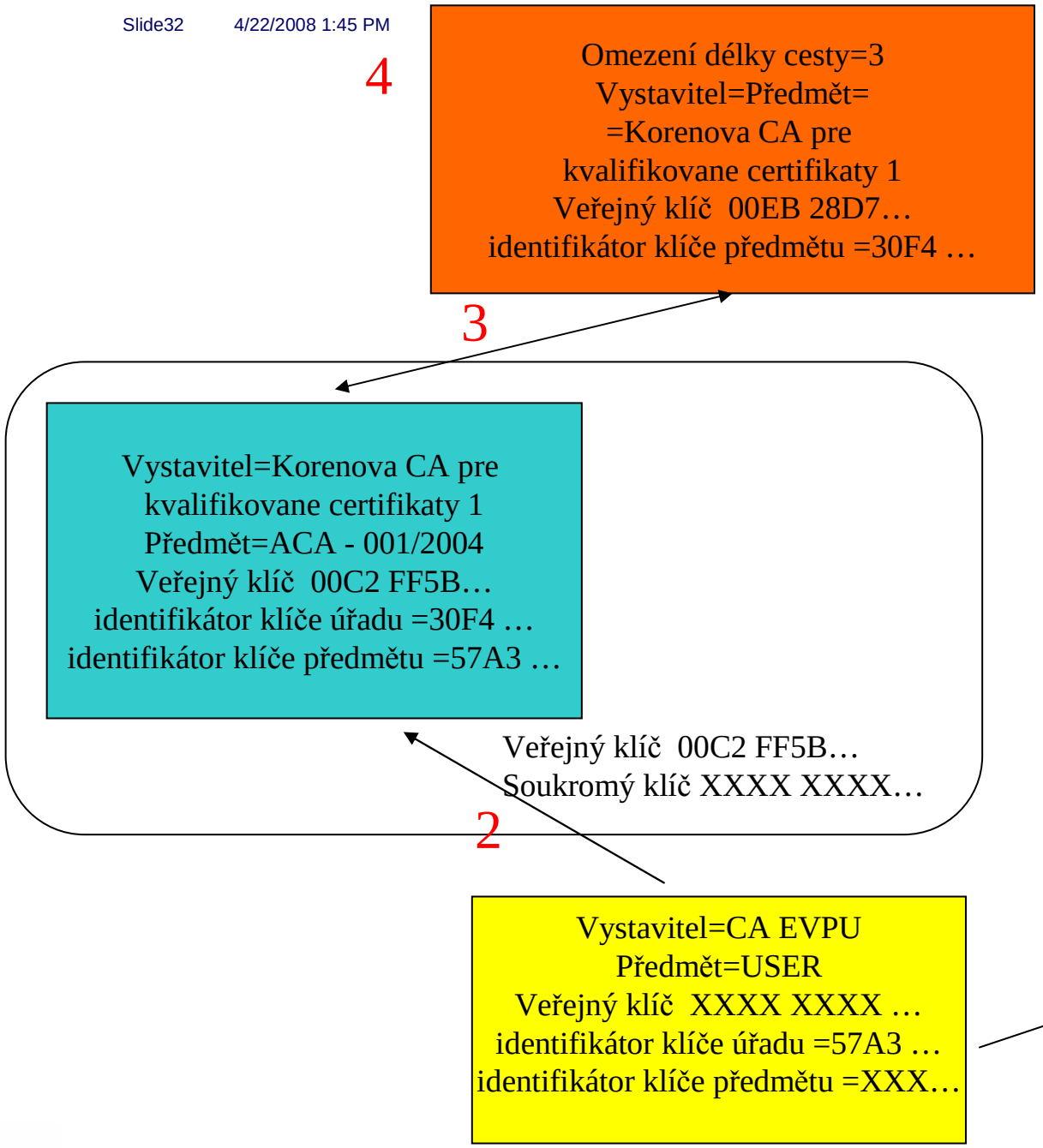

Omezení délky cesty=3
Vystavitel=Předmět=
=Korenova CA pre
kvalifikovane certifikaty 1
Veřejný klíč 00EB 28D7…
identifikátor klíče předmětu =30F4 …
Vystavitel=Korenova CA pre
kvalifikovane certifikaty 1
Předmět=ACA - 001/2004
Veřejný klíč 00C2 FF5B…
identifikátor klíče úřadu =30F4 …
identifikátor klíče předmětu =57A3 …
Vystavitel=CA EVPU
Předmět=CA EVPU
Veřejný klíč 00C2 FF5B…
identifikátor klíče úřadu =57A3 …
identifikátor klíče předmětu =57A3 …
Veřejný klíč 00C2 FF5B…
Soukromý klíč XXXX XXXX…
Vystavitel=CA EVPU
Předmět=USER
Veřejný klíč XXXX XXXX …
identifikátor klíče úřadu =57A3 …
identifikátor klíče předmětu =XXX…

Omezení délky cesty=3
Vystavitel=Předmět=
=Korenova CA pre
kvalifikovane certifikaty 1
Veřejný klíč 00EB 28D7…
identifikátor klíče předmětu =30F4 …

1) Subject=Issuer
2) Root certifikát

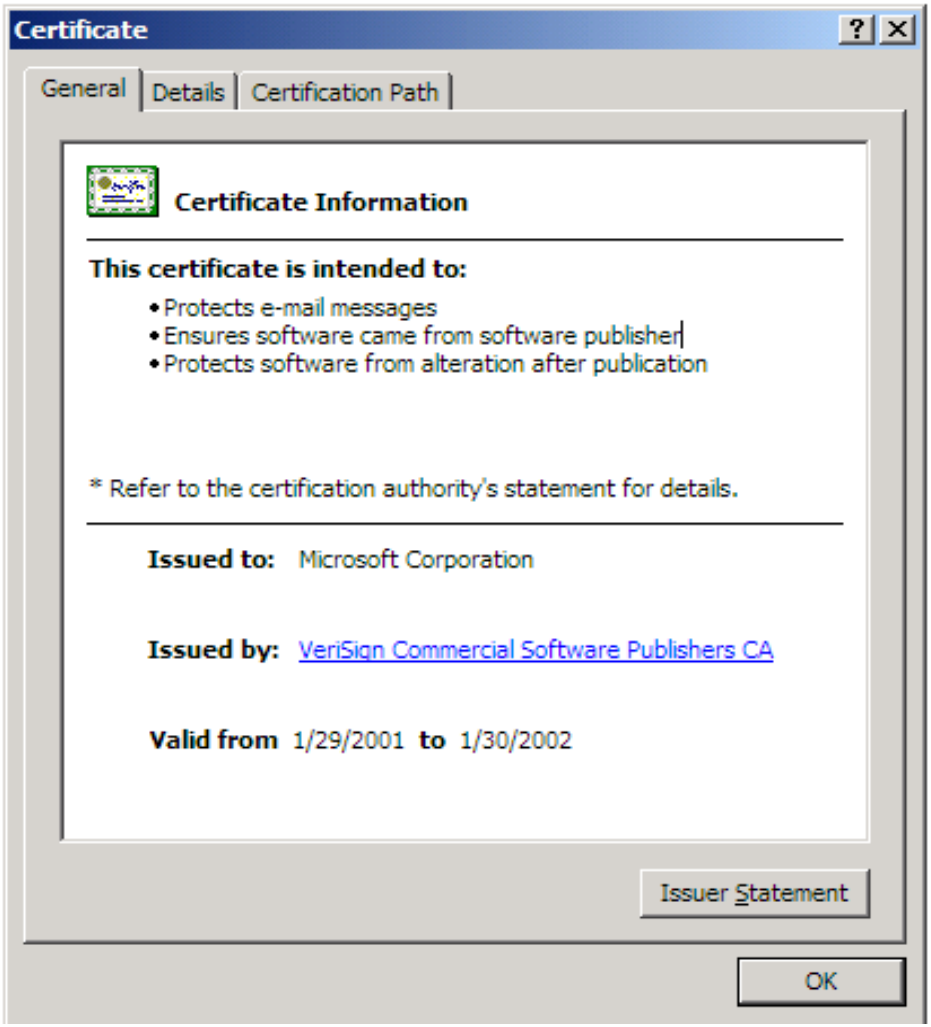
(Subject=Issuer)





1) Issuer= ? (certifikát nenalezen)
2) Klíč úřadu= klíč předmětu (AKID=SKID)
3) Subject=Issuer
4) Root certifikát (Subject=Issuer)
5) Délka cesty ?

Technické prosazení důvěry



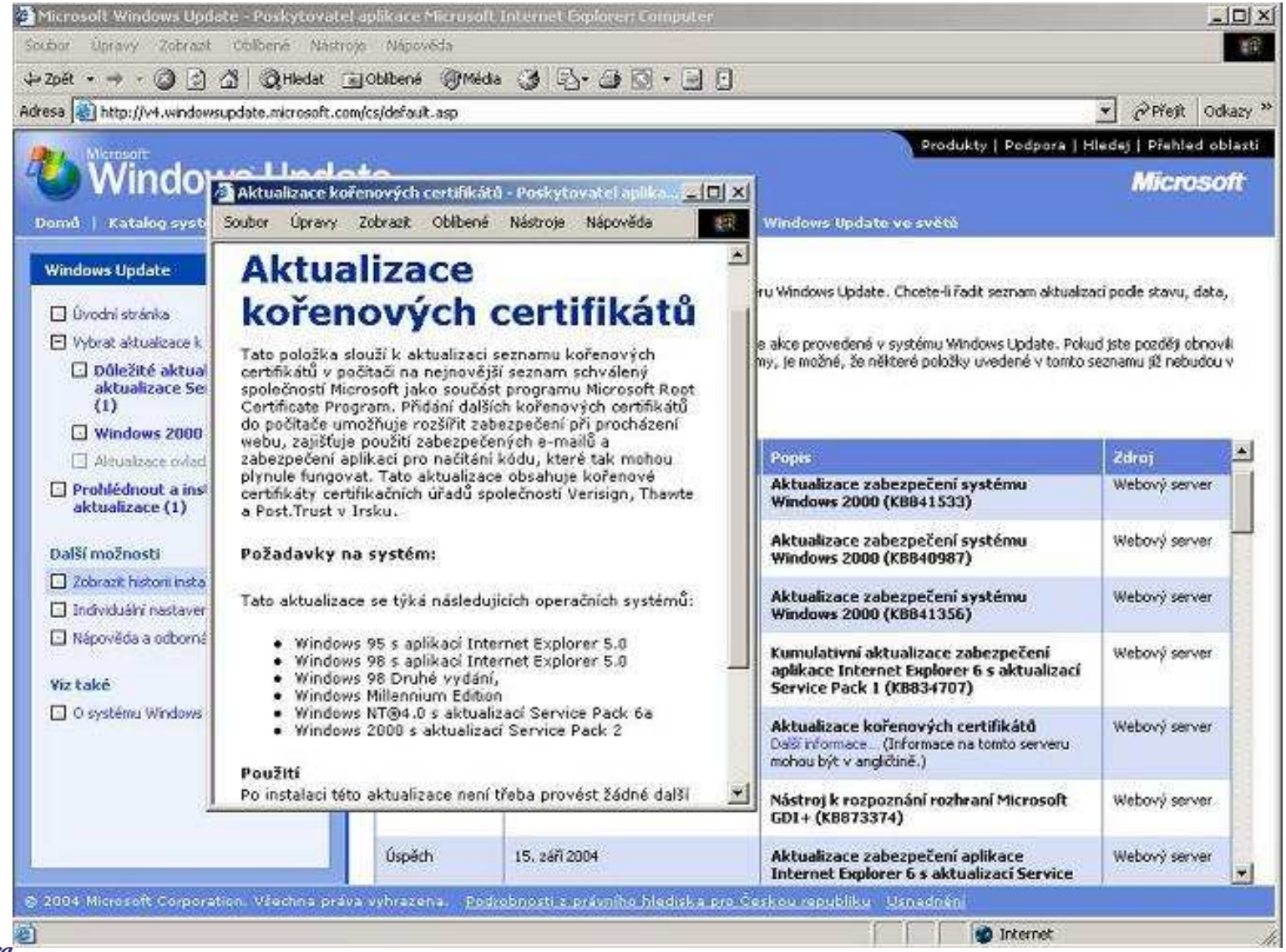
Jenže ...

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.

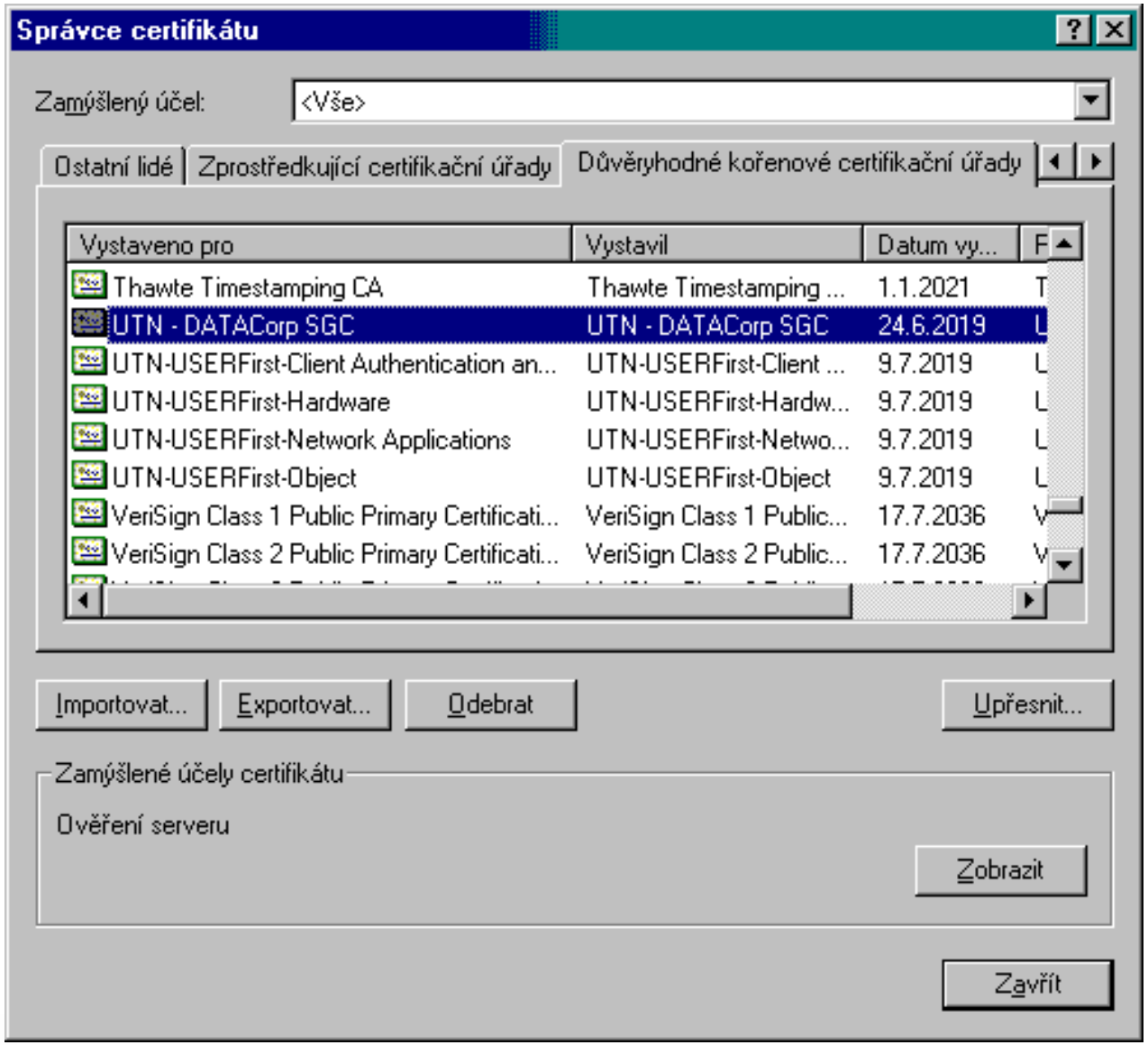
Technické prosazení důvěry



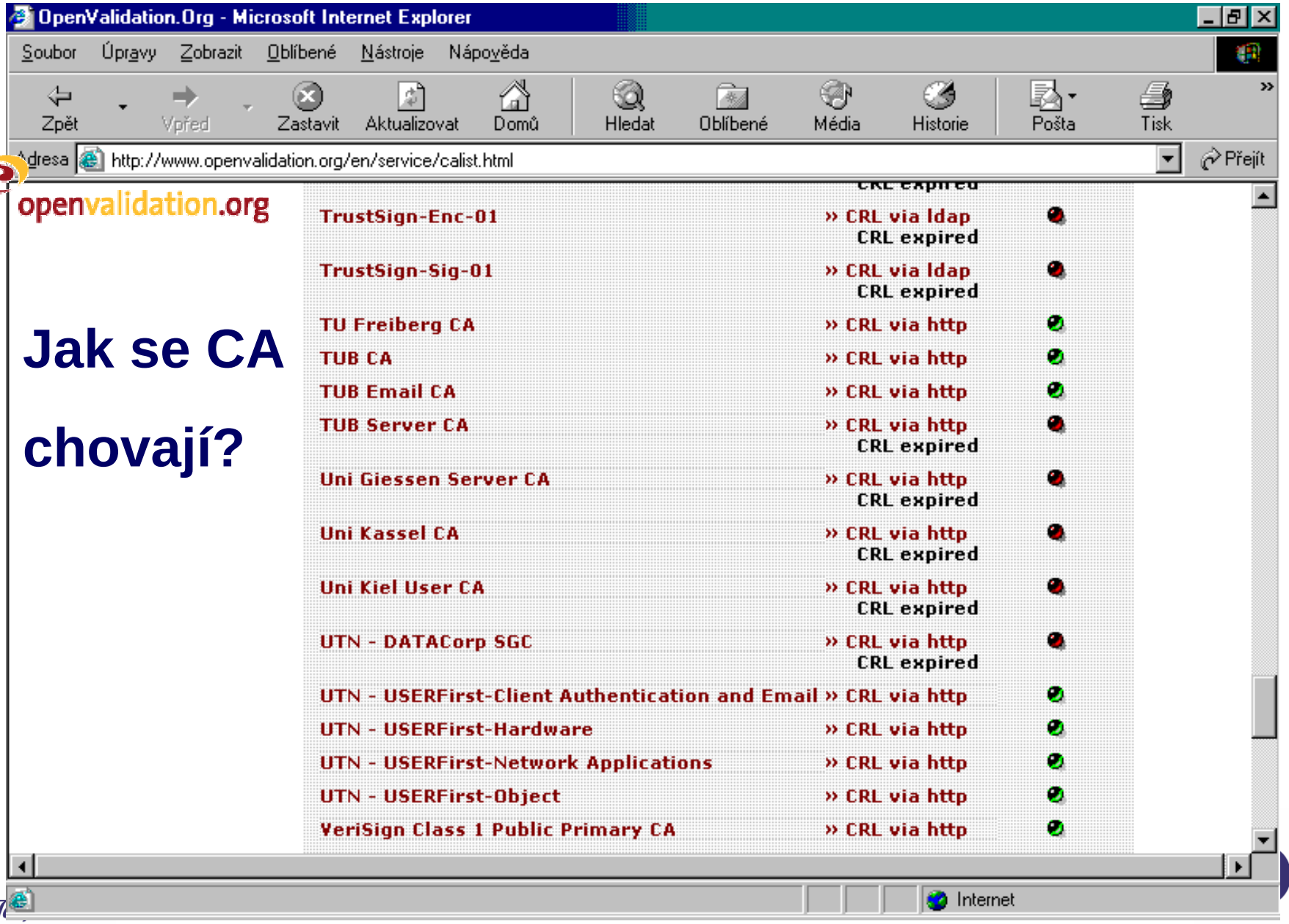
Telefónica

O2

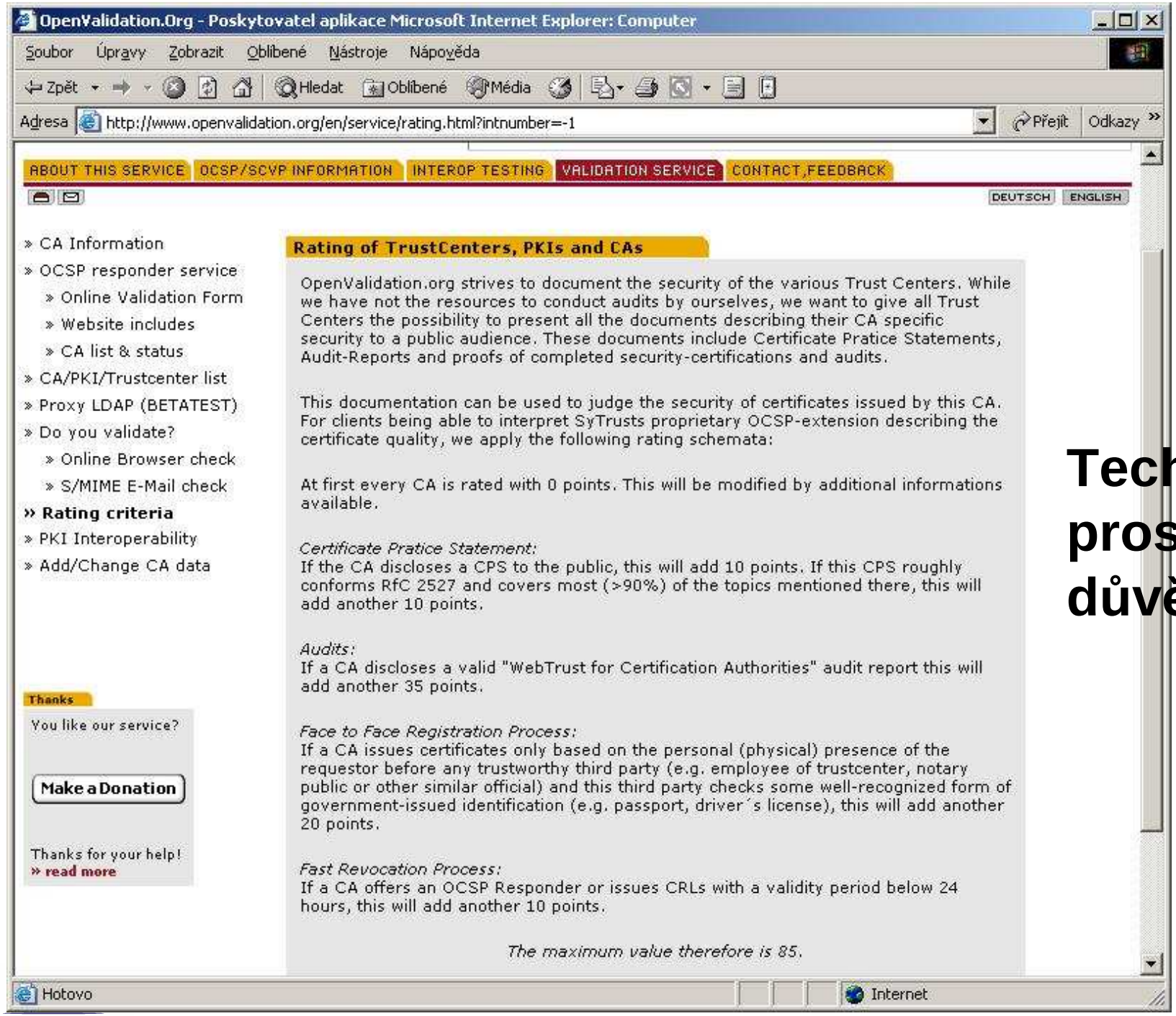
Technické prosazení důvěry



http://www.openvalidation.org/en/service/calist.html

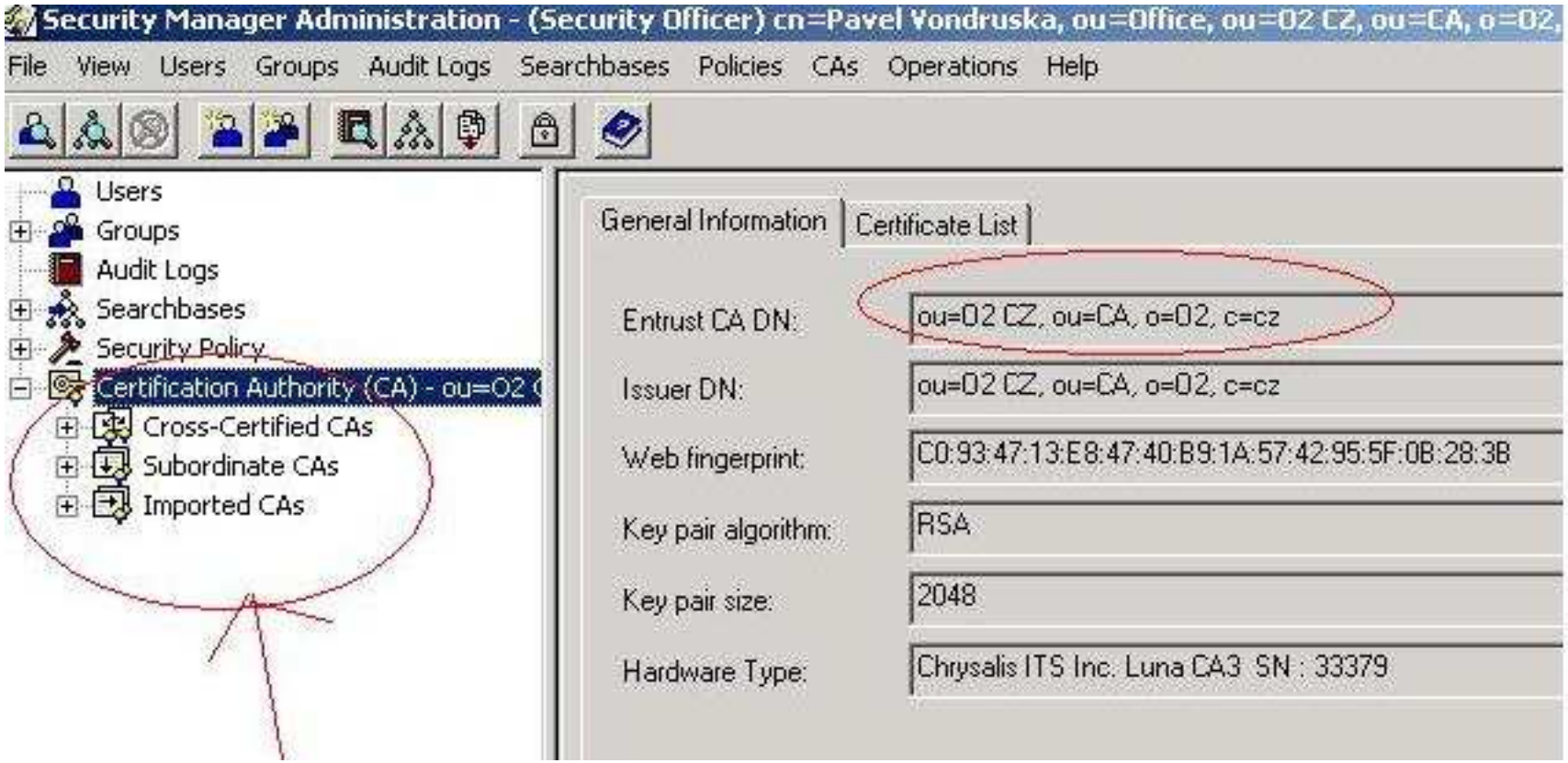


Jak se CA chovají?



Technické prosazení důvěry

Technické prosazení důvěry



Problém při ověřování certifikátů vydaných různými CA (v uzavřených systémech) by neměl být řešen na úrovni uživatelů (viz předchozí případ), ale na úrovni PKI (např. správců CA).

Technické prosazení důvěry - CRL

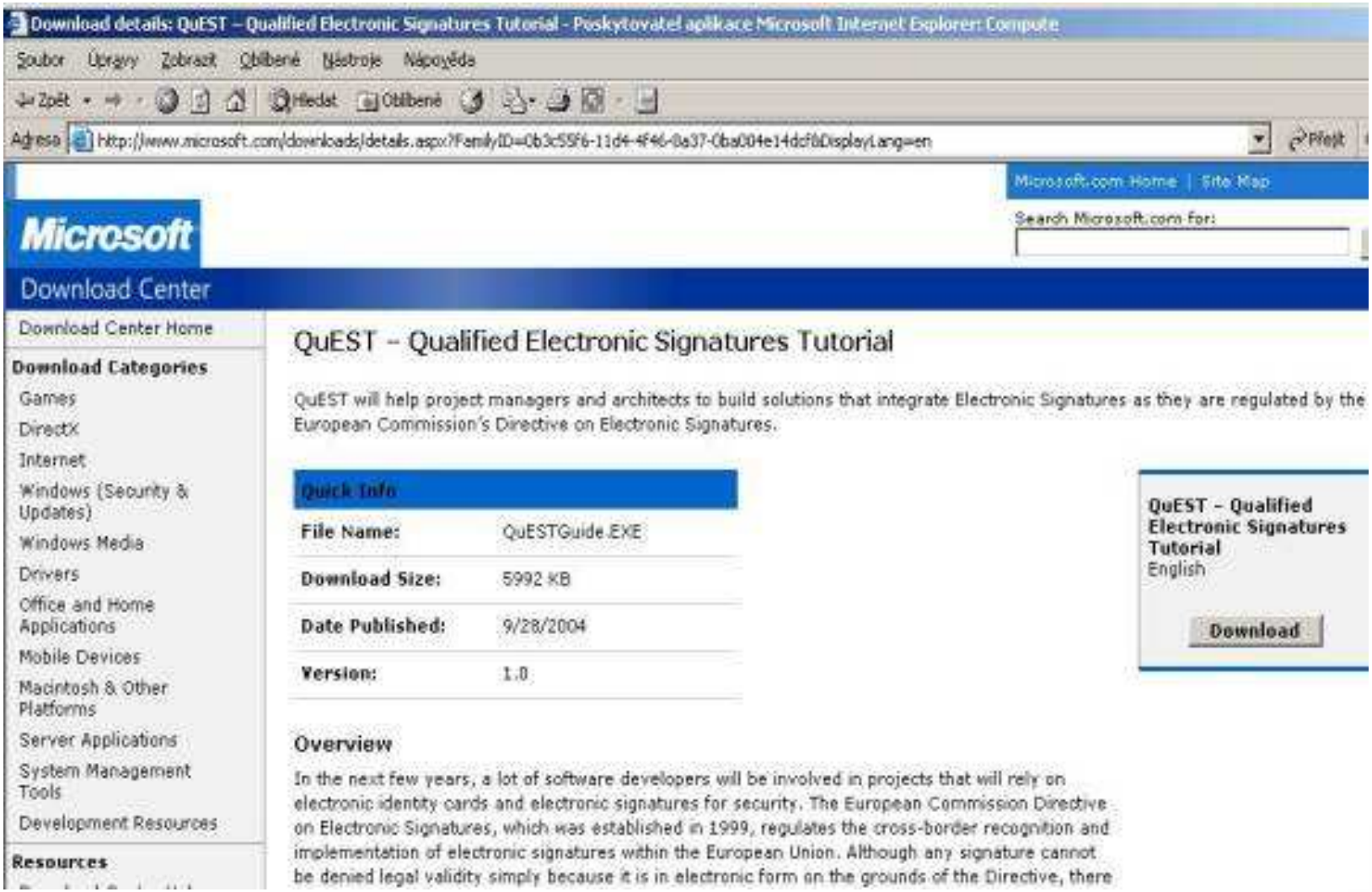
Jak je to se seznamy certifikátů, které byly zneplatněny?
Stahují se automaticky?
Pokud manuálně jak a kde?

CRL Certifikační autority O2 CZ lze stáhnout z adresy :
http://ca.cz.o2.com/crl/CA-CRL.crl
Samotná instalace je již velice jednoduchá. Nad uloženým souborem s CRL stiskněte pravé tlačítko myši a zvolte příkaz Nainstalovat seznam CRL.

Telefónica

O2

Je MS důvěryhodné prostředí i pro QC ?



REALITA

ECRYPT

(European Network of Excellence in Cryptology)

Table 7.2: Key-size Equivalence.

Security (bits)	RSA	DLOG		EC
		field size	subfield	
56	512	512	112	112
64	768	768	128	128
80	1024	1024	160	160
112	2048	2048	224	224
128	3072	3072	256	256
160	5120	5120	320	320
192	8192	8192	384	384
256	14720	14720	512	512

ECRYPT Yearly Report on Algorithms and Keysizes (2004)

D.SPA.10 (1.3.2005)

Telefónica

O2

Realita – 4.2.2007

Pavel Vondruška
Crypto-World
http://crypto-world.info
mobil +420 602 560 963
