

Certifikační autorita CESNETu

Cílem certifikační autority je poskytnout základní kamen pro důvěru uživatelů. Představte si, že například potřebujete poslat důvěrné informace Břetislavu Žvýkačkovi. Někým způsobem zjistíte, že snad má adresu *bzvykacka@kdesi.cz* a získáte i veřejný klíč, jímž můžete poštu pro něj zašifrovat. Jak si ale můžete být jisti, že zmíněná adresa a klíč patří skutečně Břetislavu Žvýkačkovi a ne někomu, kdo se za něj vydává?

Tento problém řeší certifikační autorita. Vydá certifikát obsahující veřejný klíč a adresu a další informace o dotčeném, jež jsou opatřeny jejím digitálním podpisem. Pokud dotčené certifikační autoritě důvěřujete a máte prostředky k ověření jejího elektronického podpisu, poskytne vám certifikát důvěryhodné informace o dané osobě (serveru, instituci apod.).

Důvěra uživatelů je pro funkci certifikační autority klíčová. Proto je třeba velmi přesně popsat pravidla chování autority a postupy pro jejich realizaci. To zajišťují dva základní dokumenty: *Certifikační politika* definuje pravidla, která certifikační autorita musí dodržovat. *Prováděcí předpis* pak stanoví konkrétní postupy při práci certifikační autority, které uvedou do praxe pravidla předepsaná politikou. Veškeré informace o CESNET CA, včetně uvedených dokumentů, najdete na

<http://www.cesnet.cz/cesnet-ca/>

CESNET CA

Certifikační úřad *CESNET CA* vznikl v roce 2001 pro potřeby naší účasti v evropském projektu *DataGrid*. Postupně rozšiřoval své služby a v současné se otevírá i členům sdružení.

V současné době nabízí *CESNET CA* následující služby:

- *Osobní certifikáty* - slouží pro autentizaci přístupu k neveřejným WWW serverům a pro elektronickou poštu podle standardu S/MIME. Osobní certifikáty zde mohou získat jen osoby přímo spolupracující s CESNETem (zaměstnanci, řešitelé projektů) a správci systémů a služeb provozovaných členy sdružení.
- *Certifikáty serverů a služeb* - slouží k autentizaci počítačů a aplikací. Používají se nejčastěji ke chráněné WWW komunikaci, s níž se můžete setkat v objednávkových systémech, registraci předmětů a podobně. Certifikáty se vydávají pro servery a služby provozované CESNETem či některým z jeho členů, nebo institucí spolupracujících na výzkumných projektech sdružení.
- *Certifikace dalších úřadů* - které si členové sdružení zřídí pro vlastní potřebu. Není v silách *CESNET CA* poskytovat

plošně osobní certifikáty studentům či zaměstnancům vysokých škol. K tomuto účelu si jednotlivé instituce musí vytvořit vlastní úřady - registrační či certifikační. *Registrační úřad* je jen prodlouženou rukou *CESNET CA*. Zajišťuje registraci uživatelů, ale certifikáty vydává *CESNET CA*. Naproti tomu *certifikační úřad* je zcela samostatnou institucí, která pouze používá metody a postupy, které jsou v souladu s pravidly *CESNET CA*.

Pokud se některý z členů rozhodne založit vlastní úřad, nemusí bezpodmínečně usilovat o jeho certifikaci ze strany *CESNET CA*. Nicméně certifikace úřadu přinese několik významných výhod:

- Díky řetězení důvěry budou certifikátům vydávaným takovou autoritou automaticky důvěřovat všichni, kdo důvěřují *CESNET CA*.
- Není třeba stavět vše na zelené louce. Řada postupů i softwarových řešení je připravena a stačí je jen převzít.
- Získáte přístup k rozsáhlému znalostnímu zázemí. Bude mít k dispozici řadu partnerů pro sdílení zkušeností či řešení problémů.

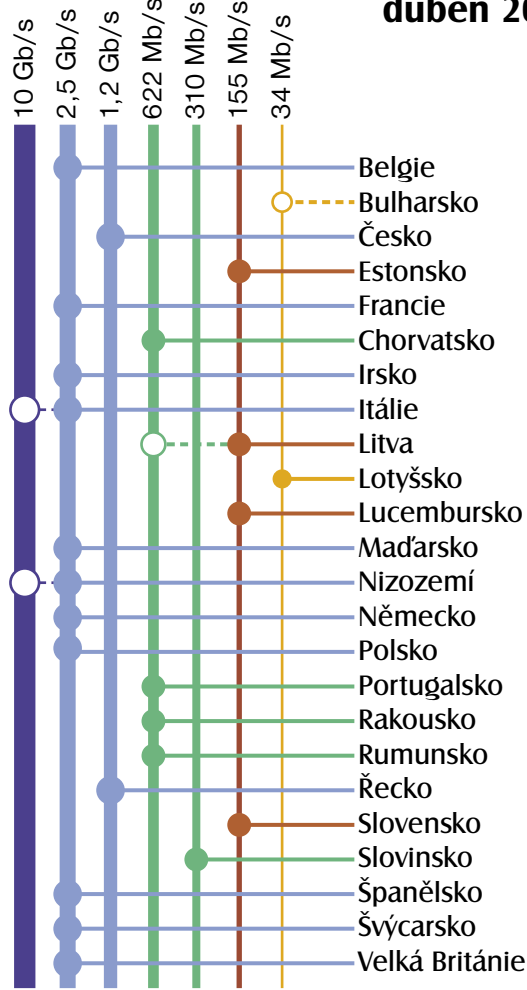
Dopady pro uživatele

Co přinese existence *CESNET CA* a jí vydávaných certifikátů uživatelům? Především je třeba přiznat, že naše autorita není státem uznanou certifikační autoritou a její certifikáty proto nelze použít například pro komunikaci se státní správou. Proces uznání autority je velmi komplikovaný a nákladný a v současnosti není dostatečný důvod, proč jej podstupovat.

Certifikáty *CESNET CA* lze využít pro zabezpečení elektronické komunikace v rámci sdružení a jeho členů. Jakmile si uživatel instaluje hlavní certifikát autority, může ověřovat certifikáty jí vydané. Například při bezpečném připojení k WWW serveru certifikovanému *CESNET CA* se neobjeví časté okénko s dotazem, jestli hodláte serveru důvěřovat.

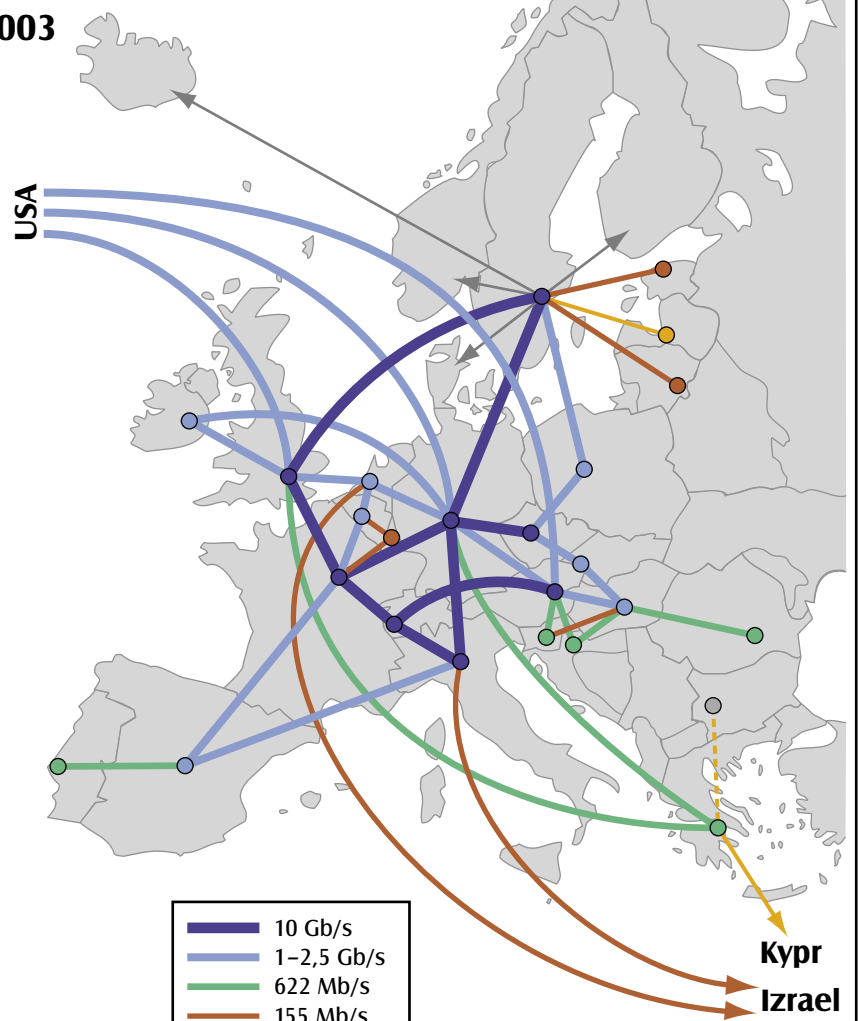
K instalaci hlavního certifikátu *CESNET CA* do WWW klienta otevřete stránku <http://www.cesnet.cz/pki/certs/ccca.crt> a ve zobrazeném dialogu zaškrtnete, že jste ochotni akceptovat tuto autoritu pro Web, e-mail i software. Svou volbu potvrďte. Tím okamžikem se *CESNET CA* stane důvěryhodnou pro vašeho WWW klienta a případné další programy, které s ním sdílejí databázi autorit (např. MSIE a MS Outlook mají společnou databázi). Dovolili bychom si požádat především správce počítačových učeben, aby tento hlavní certifikát nainstalovali.

kapacity připojení

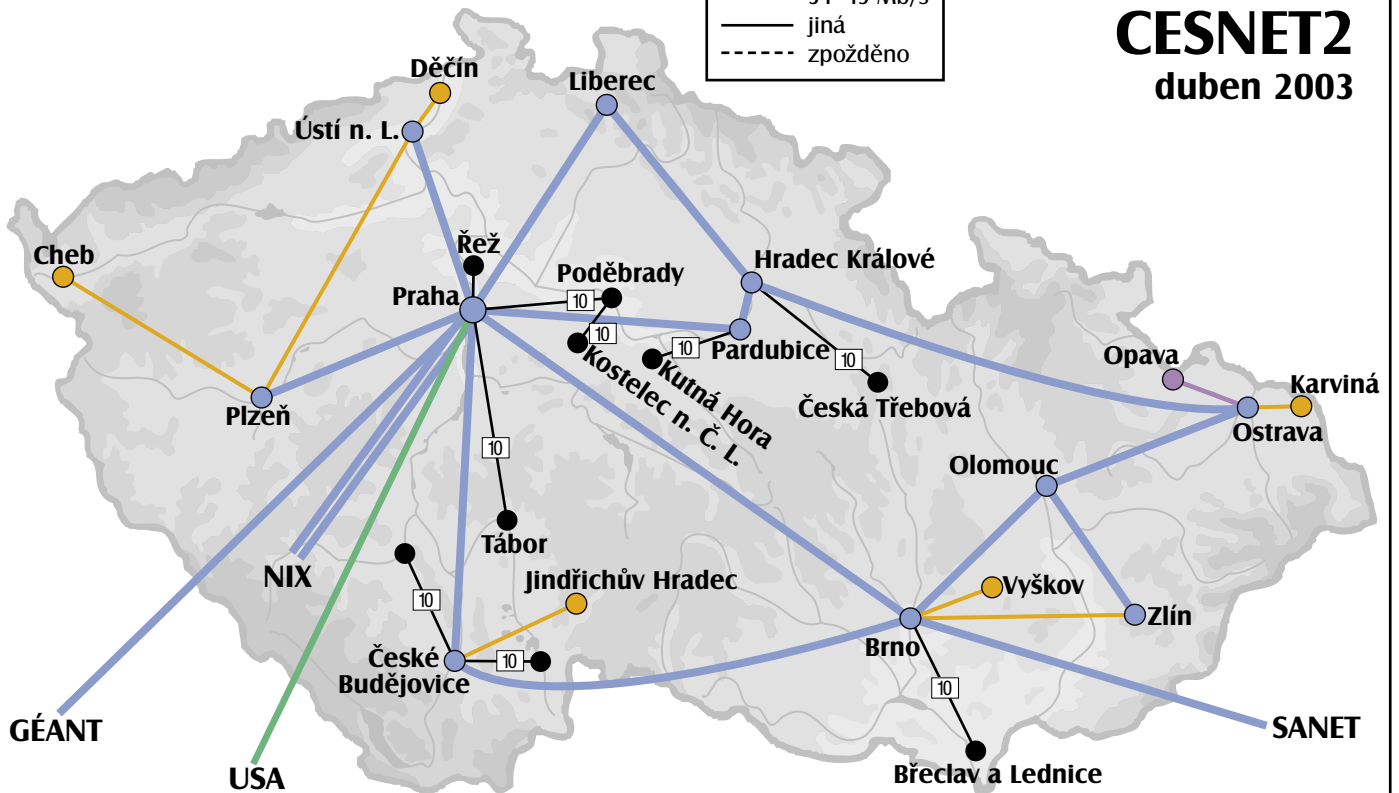


GÉANT duben 2003

páteří síť



CESNET2 duben 2003



Seminář Nové směry vysokorychlostních sítí

Naši nejvýznamnější aktivitou v prvním čtvrtletí roku 2003 byla příprava nového výzkumného záměru, o jejichž výsledcích informujeme na následující straně. Svě představy jsme konzultovali s několika zahraničními partnery, kteří zároveň přijali naši žádost o vystoupení na semináři *Nové směry rozvoje vysokorychlostních sítí a jejich aplikací*, který jsme při té příležitosti uspořádali. Konal se 20. února 2003 v prostorách Národohospodářského ústavu Akademie věd České republiky.



Seminář zahájil Josef Kubíček, předseda představenstva CESNETu. V následujícím textu vám stručně přiblížíme obsah jednotlivých vystoupení. Díky našemu videoarchivu si je můžete poslechnout v plném znění na adrese

<http://www.cesnet.cz/doc/seminare/20030220/>

kde najdete videozáznamy všech vystoupení v originálním znění i tlumočené do češtiny, prezentace jednotlivých účastníků a fotografie. Na semináři vystoupili:

Michal Frankl, Ministerstvo informatiky ČR

ocenil výsledky CESNETu jako výjimečné a důležité. Poukázal také na to, že se jedná o jeden z výsledků výzkumu a vývoje, který dokáže generovat prostředky na svůj další rozvoj.

Luis Rodríguez-Rosello, Evropská komise

představil aktivity Evropské komise v oblasti rozvoje informačních technologií a jejich pronikání do společnosti. Vyzvedl významnou roli, kterou v této oblasti hrají národní akademické sítě a významné evropské projekty, jako jsou Géant, 6NET, Euro6IX či gridové aktivity. Závěr svého příspěvku věnoval 6. rámcovému programu a jeho struktuře. Právě pokračování Géantu a gridy v něm budou hrát klíčové role.

Jan Gruntorád, CESNET

shrnuje výsledky, kterých sdružení dosáhlo při řešení výzkumného záměru v loňském roce. Jednalo se vlastně o stručný průřez roční zprávou, kterou si můžete přečíst na adrese <http://www.cesnet.cz/doc/2002/zprava/>.

Zdeněk Svoboda, MŠMT ČR

potvrdil, že ministerstvo školství vnímá význam CESNETu pro rozvoj informačních technologií, což se ostatně odráží i ve významném podílu MŠMT na financování sdružení. Vyjádřil také přesvědčení, že význam vysokorychlostních sítí v budoucnu ještě vzroste, a to pro celou oblast vzdělávání.



Fernando Liello, Géant

shrnuje ve svém vystoupení výsledky, kterých bylo dosaženo za dvacet let budování akademických sítí v Evropě. Zabýval se motivací pro jejich vznik, službami, jež přinášejí, a vztahem mezi akademickými a komerčními sítěmi. V závěru zdůvodnil, proč se hierarchický model (univerzita-národní akademická síť-evropská akademická páteř) jeví v evropském kontextu jako optimální.

Kees Neggers, SURFnet

představil připravovanou novou generaci nizozemské akademické sítě SURFnet6. Podle názoru jejich autorů nastal čas na změnu základního paradigmatu, takže další generace sítí nezvznikne prostým rozvojem těch stávajících. Významného nárůstu parametrů lze docílit jen revoluční změnou principů, na nichž je síť postavena. Především rozvoj optických technologií a lambda služeb označil za nadějný směr, od něž lze očekávat zmiňovanou radikální změnu. Prezentoval také trefnou charakteristiku vzájemného vlivu, který na sebe mají poskytování sítí pro výzkum a výzkum sítí samotné.

Bill St. Arnaud, CANARIE

vyzdvihl dojem, který na něj naše výsledky učinily a vyjádřil zájem o těsnější spolupráci mezi kanadskou CANARIE a CESNETem. Dále pak představil vizi další generace akademické sítě CA*net 4 a především dopady pokročilých aplikací z oblasti vědy a výzkumu. Podle jeho názoru jsme na počátku třetí vlny rozvoje Internetu (první byla charakterizována intraktivními textovými službami, druhou ztělesňuje Web), charakterizované distribuovanými výpočty, masivním sdílením dat a peer-to-peer službami.



Nový výzkumný záměr sdružení CESNET

Od roku 1999 jsou výzkumné aktivity sdružení CESNET v oblasti síťových technologií a aplikací finančně podporovány Ministerstvem školství, mládeže a tělovýchovy v rámci výzkumného záměru *Vysokorychlostní síť národního výzkumu a její nové aplikace*, jehož je CESNET nositelem.

Cílem tohoto pětiletého výzkumného záměru je ověřit možnosti využití pokrokových komunikačních technologií pro potřeby vědecké komunity, navrhnout a vybudovat komunikační infrastrukturu vhodnou pro přenos a zpracování dat v rámci vědeckých experimentů. Nejvýznamnějším výstupem záměru je funkční vysokorychlostní síť národního výzkumu *CESNET2*, jejíž parametry a služby jsou srovnatelné se špičkovými sítěmi obdobného charakteru v zahraničí. Postup řešení a dosažené výsledky jsou k dispozici na <http://www.cesnet.cz/doc/>.

Jelikož rok 2003 je posledním rokem řešení stávajícího výzkumného záměru, zabývalo se vedení sdružení již na konci roku 2002 otázkou, jak v následujících letech zajistit financování své hlavní činnosti, tj. výzkumu a vývoje v oblasti informačních a komunikačních technologií. V tomto období vyhlásilo Ministerstvo školství, mládeže a tělovýchovy dlouho očekávanou výzvu k podávání návrhů výzkumných záměrů na období 2004-2008 (resp. 2010). Proto sdružení CESNET podalo 27. února 2003 návrh sedmiletého výzkumného záměru *Optická síť národního výzkumu a její nové aplikace*. Návrhu byl přidělen identifikační kód MSM6383917201.

Východiskem pro návrh bylo zhodnocení současného stavu ve světových výzkumných sítích a prognózy vývoje v této oblasti. Vzhledem k rychlému vývoji v této sféře byly detailní plány rozpracovány pouze na roky 2004-2007.

Cílem výzkumného záměru *Optická síť národního výzkumu a její nové aplikace* je navrhnout integrované síťové prostředí vyhovující specifickým požadavkům vědecké, výzkumné a akademické komunity a v provozu ověřit jeho vlastnosti. Zkušenosti s provozem akademických sítí totiž ukazují, že dostatek volného přenosového pásma je pouze jedním z požadavků. Pro provozování kvalitní akademické sítě je třeba na síti implementovat další služby. Z tohoto důvodu se řešitelský tým kromě výzkumu v oblasti infrastruktury a síťových protokolů zaměřil také na oblast aplikací a oblast síťových služeb (tzv. middle-ware) zajišťující vazbu mezi vrstvou aplikační a síťovou.

V oblasti aplikací se hodláme soustředit především na rozvoj tzv. gridů jakožto prostředí pro spolupráci distribuovaných entit, ať už jimi jsou lidé, skupiny lidí, či stroje. V současnosti se

rýsuje několik typů gridových technologií:

- Výpočetní grid pro náročné vědecké výpočty se zapojením velkého počtu geograficky distribuovaných počítačů.
- Úložný grid, prostředí umožňující distribuované ukládání dat a vzdálený přístup k nim.
- Přístupový grid, standardizované prostředí pro spolupráci za využití videokonferenčních a multimediálních aplikací a prostředků pro spolupráci nad sdílenými dokumenty.

Dalším okruhem našeho zájmu bude rozvoj IP telefonie, videokonferenčních nástrojů a nástrojů pro streaming multimediálního obsahu. Velká pozornost také bude věnována problematice distančního vzdělávání.

Síťové služby, jako spojující článek mezi infrastrukturou a aplikacemi, v sobě zahrnují:

- vývoj prostředků pro sledování a vyhodnocování provozu sítě
- vývoj prostředků pro sledování výkonnostních charakteristik sítě a nástrojů k jejich optimalizaci
- autentizační a autorizační mechanismy pro přístup k prostředkům na síti.

Při návrhu a výstavbě infrastruktury se zaměříme na využití optických technologií s důrazem na využití pronajatých optických vláken, osazených vlastními aktivními prvky. Díky tomu získáme plnou kontrolu nad sítí a možnost poskytování více nezávislých kanálů na tomtéž vlákne. Předmětem výzkumu bude také možnost budování dálkových meziměstských optických tras bez regenerátorů nasazených podél trasy. Předpokládá se také vývoj a nasazení gigabitového směrovače na bázi PC.

V rámci tohoto výzkumného záměru je plánována migrace sítě na protokol IPv6 včetně zpřístupnění aplikací a služeb. Předpokládáme pochopitelně, že oba protokoly (stávající IPv4 a nastupující IPv6) budou po určitou dobu provozovány současně.

Nedílnou součástí výzkumného záměru bude také zapojení našich odborníků do mezinárodních aktivit a to především v rámci projektů 6. rámcového programu EU.

K naplnění všech těchto cílů je oproti předchozímu výzkumnému záměru výrazně rozšířena plánovaná kapacita řešitelského týmu. Pokud se struktury řízení výzkumného záměru týče, počítáme s využitím metody projektového řízení, která se ve stávajícím záměru osvědčila.

Zajímavé nové trasy

Srovnáte-li mapku sítě *CESNET2* na straně 2 tohoto *Datagramu* s její předchůdkyní, pravděpodobně si všimnete dvou přírůstků v externích spojích. Jeden směřuje do národního propojovacího centra *NIX.CZ*. Naše kapacita propojení s ostatními poskytovateli Internetu v ČR dnes činí 2×1 Gb/s a umožňuje přenášet IPv4 i IPv6.

Zajímavější je druhá z nových tras, mezinárodní spoj Brno-Bratislava, kterým jsme propojeni se slovenskou akademickou sítí *SANET*. Jeho vznik iniciovali naši slovenští kolegové, kterým se podařilo získat za velmi výhodných podmínek potřebnou optickou trasu. Její osazení a uvedení do provozu pak bylo přirozeným důsledkem příhodné situace.

Vznik této trasy ilustruje jeden z trendů dnešního síťového světa. Řada firem v uplynulých letech investovala do budování

optické infrastruktury a vznikla tak velmi bohatá nabídka. V některých oblastech je dokonce nadbytek dostupných vláken, čemuž odpovídají i ceny. Provozovatelé koncových sítí pak často takové možnosti využívají ad hoc a propojují své sítě dříve neplánovanými cestami, protože to je pro ně výhodné.

Poslední ze zajímavých tras spojuje Opavu s Ostravou. Došlo zde ke zrychlení na 100 Mb/s, což ale není ten nejvýznamnější aspekt. Důležitější je, že se jedná o trasu jednovláknovou. Zatímco klasický optický přenos používá dvě optická vlákna (jedno pro každý směr přenosu), dnes již existují technologie, které dovedou oba směry přenášet po jediném vlákne. A to i na značnou vzdálenost - dotyčná trasa měří téměř 50 km. Díky úsporám za nájem vláken se investice do obousměrné technologie vrátí za méně než rok.