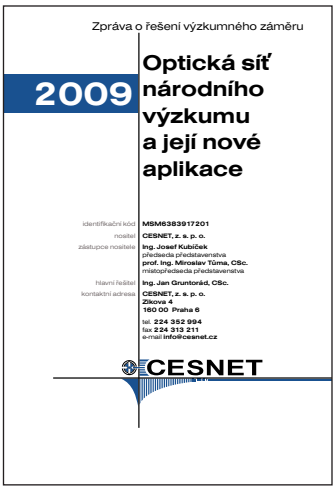
http://www.cesnet.cz/doc/datagram/

Datagram

zpravodaj sdružení CESNET číslo 22 březen 2010

Rok 2009 obhájen


Zpráva o řešení výzkumného záměru

2009

Optická síť národního výzkumu a její nové aplikace

identifikační kód: MSM6383917201
nositel: CESNET, z. s. p. o.
zástupce nositele: Ing. Josef Kubíček, předseda představenstva; prof. Ing. Miroslav Tůma, CSc., místopředseda představenstva
hlavní řešitel: Ing. Jan Gruntorád, CSc.
kontaktní adresa: CESNET, z. s. p. o., Zikova 4, 160 00 Praha 6, tel. 224 352 994, fax 224 313 211, e-mail: info@cesnet.cz

CESNET

Sdružení CESNET od roku 2004 řeší výzkumný záměr *Optická síť národního výzkumu a její nové aplikace*, v jehož rámci vyvíjí, ověřuje a podporuje nové přenosové technologie, síťové služby a aplikace. Jejich nasazení do národní sítě CESNET2 představuje klíčový prvek pro její rozvoj.

Tento výzkumný záměr je podle standardních pravidel MŠMT oponován v ročních intervalech. Oponentura výsledků roku 2009 proběhla 5. února v sídle sdružení. Podkladem pro ni byla vedle dokumentů požadovaných ministerstvem i rozsáhlá roční zpráva o řešení výzkumného záměru, která je veřejně k dispozici na adrese

http://www.cesnet.cz/doc/2009/zprava/

Více než dvousetstránkový dokument shrnuje naše nejvýznamnější aktivity a výsledky dosažené v loňském roce. Dokumentaci zhodnotila trojice oponentů:

- Ing. Michal Dočekal – GTS Novera
- prof. RNDr. Jan Slovák, DrSc. – MU
- Ing. Tibor Weis – CIT TU Zvolen

Naši činnost posuzovala oponentní rada ve složení:

- Ing. Vít Kavan, CSc. – MŠMT (předseda)
- RNDr. Jaroslav Bobovský – BESET, s. r. o.
- prof. Ing. Pavol Horváth, CSc. – STU Bratislava
- Ing. Vladimír Rudolf – ZČU v Plzni
- Ing. Pavel Zima – Seznam.cz, a. s.

Závěry, k nimž rada dospěla, navazují na úspěšné řešení výzkumného záměru v předchozích letech. Ocenila dosažené výsledky, které hodnotí jako vynikající, mezinárodního významu. Pro rok 2010 doporučila soustředit se na dokončení záměru. Zápis z oponentního řízení je také zveřejněn:

http://www.cesnet.cz/doc/2009/oponentura/

Skupina pro IPv6

Internet bude v nejbližší době čelit nemalému problému – vyčerpání dostupných adres. V současné době již zbývá méně než 10 % adresního prostoru a tempo jeho spotřeby stále roste. Aktuální prognóza, kterou na svém webu *ipv4.potaroo.net* průběžně udržuje Geoff Huston, předpovídá vyčerpání v říjnu 2012.

Konkrétní datum kolísá v závislosti na aktuální rychlosti přidělování adres, nicméně je téměř jisté, že ve druhé polovině roku 2012 skutečně dojde k přidělení posledních volných bloků. Získat poté IP adresu bude pro organizace nově připojované k Internetu čím dál těžší.

Jako řešení tohoto problému vznikla nová verze základního internetového protokolu – *Internet Protocol version 6 (IPv6)*. Nabízí mnohem větší adresní prostor a řadu zajímavých vlastností. Bohužel je nekompatibilní se současným internetovým protokolem, a proto se do praxe prosazuje jen velmi pomalu. Pro komerční poskytovatele připojení a služeb je jeho nasazení spíše nevýhodné, a proto je odkládají.

Pro organizace připojené k CESNET2 pravděpodobně nebude problém vyčerpání příliš bolestný. Své adresy většinou získaly v poměrně raných dobách rozvoje Internetu a často jich mají dostatek. Na druhé straně jednou z úloh sítí pro vědu, výzkum a vzdělávání, které nejsou svázány komerčními zákonitostmi, je podporovat nasazování moderních technologií a služeb.

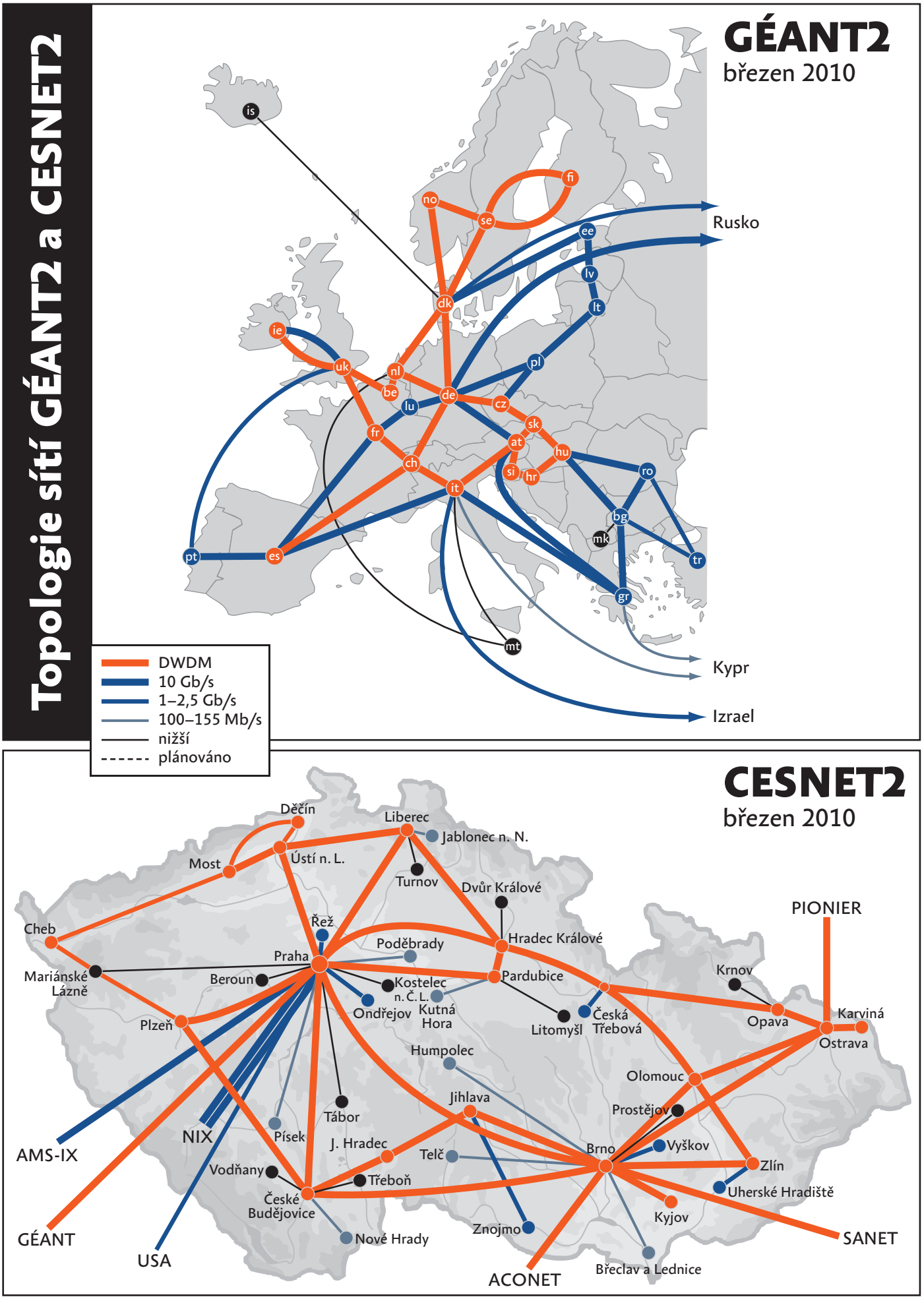
CESNET proto věnuje IPv6 značnou pozornost. První experimenty s novým protokolem jsme zahájili v roce 1999 a od roku 2004 jej v páteřní síti podporujeme na produkční úrovni, zcela srovnatelné s IPv4.

Zatím se však nedaří rozšířit jej i do koncových sítí členů sdružení a dalších připojených organizací. Abychom podpořili jeho rozvoj, rozhodli jsme se založit *pracovní skupinu pro IPv6*. Členství v ní je zcela dobrovolné, vychází jen ze zájmu o danou problematiku. Skupina slouží k výměně zkušeností s nasazením IPv6, bude pořádat semináře a připravovat dokumenty popisující osvědčené postupy v této oblasti.

Budeme rádi, když se správci sítí připojených k CESNET2 zapojí v co největším počtu.

http://www.cesnet.cz/ipv6/

Topologie sítí GÉANT2 a CESNET2



Multimediální přenosy ve špičkové kvalitě

Jednou z oblastí, kterým se CESNET dlouhodobě věnuje, jsou videokonferenční nástroje a prostředky pro vzdálenou spolupráci distribuovaných týmů. Tato oblast je velmi široká a sahá od personálních, nejčastěji softwarových nástrojů (Skype, Windows Live Messenger a podobné), které si vystačí s datovými toky v řádu desítek až stovek kilobitů za sekundu a jsou dnes poměrně běžně užívány, až po špičkové prostředky, jejichž vysoká obrazová kvalita a minimální zpoždění vyžadují gigabitové přenosové rychlosti. Právě v této oblasti se nám daří dosahovat zajímavých výsledků.

Špičkové přenosy multimediálních dat jsou využívány zejména v oblastech náročných na kvalitu obrazu, kde případné zkreslení, ztráta detailu nebo zpoždění přesahující zlomky sekund způsobí, že technologie bude pro danou aplikaci nepoužitelná. Během posledních měsíců jsme prokázali, že i velmi náročným oborům máme co nabídnout. Zvláštní pozornost si zaslouží především dvě oblasti:

Videopřenosy pro lékaře

Konferenci očních chirurgů *Live+Video Surgery* lze již považovat za tradičně podporovanou – na zajištění obrazových přenosů pro ni jsme spolupracovali již čtvrtým rokem. Letošní ročník se konal 22. a 23. ledna a jeho součástí byly živé přenosy operací ze sálů Ústřední vojenské nemocnice Praha a z očních klinik fakultních nemocnic v Hradci Králové, Olomouci a Ostravě. Diváci v kongresovém sále tak měli k dispozici pohled do operačního pole i komentář operatéra.

Technickou stránku přenosů a podporu pro mimopražské kliniky zajišťovali odborníci ze společnosti CNC Praha. CESNET poskytl technologii vzájemného propojení více účastníků umožňující současný přenos z několika sálů a vzájemnou interakci jednotlivých týmů. Přenosy probíhaly v HD kvalitě v závislosti na schopnostech operačních kamer. Jako komunikační infrastruktura sloužila síť CESNET2.

Počátkem března jsme pak živě přenášeli operaci štítné žlázy pro účastníky mezinárodního lékařského fóra *Střešovické jaro 2010*. Přenos mezi Otorhinolaringologickou klinikou 3. LF UK a Ústřední vojenskou nemocnicí zahrnoval několik HD kanálů a umožňoval i diskusi mezi auditoriem a operačním týmem.

CineGrid 2009

Lékařské přenosy zmiňované v předchozí části mají vysoké požadavky na kvalitu obrazu, vůči zpoždění jsou však poměrně odolné. Řádově náročnější byla ukázka, kterou jsme ve spolupráci se společností Cinepost připravili pro *4th CineGrid Workshop* pořádaný v prosinci 2009 na University of California v San Diegu.

CineGrid je mezinárodní nezisková organizace se sídlem v Kalifornii, jejímž cílem je budovat mezioborovou komunitu zaměřenou na výzkum, vývoj a demonstrace síťových nástrojů pro výrobu, využívání a výměnu multimédií v mimořádně vysoké kvalitě. Vzhledem k datovým objemům, které takové aplikace vyžadují, se orientuje především na optické sítě.

Pro její poslední workshop jsme připravili ukázku týmové postprodukce (konkrétně barevné korekce) videa. Spočívala v provádění barevných úprav videomateriálu na dálku, kdy se úložiště videomateriálu, operátor softwaru pro správu barev a odborník posuzující výsledek operace nacházejí v různých lokalitách. V tomto případě byly vzdálenosti extrémní, protože postprodukce byla prováděna v Barrandově a konzultována ze San Diega. Datové toky procházely sítěmi na vzdálenost přesahující 10 tisíc km. Do přenosu byly zapojeny sítě PragueMediaNet, CzechLight, CESNET2, StarLight a C-wave, které jsou součástí globálního prostředí GLIF (Global Lambda Intergated Facility).

Zpracovával se signál ve špičkové kvalitě 4K, tedy v rozlišení 4096×2160 bodů – proti HD více než čtyřnásobek. Vzhledem k interaktivnímu charakteru práce a k nevyhnutelnému zpoždění danému vzdáleností bylo neakceptovatelné zpomalovat odezvy systému komprimačními algoritmy. Data proto byla přenášena v nekomprimované podobě, která si vyžádala datový tok přibližně 6 Gb/s. Jako přenosová technologie posloužil desetigigabitový Ethernet.

Platforma MVTP-4k

Jedním ze zařízení využitých při demonstraci byla i námi vyvinutá platforma *MVTP-4k (Modular Video Transfer Platform 4k)* pro přenos videosignálu počítačovou sítí. Zařízení je založeno na technologii programovatelného hardwaru a umožňuje přenos několika nezávislých videosignálů po desetigigabitovém Ethernetu. Podporuje signály 4k (4096×2160 nebo 3840×2160), 2k (2048×1080) i HD (1920×1080).

Předvedená ukázka vzbudila mezi účastníky workshopu značný zájem a otevřela nám nové kontakty. Naše spolupráce s partnery v oblasti zpracování filmů a multimédií špičkové kvality nepochybně bude pokračovat i v budoucnosti.

Serverové a osobní certifikáty TERENA

S rostoucím počtem služeb využívajících Internet pro komunikaci s uživatelem roste i význam mechanismů chránících přenášená data. Řada z nich využívá metody asymetrické kryptografie, kdy jeden klíč je soukromý a nikdy neopustí svého vlastníka, zatímco druhý, veřejný klíč je volně distribuován, aby si kdokoli mohl ověřit data zašifrovaná jeho soukromým protipólem. Jak ale ověřit, že daný veřejný klíč skutečně patří určité osobě či serveru?

Řešením jsou certifikační autority – instituce, které ověří a svým digitálním podpisem potvrdí vztah vlastníka k určitým technickým údajům, jako je adresa či veřejný klíč. Toto ověření je uloženo ve formě certifikátu, jímž uživatel či server může prokázat svou totožnost.

Klientský program potřebuje k ověření certifikátu veřejný klíč vydávající autority, aby mohl zkontrolovat její digitální podpis. Klíče nejvýznamnějších světových certifikačních autorit jsou obsaženy přímo v základní distribuci běžných programů – webových prohlížečů či poštovních agentů – a jejich certifikáty díky tomu mohou být přímo ověřeny.

Jiné certifikační autority je třeba nejprve nainstalovat, což snižuje jejich užitečnost. Dokud uživatel neprovede instalaci, klient zachází s certifikátem jako s neplatným a signalizuje chybu. Častý výskyt neopodstatněných varování uživatele obtěžuje a ti si zvyknou je bez většího zkoumání potvrzovat. Proto je velmi žádoucí používat certifikáty vydané některou ze standardně podporovaných autorit.

CESNET je zapojen již několik let do programu *TERENA Certificate Service (TCS*, dříve *SCS)*, který nám umožňuje takové certifikáty vydávat. V roce 2009 došlo ke změně poskytovatele této služby, jímž se stala společnost *Comodo*. V návaznosti na tento krok se rozšířila i nabídka certifikátů, které lze získat.

Serverové certifikáty

Serverové certifikáty jsou využívány zejména při šifrované komunikaci s webovými servery. Ověřují doménové jméno a IP adresu cílového serveru a dávají uživateli jistotu, že své heslo či jiné důvěrné údaje nezadává na podvržený server. Členům sdružení, kteří provozují zabezpečené webové aplikace, rozhodně doporučujeme opatřit příslušné servery TCS certifikátem.

Tento typ certifikátů vydáváme již od roku 2006. Do podzimu 2009 byly tyto certifikáty garantovány společností *Globalsign*, během přechodného období na konci roku 2009 byly postupně nahrazeny certifikáty nového poskytovatele služby, společnosti *Comodo*.

Žádost o nový certifikát se podává na adrese

https://tcs.cesnet.cz/

Může ji podat každý správce serveru se jménem v některé z registrovaných domén. Jejich seznam, stejně jako seznam institucí zapojených do programu TCS, najdete na zmíněné adrese. Každá zúčastněná organizace jmenuje své správce, kteří schvalují žádosti pro servery z domén příslušejících dané instituci. Doporučujeme žadatelům, aby svůj záměr konzultovali s lokálními správci ještě před podáním žádosti – poradí vám s hodnotami jednotlivých parametrů a vyřízení pak bude rychlejší.

Osobní certifikáty

Novinku v našich certifikačních službách představují osobní certifikáty, jež usnadní uživatelům přístup k síťovým službám. K dispozici jsou dva typy:

- *TCS Personal Certificate* představuje základní osobní certifikát, který ověřuje identitu konkrétního uživatele. Můžete jej využít například k zabezpečení elektronické pošty nebo pro přístup k některým webům.
- *TCS eScience Personal Certificate* je určen zejména gridovým uživatelům. Jelikož je tato služba akreditována u mezinárodní organizace *EUGridPMA*, jsou její certifikáty akceptovány všemi významnými gridovými infrastrukturami.

Při implementaci jsme se snažili o maximální uživatelskou přívětivost. Žádost o osobní certifikát si podává každý sám na adrese

https://tcs-p.cesnet.cz/

Žádost o TCS osobní certifikát může podat každý uživatel s účtem vedeným některým členem federace *eduID.cz* (jeho domovská organizace musí s vydáním certifikátu souhlasit). Jméno, adresa pro elektronickou poštu a další osobní údaje vkládané do certifikátu dodává poskytovatel identity, nemusíte je tedy zadávat. Před vlastním vydáním certifikátu systém vyžaduje opakované ověření identity, aby se potvrdila vaše osobní přítomnost u prohlížeče.

Výsledkem procedury je vytvoření osobního certifikátu a jeho instalace do webového prohlížeče. Elektronickou poštou vám dorazí potvrzení s odkazem na stránku, kde se můžete k certifikátu vrátit, zobrazit jej či zrušit (revokovat) jeho platnost.

Instalace certifikátu do prohlížeče a programu pro elektronickou poštu se liší v závislosti na tom, co používáte. Programy firmy Microsoft (Explorer + Outlook) mají společné úložiště certifikátů. Jakmile jej nainstalujete do MSIE, bude certifikát k dispozici i v poštovním programu. Naproti tomu produkty z rodiny Mozilla mají svá vlastní nezávislá úložiště. Po instalaci do Firefoxu musíte certifikát uložit (zálohovat) a tento uložený soubor pak instalovat do Thunderbirdu.

Nainstalovaný certifikát si v každém případě zálohujte, raději na více než jedno médium. Během vytváření zálohy také určíte heslo, jímž bude později chráněn přístup k němu a veškeré operace s ním (zejména instalace do dalších programů či systémů). Při ukládání souboru doporučujeme použít ve jméně příponu *.p12*, obvyklou pro certifikáty v použitém formátu PKCS12. Mějte na paměti, že certifikát má omezenou platnost, po jejímž vypršení jej již nelze používat.