ÚVT MU
zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • prosinec 2010 • roč. XXI • č. 2

Ráno Eduroamisto, večer takisto

David Antoš, Martin Osovský, Marek Saitl, Václav Lorenc, ÚVT MU

1 Úvod

Od doby, kdy se notebooky a další mobilní zařízení vybavená Wi-Fi (PDA, pokročilé mobilní telefony, ...) staly běžnou výbavou jak vědeckých pracovníků, tak i studentů, a kdy bez připojení k síti téměř nelze pracovat, narážíme na častý problém: jak na cestách připojit zařízení k síti.

Pomineme-li komerční možnosti, jako (nezřídka placené) připojení v hotelích nebo obvykle v zahraničí velmi drahé připojení mobilním telefonem, zbývají kavárny nebo podobné podniky, kde často mívají pro hosty otevřené bezdrátové připojení. Jak se ale připojit k síti v místech, kde pracovat skutečně potřebujeme, na univerzitách a vědeckých ústavech? Jejich sítě bývají často zabezpečené, získávání účtu zdržuje a zatěžuje uživatele i správce a je docela nesystémové. Proto v rámci aktivit sdružení TERENA (přesněji skupiny TF-Mobility and Network Middleware [5]) vznikl projekt Eduroam [1]. TERENA koordinuje projekt celosvětově, národní infrastrukturu ČR spravuje sdružení CESNET. Ústav výpočetní techniky MU zajišťuje provoz poskytovatele identit uživatelů z MU, ve spolupráci s lokálními správci sítí koordinuje zavádění Eduroamu na univerzitě a značné části sítě Eduroam na MU samo spravuje.

Obrázek 1: Logo Eduroamu

Základním účelem Eduroamu je umožnit studentům a zaměstnancům akademických institucí bezplatný přístup k síti, kdekoli je Eduroam dostupný, bezpečně a co možná jednotným způsobem bez nutnosti změny konfigurace jejich počítačů.

Síť Eduroam je dostupná v rostoucím počtu budov MU. Eduroamem postupně nahrazujeme starší bezdrátové připojení, tzv. MUNI-VPN. Oproti MUNI-VPN přináší Eduroam většinou vyšší rychlost připojení a zejména výhodu mobility. MUNI-VPN je čistě lokální přístupový mechanismus MU a ve střednědobém horizontu přestane být podporován.

Tento článek se zaměří spíše na uživatele, jehož technické detaily příliš nezajímají, a také na zcela praktické rady v prostředí MU. V sekci 6 se zmíníme také o novince: do Eduroam sítě MU je možno dovolit přístup hostům, kteří nemají ve své domovské organizaci správce identit pro síť Eduroam. Pro ty, kteří by se rádi dozvěděli více o technických principech implementace Eduroamu, můžeme odkázat na starší přehledový

článek ve Zpravodaji [6], případně na webové stránky projektu [1, 3], které obsahují podrobný technický popis. Pro uživatele z MU je hlavním zdrojem informací o Eduroamu a jeho nastavení portál [2].

2 Jak použít Eduroam

Pro připojování k síti Eduroam je třeba mít nainstalován program pro autentizaci, tzv. suplikant. Ve většině moderních operačních systémů je přímo součástí systémové instalace (zejména uživatelé Windows od verze XP výše nebudou mít problém). Aktuální návody pro řadu operačních systémů naleznete na univerzitních stránkách [4].

Jak proběhne připojení k bezdrátové síti, to si ukážeme na příkladu. Předpokládejme, že uživatel z MU je zrovna v budově ČVUT v Praze. Na svém notebooku, jako jednu z dostupných bezdrátových sítí, vybere síť „eduroam“. Pro jednoduchost hovoříme o notebooku, ale principy se týkají většiny zařízení s Wi-Fi. V konfiguraci suplikantu má zadáno uživatelské jméno ve tvaru učo@eduroam.muni.cz a sekundární heslo z ISu[1]. Není třeba se obávat, že uživatel zadává tyto údaje v cizí síti – jméno a heslo se zadává pouze do konfigurace uživatelova stroje. Je to daleko bezpečnější, než třeba přes webový formulář. Heslo se ověří vůči serverům MU. Tyto autentizační servery (říká se jim také poskytovatelé identit) příslušné vzdálené síti potvrdí, že uživatel skutečně pochází z MU, a tudíž je oprávněn síť použít. Uživatel pak dostane do sítě přístup a může ji využívat v souladu s její lokální politikou. Bezdrátové spojení notebooku uživatele s příslušným přípojným místem je navíc kompletně šifrováno, takže nehrozí odposlech samotného bezdrátového provozu v blízkosti uživatelova notebooku.

Z pohledu uživatele proběhne připojení zcela shodně, ať je uživatel kdekoli v dosahu nějaké sítě Eduroam. Třebaže síť Eduroam nejčastěji používá jméno (SSID) „eduroam“, není tomu tak vždy. Bývá nicméně zvykem, že toto slovo v názvu alespoň obsahuje, často se používá forma „eduroam-xyz“, kde „xyz“ je zkratka poskytující instituce (například eduroam-fi na Fakultě informatiky MU).

Jméno sítě by nemělo být skryté (tj. má být přístupovým bodem oznamováno, konfigurační program jej pak umí vypsat), nicméně pokud ve výpisu dostupných sítí uživatel žádné nadějné jméno nenalezne, lze alespoň zkusit připojení k síti „eduroam“. Národní politika Eduroamu dovoluje, že toto jméno oznamováno být nemusí. K síti, jejíž jméno není oznamováno, se lze připojit, pokud toto jméno a další potřebné údaje známe předem a do konfigurace je zadáme.

Je vhodné si uvědomit, že připojení není anonymní. Vzdálená síť uchovává o uživateli uživatelské jméno, přidělenou adresu a dobu, kdy byl uživatel připojen. Pokud se uživatel dopustí nějakého bezpečnostního incidentu, správci sítě musí incident řešit. Protože ale o uživateli mají jen velmi strohé údaje, budou kontaktovat správce domovské organizace uživatele (které organizaci uživatel patří se pozná z uživatelského jména), kterému sdělí uživatelské jméno a popis incidentu. Správce domovské organizace je politikou Eduroamu zavázán ke spolupráci a zodpovídá za vyřešení incidentu včetně odpovědi správci vzdálené sítě.

Přestože celý princip fungování sítě Eduroam vypadá triviálně, za uživatelskou jednoduchostí a transparentností se skrývá košatá struktura autentizačních serverů, které si šifrované autentizační údaje předávají podle dosti složitých pravidel.

3 Používám Eduroam na MU

Všichni, kdo jsou oprávněni používat Eduroam, jej mohou používat i na MU. To se samozřejmě týká i vlastních zaměstnanců a studentů univerzity. Provoz v této síti není omezen firewallem a platí v ní stejná pravidla použití jako v dalších sítích MU.

Aktuální seznam míst pokrytých sítí Eduroam v prostorách MU najdete na webu ÚVT [2]. Na tomto webu také najdete formulář pro hlášení problémů. Kromě kontaktování správců elektronickou cestou je možné osobně navštívit Celouniverzitní počítačovou studovnu, jejíž operátoři

[1] Sekundární heslo v ISu lze nastavit na stránce `https://is.muni.cz/auth/system/heslo.pl`

také umí pomoci s konfigurací mobilního zařízení a nastavení lze přímo ve studovně otestovat.

4 Časté problémy

Než se uživatel obrátí na správce s žádostí o řešení problému, je vhodné, aby si zkontroloval základní nastavení. Často se chybuje v zadání uživatelského jména, to je pro uživatele z MU ve formátu „učo@eduroam.muni.cz“, kde „učo“ je identifikační číslo osoby, které najdete například v ISu. Uživatelé často zapomínají na ono „@eduroam.muni.cz“, to je ale nezbytné, aby autentizační servery poznaly, kterou instituci kontaktovat pro ověření identity uživatele.

Další častou chybou je použití jiného než sekundárního hesla z ISu (např. primárního). Primárním heslem se uživatel přihlašuje k ISu a dalším základním systémům MU, jako například k systému Inet. Sekundární heslo slouží pro stahování pošty, přístup k Eduroamu, přístup k federovaným webům atd.

Pokud se připojení k síti systematicky nedaří, je dobré ověřit celé nastavení podle návodů na [2], problém někdy bývá v nastavení jiného šifrovacího protokolu. Typickým projevem chyby v nastavení šifrování v systémech rodiny Windows je, že se Eduroam v seznamu sítí ukáže, ale s červeným křížkem jako nedostupná síť.

Uživatelé si občas stěžují na sníženou rychlost nebo výpadky připojení. Celá infrastruktura přístupových bodů je nepřetržitě monitorována a výpadky jsou řešeny, jak je to jen nejdříve možné. Přesto propustnost přípojných míst není neomezená. Pokud se do posluchárny nahrne sto studentů s notebooky, všichni se připojí (a často někteří z nich začnou stahovat větší data, jak už to studenti dělávají), už jen samotné principy bezdrátového připojení nedovolí, aby pak připojení bylo stejně rychlé, jako když přístupové body sítě nejsou tak zatíženy. Otázka přidání více přípojných míst se samozřejmě převádí na zcela konkrétní částky požadované z univerzitního rozpočtu.

Občas také od uživatelů slýcháme stížnosti typu, že připojení se obnovuje a zase rozpadá, případně že se přenosy dat zasekávají. Obvyklou příčinou je opět bezdrátová technologie. Radiové vlny jsou v budovách pohlcovány a odráženy zejména železobetonovými konstrukcemi. Bezdrátové sítě musí odpovídat průmyslovým standardům a hygienickým normám, proto zvyšování výkonu přípojných míst nepřichází v úvahu. Často postačí se v místnosti přesunout s notebookem o kousek jinam. Autoři tohoto článku mají bohaté zkušenosti s kancelářemi ÚVT na Botanické, kde – jako důsledek konstrukce budovy – vznikají desítky centimetrů široká pásma s nevalným signálem těsně vedle míst s velmi dobrým připojením. Tyto problémy vznikají prakticky ve všech v současnosti používaných sítích. Na výraznější zlepšení si budeme nejspíš muset počkat na další generaci těchto technologií. Rozhodně ale s problémy se signálem bezdrátových sítí není od věci kontaktovat lokálního správce, může pomoci i přemístění přípojného bodu.

5 Používám Eduroam na MU a chystám se na cesty

Pokud se uživatel z MU chystá na cesty, může se předem podívat, zda je cíl cesty pokryt sítí Eduroam. Portál [3] hned na první stránce obsahuje mapu pokrytí pro ČR. Eduroam je dostupný na mnoha univerzitách nejen v Evropě, ale také v USA, Kanadě, Austrálii a Japonsku. Na portálu [1] je k dispozici mapa pokrytí pro všechny tyto regiony, stačí kliknout na správný region a pak potřebný stát, a postupně se na mapě proklikat až k příslušnému místu – cílové instituci.

Na webových stránkách cílové instituce jsou zveřejněny podrobné instrukce pro uživatele, obsahující informace o použitých jménech (SSID) sítí, popis prostoru pokrytého bezdrátovým signálem a další informace nezbytné pro úspěšné použití sítě. Stránky také obsahují kontakt na lokální technickou podporu.

Není od věci si zjistit tyto údaje dříve, než se vypravíme na cestu. Pokud se připojení nezdaří, narazíme na nejslabší místo Eduroamu – velmi složité hledání problému. O postupu při řešení situace, kdy se uživateli nezdaří připojit, vede mezinárodní komunita kolem Eduroamu již několik let vášnivé diskuse, tak vášnivé, že obvykle

ani weby s návody neobsahují žádné doporučení pro tento případ. Jak jsme ověřili dotazem u národních koordinátorů sítě Eduroam ze sdružení CESNET, doporučeným postupem pro tyto případy je kontaktovat nejdříve správce z domovské organizace uživatele. Často je nezbytné k tomu použít telefon. Domácí správce ověří, zda přišel ze vzdálené sítě autentizační požadavek a zda byl serverem (poskytovatelem identit) domovské instituce správně zpracován. Pokud je na této straně vše v pořádku, problém bude ve vzdálené síti nebo ve stroji uživatele. Správce z domovské organizace uživatele bude také většinou schopen pomoci i s případnou změnou konfigurace uživatelova stroje, případně alespoň poskytnout kontakt na správce vzdálené sítě (ten je sice na příslušných webových stránkách, ale problémem uživatele je přesně to, že se k síti nemůže dostat).

Místa pokrytá signálem Eduroamu jsou také často označena logem projektu (obr. 1).

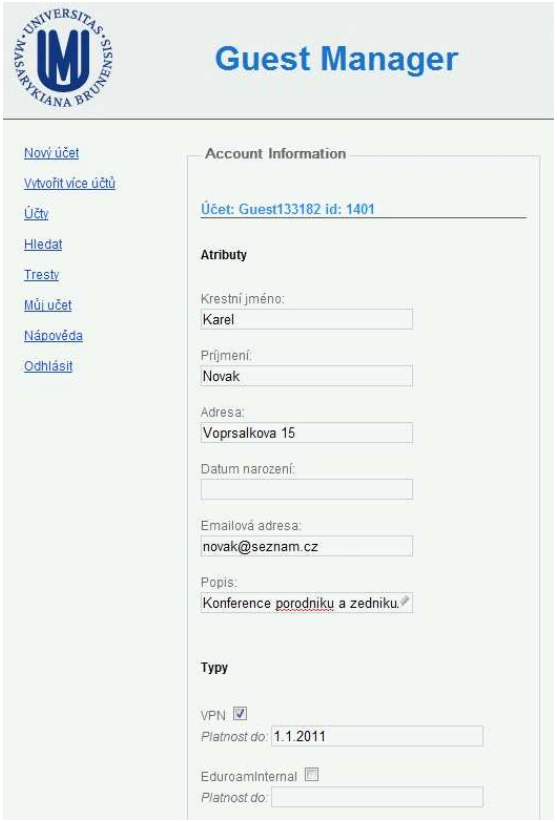
Pokud na cestách narazíte na problém s připojením k Eduroamu, kontaktujte dohledové centrum datových sítí ÚVT na telefonním čísle +420 54949 4241.

6 Mám na MU hosta s notebookem

Jak je z předchozích částí patrné, návštěvníci univerzity přicházející z organizací zapojených do Eduroamu, by s připojením k naší síti neměli mít problém. Co ovšem s těmi, kteří takovou domovskou organizaci nemají, přesto jsou u nás třeba účastníky konference nebo hosty univerzitního hotelu, a potřebujeme jim proto umožnit přístup na síť?

Na většině fakult je možné se obrátit na místní laboratoř výpočetní techniky nebo jiné oddělení, které má na starost výpočetní techniku. Pracovníci těchto oddělení jsou oprávněni vytvořit dočasný účet nebo účty s oprávněním přístupu na internet pomocí Eduroamu. Účet platí pouze pro přístup do Eduroam sítě Masarykovy univerzity (tj. nikoli do sítí jiných organizací) a vytváří se na omezenou dobu.

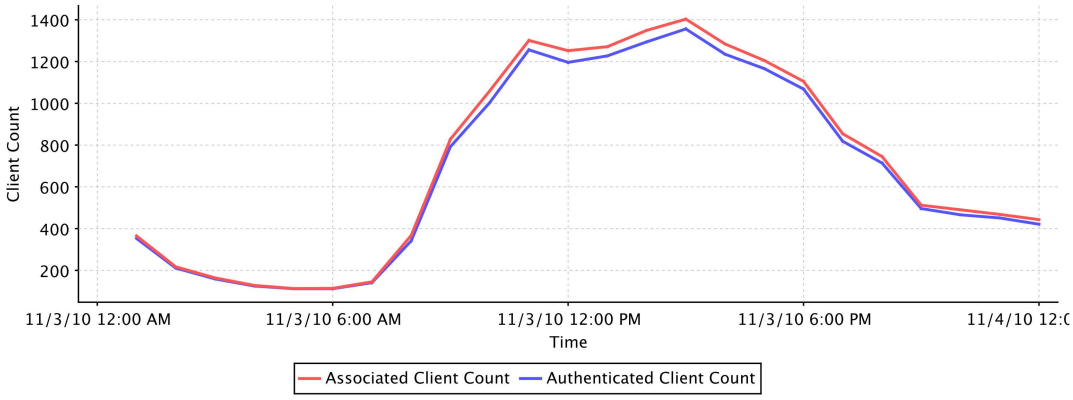
Oprávněné osoby mají za tímto účelem k dispozici aplikaci vyvinutou na ÚVT (obr. 2, která umožňuje



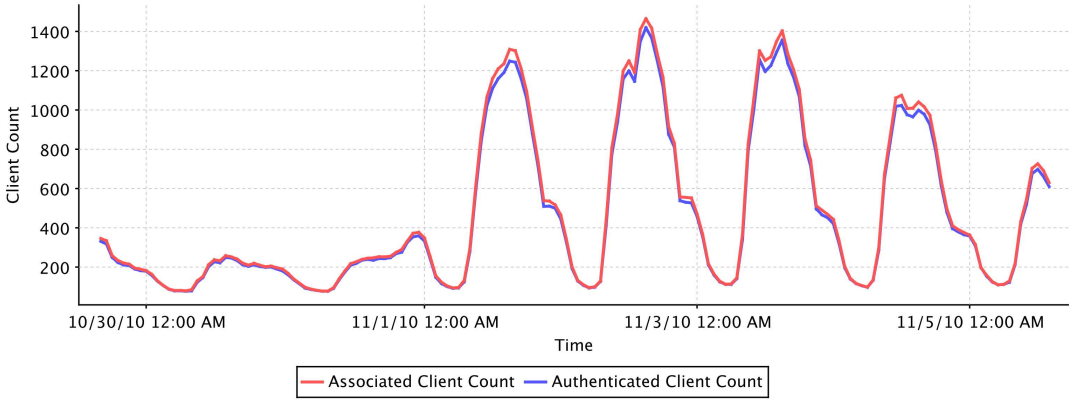
Obrázek 2: Správce hostujících identit

- vytvořit jeden nebo několik účtů ručně (informace o osobě, pro kterou je účet vytvářen, se zadávají do systému),
- vytvořit účty hromadně ze souboru (CSV nebo Excel),
- vytisknout po vytvoření účtu kartičku s vytištěným přihlašovacím jménem, případně jménem a příjmením a heslem,
- přiřadit do nějakého data nebo odebrat účtu jedno nebo více z nabízených oprávnění (obvykle Eduroam nebo VPN),
- změnit heslo existujícího účtu.

Bezpečnostní politika MU vyžaduje, aby hostující uživatelé bezdrátových sítí byli identifikovaní a dohledatelní. Proto je nejvhodnější dočasné účty vytvářet přímo pro konkrétní osoby. Pokud to není možné, lze vytvořit i sadu anonymních účtů, pořadatelé příslušné akce pak ovšem zodpovídají za to, že evidují, které osobě přiřadili příslušné uživatelské jméno. Při pořádání konference nebo workshopu jsou nicméně seznamy účastníků obvykle známy předem, takže příslušné účty lze také předem připravit. Detailní



Obrázek 3: Denní průběh počtu klientů na MU



Obrázek 4: Týdenní průběh počtu klientů na MU

informace a podporu poskytnou pracovníci laboratoří výpočetní techniky.

Systém pro správu identit hostů je vyjma Eduroamu možno použít i pro zpřístupnění dalších služeb, jako jsou webové stránky, přihlašování na počítače a podobně.

7 Jak je síť Eduroam na MU využívána

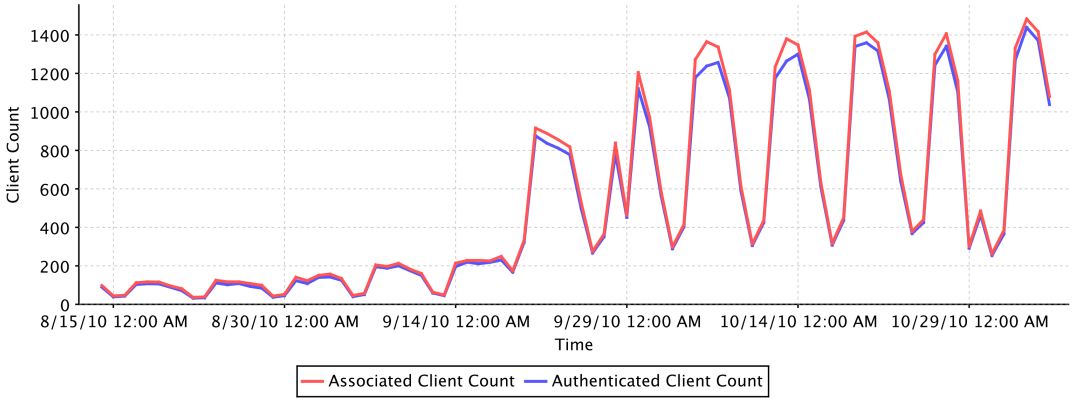
Oddělení datových sítí ÚVT aktuálně spravuje celkem 376 přístupových bodů bezdrátové sítě Eduroam. Počty připojených klientů kolísají v závislosti na tom, zda běží semestr, během týdne i během dne.

Grafy na obrázcích zachycují typický vzor počtu uživatelů. Červená čára je počet klientů, kteří se připojí k přístupovým bodům sítě, modrá čára pak zobrazuje ty, kteří se úspěšně autentizují, tj. byli do sítě vpuštěni. Je patrné, že ne všichni připojení klienti se také autentizovali, mezi ně typicky patří zařízení, která nemají Eduroam nakonfigurovaný, nicméně jsou nastavena tak, že se zkusí připojit k nějaké dostupné síti. Obr. 3 zachycuje typický den v semestru, je zjevné, že průběh odpovídá obvyklé pracovní době akademických pracovníků i době, kdy se obvykle koná výuka. Ve špičkách je připojeno kolem 1400 uživatelů. Obr. 4 znázorňuje typický týdenní průběh (graf začíná víkendem). Je patrná tendence studentů (i tvůrců rozvrhu) mít většinu přednášek začátkem pracovního týdne. Na grafu 5 je jasně patrný vliv prázdnin a náběhu semestru.

Množství přenášených dat silně koreluje s počtem klientů. Datové toky ve špičkách dosahují 200 Mbit/s, přitom přibližně dvě třetiny až čtyři pětiny tohoto toku směřují k uživatelům (download). Uživatelé Eduroamu se tedy chovají srovnatelně s uživateli pevně připojených strojů.

8 Shrnutí

Síť Eduroam, oproti jiným způsobům připojování k bezdrátové síti univerzity, přináší zásadní



Obrázek 5: Dlouhodobý průběh počtu klientů

výhodu uniformního přístupu k síti na stále rostoucím množství institucí a míst jak v Evropě, tak i na jiných kontinentech. Od roku 2005, kdy se tato technologie začala na MU zavádět, se neustále zvětšuje počet přípojných bodů i na naší univerzitě. Jsme přesvědčeni, že výhody této technologie výrazně převažují nad poněkud složitější prvotní konfigurací a předpokládáme, že se Eduroam po dlouhou dobu udrží jako dominantní metoda přístupu k síti pro studenty a pracovníky v akademické sféře.

Tento článek byl podpořen projektem „Vzdělávání akademických pracovníků v oblasti e-Infrastruktur“ (CZ.1.07/2.3.00/09.0074). Tento projekt je spolufinancován z Evropského sociálního fondu a státního rozpočtu České republiky.

Literatura

[1] Eduroam. `http://www.eduroam.org/`.

[2] Eduroam na MU. `htpp://eduroam.muni.cz/`.

[3] Eduroam.cz. `http://www.eduroam.cz/`.

[4] Návody pro konfiguraci na stránkách Eduroamu MU. `http://eduroam.muni.cz/doku.php?id=navody`.

[5] TERENA TF-Mobility and Network Middleware. `http://www.terena.org/activities/tf-mobility/`.

[6] Michal Procházka. Všichni chceme Eduroam! *Zpravodaj ÚVT MU*, XVII(2):4–6, 2006. ISSN 1212-0901. □

Dynamický nákupní systém na MU

Jana Kohoutková, ÚVT MU a Michaela Poremská, PrF MU

Co je to DNS? Proč je to tak složité? Jak to vlastně funguje? A jak se to týká mne? Na tyto a další otázky se budou snažit odpovědět následující odstavce. Nepochybně vyvolají řadu následných otázek a kritických připomínek, ale přinesou i dobré zprávy – například že se centrální veřejné zakázky na standardní kancelářské potřeby a standardní kancelářskou výpočetní techniku zahajují na MU každý měsíc, nebo že celý průběh veřejné zakázky od zahájení k plnění, se všemi legislativními náležitostmi, lze zvládnout do dvou měsíců?

1 Elektronizace zadávání veřejných zakázek

Zákon o veřejných zakázkách č. 137/2006 Sb., který nabyl účinnosti dne 1. července 2006, zavedl elektronický způsob zadávání veřejných zakázek.

K rozšíření elektronizace významně přispěla i poslední novela tohoto zákona (č. 179/2010 Sb., účinná od 15. září 2010), která klade důraz na elektronizaci například tím, že zavedla, mimo

jiné, povinné uveřejňování výzvy k podání nabídky a k prokázání splnění kvalifikace ve zjednodušeném podlimitním řízení, a to na profilu zadavatele pomocí elektronického nástroje. V případě MU se jedná o internetovou adresu `https://zakazky.muni.cz`.

Dále se nepřímo elektronizace prosazuje při aplikaci Pravidel pro výběr dodavatelů v rámci Operačního programu Výzkum a vývoj pro inovace, do něhož je Masarykova univerzita zapojena (`http://www.msmt.cz/strukturalni-fondy/spolecne-prilohy-prirucek-pro-zadatele-a-prijemce-op-vavpi-3`): „*Při zadávání zakázek organizačními jednotkami subjektu, které mohou být považovány za samostatného veřejného zadavatele (zejm. fakulty VŠ), jakožto samostatnými hospodářskými jednotkami, je možné zadávat zakázky samostatně touto organizační jednotkou pouze v odůvodněných případech, pokud neexistuje konkrétní vazba na plnění zadávané v rámci subjektu a tento postup neodporuje zásadám hospodárnosti a transparentnosti zadávání zakázek. (část III., bod 10.)*“ Z uvedeného vyplývá, že je třeba sčítat plnění (předmět veřejné zakázky) za celý subjekt, a z organizační jednotky subjektu nelze zadávat veřejné zakázky, pokud se nejedná o specifické plnění organizační jednotky.

Uvedená Pravidla jsou v souladu se zákonem o veřejných zakázkách, který definuje zadavatele jako právnickou osobu čili univerzitu jako celek.

Je stěží představitelná koordinace zadávání veřejných zakázek na Masarykově univerzitě, která má devět fakult s více než 200 katedrami, ústavy a klinikami a další hospodářská střediska, pouze v listinné podobě, a tudíž byl implementován elektronický nástroj pro zadávání veřejných zakázek E-ZAK.

Elektronizace a především dynamický nákupní systém, jemuž věnujeme následující kapitolu, umožňuje na Masarykově univerzitě zachovat v souladu se zákonem o veřejných zakázkách decentralizaci subjektu na hospodářská střediska a zadávat veřejné zakázky na střediscích (aniž by se jednalo o speciální plnění pro dané hospodářské středisko), nebo umožňuje i centrální zadávání[1], tzn. že se požadavky ze všech hospodářských středisek sesbírají a z administrativní jednotky – rektorátu – se zadává centrální veřejná zakázka.

2 Elektronický nástroj pro zadávání veřejných zakázek na MU a především dynamický nákupní systém

Atestovaný elektronický nástroj E-ZAK, který je dostupný na adrese `https://zakazky.muni.cz`, je na Masarykově univerzitě používán k 31. říjnu 2010 již jeden rok. Za první rok provozu nástroje zahájila Masarykova univerzita administraci celkem 95 zakázek na dodávky, služby a stavební práce. Jednalo se o 43 nadlimitních, 12 podlimitních a 40 veřejných zakázek malého rozsahu.

V únoru tohoto roku začala univerzita kromě „klasických“ elektronických řízení využívat i dynamický nákupní systém (DNS). DNS je plně elektronický systém pro pořizování běžného a obecně dostupného zboží, služeb nebo stavebních prací, který je časově omezený a otevřený po celou dobu svého trvání všem dodavatelům, kteří splní podmínky pro zařazení do dynamického nákupního systému a podají předběžnou nabídku.

Zadavatel zařazuje do dynamického nákupního systému dodavatele, který splní podmínky pro zařazení do DNS a který předloží předběžnou nabídku v souladu s požadavky zadavatele uvedenými v zadávacích podmínkách, přičemž dodavatel může podat předběžnou nabídku nejenom při zavádění DNS ve lhůtě nejméně 40 dnů, ale po celou dobu jeho trvání, tzn. i v každé veřejné zakázce v DNS (viz dále), a tuto svou nabídku po celou dobu trvání DNS upravovat.

Výzvu k podání „*ostrých*“ nabídek odešle zadavatel zájemcům zařazeným do DNS až poté, co byly posouzeny veškeré předběžné nabídky. Lhůta pro podání předběžných nabídek v konkrétní zakázce v DNS nesmí být kratší než 15

[1] Nezaměňovat pojem s centralizovaným zadáváním u centrálního zadavatele podle § 3 zákona o veřejných zakázkách.

dnů ode dne uveřejnění zjednodušeného oznámení[2] v ISVZUS, přičemž uveřejnění oznámení odeslaného elektronicky proběhne do 5 dnů ode dne jeho odeslání do ISVZUS, tj. od zahájení zakázky do odeslání výzvy k podání nabídek uplyne přinejmenším 20 dnů. Výzva k podání nabídek nesmí obsahovat lhůtu pro podání nabídek kratší než 7 dnů.

Smlouva s dodavatelem může být uzavřena až po uplynutí lhůty pro podání námitek, která trvá 15 dnů po doručení oznámení o výběru nejvhodnější nabídky. K plnění veřejné zakázky může proto dojít až po více než měsíci a půl po zahájení zakázky.

Lhůty pro zadávání zakázek v dynamickém nákupním systému bohužel nejsou dynamické ve smyslu „do druhého dne“. Dynamičnost spočívá v otevřenosti systému pro dodavatele pro dobu jeho trvání.

V současné době má univerzita zavedeny DNS pro pořizování standardních kancelářských potřeb, standardních propagačních předmětů, standardních tiskařských služeb, standardního kancelářského ICT vybavení, standardního kancelářského nábytku, dále dynamický nákupní systém pro kancelářskou a audiovizuální techniku a tonery[3]. DNS na kancelářské potřeby a kancelářské ICT vybavení jsou tzv. *katalogové* neboli *centrální* dynamické nákupní systémy, do nichž jsou požadavky sbírány ze všech hospodářských středisek, a veřejná zakázka se pak zadává jako soubor těchto požadavků z centrální administrativní jednotky – rektorátu. Ostatní DNS jsou decentralizované.

Sběr požadavků pro centrální DNS vyvstal jako problém k řešení na jaře letošního roku, a realizace byla zadána týmu Inetu. Narychlo implementovaná jednoduchá sběrná aplikace byla po krátkém provozu nahrazena systémem, který centrálním DNS poskytuje servis jak před zahájením veřejné zakázky (zajištěním sběru a schvalování požadavků), tak po výběru ekonomicky nejvhodnější nabídky (podporou jejího zpracování v ekonomickém informačním systému). Tomuto servisnímu systému jsou věnovány následující kapitoly.

3 Sběr a schvalování požadavků pro centrální DNS

Sběry požadavků do obou centrálních DNS provozovaných na MU mají pravidelné uzávěrky jedenkrát měsíčně (kancelářské potřeby k poslednímu dni a kancelářské ICT ke 14. dni v měsíci). Jádrem sběrného systému je trojice aplikací *zadávání žádanek, schvalování žádanek a export žádanek*.

Zadávání žádanek (`https://inet.muni.cz/app/dns/zadavani`) slouží k pořizování žádanek na jednotlivých hospodářských střediscích, která mohou dle svého uvážení distribuovat práva na zadávání až na dílčí pracoviště (katedry, oddělení). Žádanka má vždy několik položek, z nichž každá specifikuje předmět (z katalogu předmětů daného DNS), zdroj financování (zakázku a další účetní analytiky), odpovědnou osobu, místo dodání a řadu dalších údajů. Kompletní žádanku odešle zadavatel4 ke schválení příslušným správcům rozpočtu – podle zdrojů financování jednotlivých položek.

Jistými pojistkami v systému zadávání jsou tzv. superzadavatelé, kteří mohou upravovat všechny žádanky svého hospodářského střediska, a tedy mohou kteréhokoli zadavatele operativně zastoupit (žádanky, které zadavatel nestihl odeslat ke schválení do uzávěrky sběru, se totiž nemilosrdně přesouvají do sběru následujícího, a tím o celý měsíc zpožďují).

Schvalování žádanek (`https://inet.muni.cz/app/dns/schvalovani`) slouží ke schvalování položek žádanek příslušnými správci rozpočtu. Položky předané ke schválení lze schvalovat již v průběhu sběru, a po jeho uzávěrce ve striktně šestidenní lhůtě (kalendářních, nikoli pracovních dní). Po uzávěrce schvalování se schválené položky exportují, a ostatní propadají.

Pojistkou proti propadání jsou jednak tzv. superschvalovatelé s právy schválit kteroukoli

[2] Formulář, který se uveřejňuje v Informačním systému o veřejných zakázkách – uveřejňovacím subsystému (ISVZUS) a jímž se zahajuje veřejná zakázka v DNS.

[3] DNS pro kancelářskou a audiovizuální techniku a tonery byly prozatím pouze zahájeny a běží lhůta pro podání předběžných nabídek při zavádění DNS.

položku svého hospodářského střediska, dále systém automaticky rozesílaných notifikací, a ve velmi neposlední řadě tým uživatelské podpory Inetu, který před uzávěrkou schvalování upomíná všechny opozdivší se schvalovatele i telefonicky.

Export žádanek (`https://inet.muni.cz/app/dns/do_excelu`), poslední z trojice, slouží k vygenerování excelovského souboru, v jehož řádcích jsou schválené položky žádanek z daného sběru. Soubor definuje souborný předmět veřejné zakázky pro vypsání v E-ZAKu.

4 Zpracování vítězných nabídek z centrálních DNS v ekonomickém systému MU

Vítězná, tedy ekonomicky nejvhodnější nabídka z veřejné zakázky proběhnuvší v E-ZAKu se zavádí jako objednávka resp. sada objednávek do ekonomického systému Magion, kde projde povinnou finanční kontrolou. Její schválená podoba se pak jako závazná (souborná) objednávka odešle dodavateli k realizaci, tj. dodání a fakturaci.

Jedná-li se o nabídku z necentrálního DNS, zavede se do Magionu ručně. V případě centrálních DNS se vytváří po jedné objednávce ke každé původní žádance, což je ručně prakticky nerealizovatelné. Nabídka se proto nejprve předá Inetu, který ji transformuje do sady dílčích objednávek, a ty automaticky vloží do Magionu. Po provedení finanční kontroly zkompiluje výsledné schválené objednávky opět do jediné souborné, která je pak odeslána vítěznému dodavateli k realizaci. Na ekonomickém zpracování vítězných nabídek z centrálních DNS se tedy Inet podílí dvojicí aplikací – *přenosem do Magionu* a *exportem objednávek*.

Přenosy do Magionu (`https://inet.muni.cz/app/dns/do_magionu`) zajišťují jednak import údajů o vítězném dodavateli a cenách do původních žádanek, a dále vlastní přenos těchto žádanek (pouze v rozsahu původně schválených položek) jako objednávek do Magionu. Jak importy tak přenosy jsou provázeny řadou kontrol (údajů o dodavateli vůči adresáři obchodních partnerů MU, cen vůči sazbám DPH, předpokládaných vs. vysoutěžených cen vůči chybám v desetinné čárce, zdrojů financování vůči aktuálně platným zdrojům aj.), které odhalují i neradostné skutečnosti typu zrušeného pracoviště, k němuž se váže část vysoutěžené nabídky, kterou je nezbytné uplatnit na některém jiném, dosud nic netušícím pracovišti?

Export objednávek (`https://inet.muni.cz/app/dns/do_excelu`) slouží k vygenerování excelovského souboru obsahujícího položky objednávek z daného sběru, schválených finanční kontrolou. Soubor je závaznou objednávkou pro vítězného dodavatele k realizaci dodávek a fakturaci.

5 Ještě krátce o podpůrných funkcích centrálních DNS a finanční kontrole v Magionu

Stěžejní komponenty centrálních DNS, jak byly výše popsány, mají samozřejmě celou řadu podpůrných funkcí, z nichž si některé zaslouží alespoň stručnou zmínku:

- Každý centrální DNS má kromě *harmonogramu sběrů* (`https://inet.muni.cz/app/dns/harmonogram`) také svůj *katalog předmětů* (`https://inet.muni.cz/app/dns/predmety`), který v případě kancelářských potřeb obsahuje i (foto)grafické náhledy téměř čtyř stovek předmětů.
- *Sestavy žádanek* (`https://inet.muni.cz/app/dns/sestavy`) poskytují superzadavatelům a superschvalovatelům přehledy žádanek a položek z jejich hospodářského střediska, s informacemi o aktuálním stavu schvalování a finanční kontroly.
- Prevence odkládání či propadání žádanek je zajišťována automaticky generovanými e-maily – *notifikacemi* – upozorňujícími zadavatele a schvalovatele na termíny harmonogramů a dosud neschválené žádanky či objednávky.
- *Přehled zadavatelů* (`https://inet.muni.cz/app/dns/prava_zadav`) vypisuje seznam zadavatelů podle pracovišť.

Finanční kontrola objednávek ručně nebo automaticky vložených do Magionu, která je jádrem

ekonomického zpracování vítězné, ekonomicky nejvhodnější nabídky, probíhá v menším rozsahu papírovou cestou (podpisy na průvodce vytištěné z Magionu), a v jednoznačně převažující míře elektronicky – prostřednictvím inetovské aplikace *Finanční kontrola objednávek* (`https://inet.muni.cz/app/obj/schvalObj`), pracující nad daty Magionu. Aplikace zobrazuje – nad rámec údajů pro finanční kontrolu standardních objednávek – srovnávací tabulku položek *schvalované objednávky* a položek *žádanky*, z níž objednávka vznikla.[4]

6 Shrnutí fungování DNS z pohledu zaměstnance MU

Potřebuje-li zaměstnanec MU nakoupit standardní kancelářské potřeby, standardní propagační předměty, standardní tiskařské služby, standardní kancelářské ICT vybavení, standardní kancelářský nábytek, dále kancelářskou a audiovizuální techniku nebo tonery, je třeba:

1. Obrátit se na manažera veřejných zakázek na svém hospodářském středisku, který posoudí, zda se jedná o zboží či službu pořizovanou v DNS (příp. tak učiní zaměstnanec sám), a v kladném případě se dále posoudí, zda se jedná o centrální či necentrální zboží či službu. Souborné katalogy předmětů centrálních DNS jsou zaměstnancům MU dostupné v Inetu, v aplikaci *Katalog předmětů* (`https://inet.muni.cz/app/dns/predmety`), odkud je lze exportovat do formátu XLS.
2. V případě necentrálního nákupu bude veřejná zakázka administrována v DNS na hospodářském středisku, a to většinou manažerem veřejných zakázek.

V případě centrálního nákupu zadá příslušný zadavatel žádanku do zaměstnancem požadovaného, zpravidla nejbližšího sběru požadavků. *Přehled zadavatelů* i *Harmonogramu sběrů* jsou opět k dispozici v Inetu (`https://inet.muni.cz/app/dns/prava_zadav` a `https://inet.muni.cz/app/dns/harmonogram`). Po zadání žádanky trvá přibližně dva měsíce, než je zboží dodáno, přičemž v dané době proběhne schválení žádanky, zahájení veřejné zakázky, hodnocení nabídek a výběr ekonomicky nejvhodnější nabídky, finanční kontrola a nakonec dodání a fakturace (podrobněji viz předchozí kapitoly). Zboží je dodáno na místo a v termínu, které jsou uvedeny v žádance.

7 A na závěr: Jaké jsou výhledy DNS na MU

Dalšími kandidáty na přívlastek „centrální“ jsou i takové DNS, jejichž předměty nebude možné plně popsat jen katalogem – například *tiskařské služby* nebo *propagační předměty*. Pro tyto DNS je v Inetu již nachystána potřebná podpora jak v aplikacích zadávání a schvalování položek žádanek (možnost připojit k položce soubor obsahující specifikaci předmětu), tak v aplikaci generující export žádanek (export excelovského souboru spolu se sadou specifikačních dokumentů, odkazovaných z příslušných řádků excelu).

Že jsou možnosti DNS skutečně široké a inspirující, ukazuje i příklad z diskusí s uživateli, v nichž zazněl námět na zřízení „burzy“ schválených položek, které byly odeslány do veřejné zakázky, a poté zadavatelské pracoviště zjistilo nedostatek zájmu či finančních prostředků.

Diskusi o dynamické nákupním systému provozovaném na MU uzavřeme zmínkou o domácích autorech: Servisní systém pro centrální DNS, realizovaný v Inetu, je společným dílem Odboru veřejných zakázek RMU, vývojového a provozního týmu Inetu a početného metodického týmu složeného z tajemníků a pověřených osob řady fakult a součástí MU. Kontakty pro uživatele jsou jednak pracovníci Odboru veřejných zakázek RMU a dále helpdeskový systém uživatelské podpory Inetu na adrese `https://inet.muni.cz/app/issue/ihelpMain`.

Na úplný závěr uveďme, že zadavatelé a dodavatelé mohou dnes již běžně užívat při zadávání veřejných zakázek elektronické nástroje.

[4] V aplikacích *Přenosy do Magionu* a *Finanční kontrola objednávek* se zúročila práce vložená v minulých měsících a letech do elektronizace procesů finanční kontroly (objednávek, závazků, cestovních příkazů a pohledávek), včetně nákladů vložených v této souvislosti do úprav systému Magion. K elektronizaci finanční kontroly se podrobněji vrátíme v některém z příštích čísel Zpravodaje.

Na Masarykově univerzitě je v provozu elektronický nástroj E-ZAK a interní aplikace pro veřejné zakázky v Inetu; kromě servisních aplikací pro centrální DNS popsaných v tomto článku je v Inetu i *Správa veřejných zakázek* zadávaných v listinné podobě a prezentovaných na veřejných stránkách MU (`https://inet.muni.cz/app/w3mu/verejne_zakazky`, `http://www.muni.cz/general/public_tenders`). Do budoucna však v elektronizaci veřejných zakázek, tzn. i na Masarykově univerzitě, zůstává k zodpovězení a řešení spousta otázek, například jak dosáhnout souladu elektronického nástroje a spisové služby, nebo jak zefektivnit zadávání veřejných zakázek v dynamickém nákupním systému, např. zkrácením lhůt. Ale to je již otázka i pro Evropskou unii a změnu jejích směrnic pro veřejné zadávání. □

Stavební pasport MU, import a export grafických dat a automatické generování kót

Petr Kroutil, Martin Vytrhlík, ÚVT MU

1 Stavební pasport MU

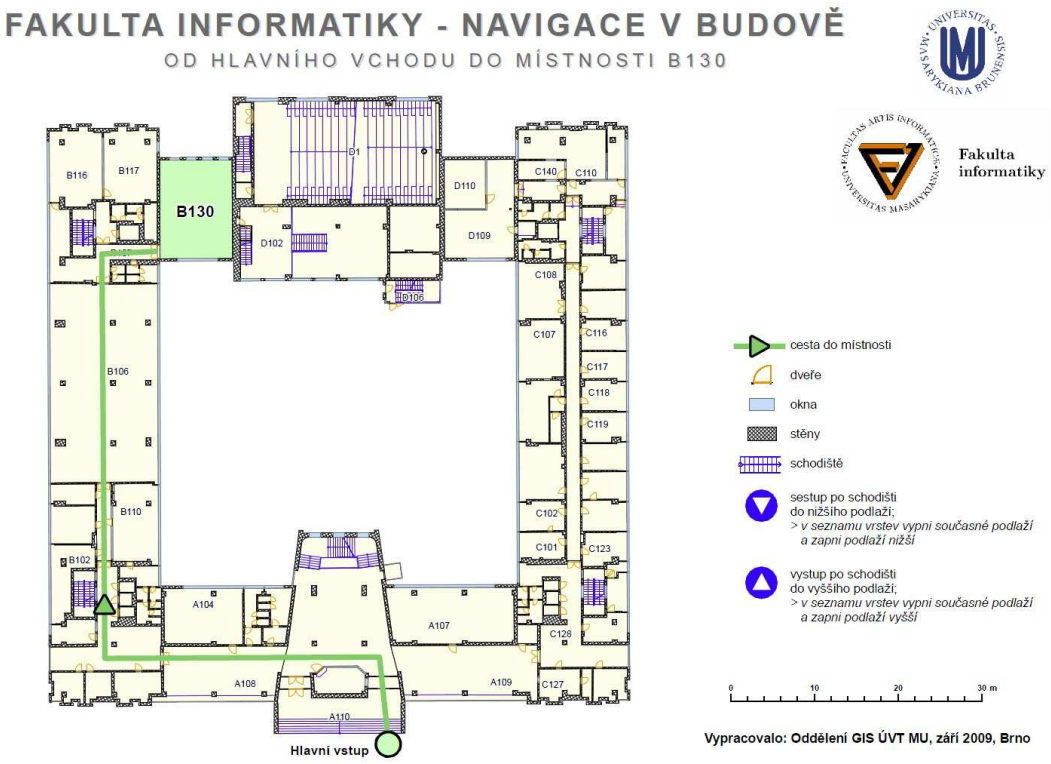
Masarykova univerzita je instituce, v jejímž rámci se potkává zhruba 35 tisíc studentů a 4 a půl tisíce zaměstnanců. Toto setkávání se odehrává v přibližně 250 budovách, 20 500 místnostech, na 366 000 m^2. Tato čísla byla před šesti lety menší, ale už tehdy jsme si kladli otázku, zda je vhodné udržovat stavební dokumentaci ke každé budově odděleně a ve formátech, které se velmi špatně aktualizují a publikují. Odpovědí na tuto otázku byla myšlenka na Stavební pasport MU. Základní paradigmata zněla zhruba takto:

- Získávat a udržovat aktuální stavební dokumentaci.
- Možnost poskytovat dokumentaci na požádání ve formátu a formě vhodné pro uživatele.
- Pasport by měl být použitelný pro provoz a správu budov a místností.
- Používáním stavebního pasportu by mělo dojít k optimalizaci využití budov a místností a potažmo ke snížení nákladů na provoz.

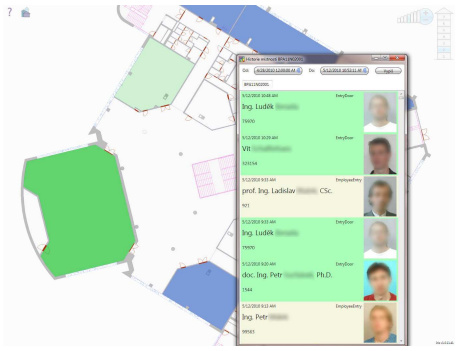
Za šest let práce se nám stavební pasport MU podařilo vybudovat a své využití našel v mnoha oblastech. Ty lze rozdělit do dvou skupin – využití stavebního pasportu samotného a využití stavebního pasportu jako podkladu v jiných aplikacích či informačních systémech.

Grafickou část stavebního pasportu si může prohlížet každý zaměstnanec či student univerzity na adrese `https://gisweb.muni.cz/Pasport`. Tato webová aplikace je interaktivně provázaná s webovou aplikací pro procházení atributové části stavebního pasportu, která pracuje v rámci Integrovaného a řídicího systému MU (`http://inet.muni.cz`). Zde lze zjistit informace o výměrách místností v rámci jednotlivých budov, výměrách ploch podlah dle jejich povrchu např. pro potřeby úklidu, výměrách stěn a stropů dle povrchů pro potřeby malování apod. Lze zde také vytvářet sestavy účelů místností. Stavební pasport MU jsme navrhli tak, aby z něj bylo možné vytvářet 3D modely na přání. Příklady 3D modelů budov ve formátu KMZ zobrazitelném v programu Google Earth můžete nalézt na adrese `//maps.muni.cz`. Fakultě informatiky jsme na přání vytvořili navigační plánky ve formátu PDF pro přístup do jednotlivých posluchárен a učeben, které je možno stáhnout z interaktivních rozvrhů Informačního systému MU. Jsme schopni generovat plánky či výkresy podlaží a místností na požádání v různých formátech. Problematice importu a exportu dat stavebního pasportu se věnujeme podrobněji v dalších kapitolách tohoto článku.

Stavební pasport se MU používá jako podklad v různých aplikacích, kde je vhodné vizualizovat různá prostorová data či děje anebo provádět analýzy na základě prostorového kontextu. Zde je několik příkladů: Informační systém pro správu Brněnské akademické počítačové sítě používá našich plánů k lokalizaci zařízení a komponent této sítě. Aplikace pro správu majetku umožňuje lokalizovat vybranou věc opatřenou kódem DHM v místnosti, popř. zobrazit, jaký majetek je vybrané místnosti přiřazen. Oddělení vývoje systémových služeb ve své aplikaci používá grafickou část stavebního pasportu pro vizualizaci a ovládání Elektronického zabezpečovacího systému (EZS) a Elektronické kontroly vstupu



Obrázek 1: Navigace v budově.



Obrázek 2: Aplikace pro správu a vizualizaci

(EKV) pro studovny a učebny.

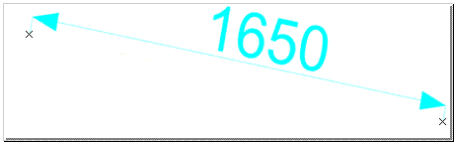
Další informace můžete získat v článku [1] z roku 2009.

2 Import grafických dat

Grafická data stavebního pasportu jsou udržována a publikována pomocí geografického informačního systému (GIS) – informační systém pro získávání, ukládání, analýzu a vizualizaci dat s grafickou složkou. Nerozhodli jsme se pro CAD (computer-aided drafting), který se ve vztahu k budovám nabízel a který využívaly informační systémy pro zprávu dat o budovách v době zakládání stavebního pasportu MU, protože data uložená v GIS jsou topologicky správná a je jim možno přiřazovat symboliku na přání. Více k této problematice v [1] .

Všechna data stavebního pasportu ale nejsou vytvářena přímo v GIS. Značnou část grafických dat získává univerzita ve formátu DWG, což je obvyklý výstup programu AutoCAD užívaný projektanty staveb. Z tohoto důvodu byl od začátku výstavby datového skladu grafické části stavebního pasportu MU vyvíjen nástroj pro automatické načítání výkresů ve formátu DWG. Výkres samozřejmě musí dodržovat pevně stanovenou strukturu popsanou v metodice stavební pasportizace MU.

Problém importu dat jsme zvládli poměrně snadno. Větší problémy činí nutnost oprav grafických dat předávaných ve formátu DWG, protože AutoCAD nedisponuje tak mocnými nástroji pro topologickou kontrolu jako GIS.



Obrázek 3: Kóta délky 1650 mm.

3 Export grafických dat

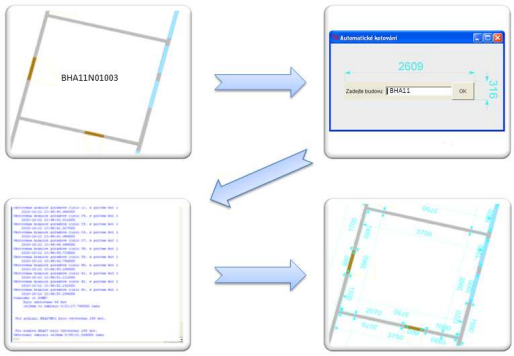
Námi užívané nástroje GIS firmy ESRI umožňují generovat velice jednoduše kvalitní mapové výstupy s přidanou symbolikou na přání ve většině obrazových formátů, jako jsou BMP, PNG, GIF, JPEG apod. Samozřejmě lze vytvářet i mapové dokumenty ve formátu PDF. Vzhledem k tomu, že jsme od počátku uvažovali o stavebním pasportu MU jako o jednotném skladu stavební dokumentace budov MU, snažili jsme se vytvořit nástroj pro export grafických dat do formátu DWG, aby bylo možno generovat na přání dokumentaci ve formátu akceptovatelném a editovatelném stavbaři. Tento úkol se nám dlouho nedařilo splnit, protože proklamovaná podpora exportu do DWG v nástrojích firmy ESRI se neukázala tak silná. Nakonec jsme však uspěli i při řešení tohoto úkolu. Do generovaných výkresů jsou přidávány informace z atributové části stavebního pasportu ve struktuře popsané v metodice stavební pasportizace MU.

4 Jedno malé ale – kóty

Import i export grafických dat z DWG do geodatabáze a opačně jsme zvládli, avšak s jednou výjimkou. Touto výjimkou jsou kóty.

V našem případě rozumíme pod pojmem kóta grafické znázornění délky s informací o vzdálenosti dvou bodů (mimo jiné existují také kóty úhlů, poloměrů, průměrů atd.). Námi použitá kóta reprezentuje nejkratší vzdálenost mezi dvěma body (viz Obr. 3). Stavební pasport (a stavební a technické výkresy obecně) s využitím kót jasně a srozumitelně prezentuje rozměry stavebních prvků.

Import kót byl natolik komplikovaný a kvalita kót tak špatná, že jsme se jejich importu až na výjimky vyhýbali. Poté jsme samozřejmě neměli



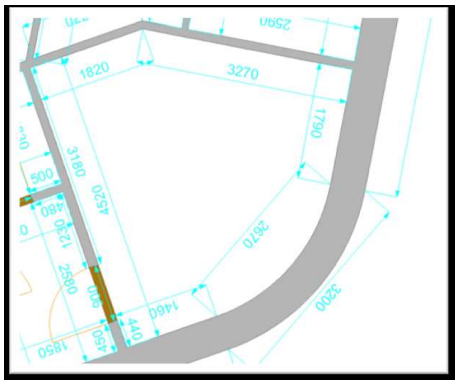
Obrázek 4: Práce s aplikací pro automatické generování kót.

co exportovat, a tak jsme dočasně kóty vytvářeli ručně. Věděli jsme, že se jedná o neudržitelný stav, proto jsme hledali nějaké vhodné řešení. Nabízel se nástroj pro automatizované generování kót v programu AutoCAD. Ten se nám však zásadně neosvědčil. Jiný automatický nástroj vyhovující našim potřebám jsme nenašli. Proto jsme se rozhodli vytvořit automatický nástroj pro generování kót přímo nad úložištěm grafických dat. Tento úkol jsme svěřili v rámci diplomové práce Martinu Vytrhlíkovi [2].

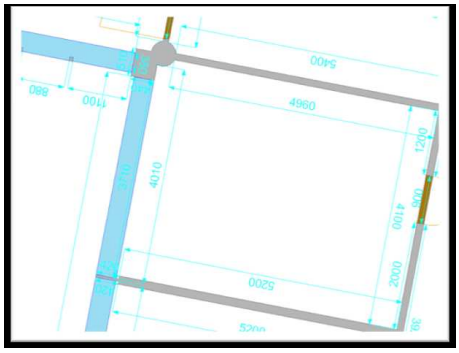
5 Automatické generování kót

Nástroj pro automatické generování kót umožňuje s využitím grafické reprezentace půdorysů stavebního pasportu vygenerovat kóty, které odrážejí skutečný stav tak, jak je zanesen v naší databázi. Jedná se tedy o „živé kóty“, nikoliv o kóty na základě starších výkresů (tyto mohou být vlivem proběhlých stavebních úprav neaktuální). Nástroj je realizován v jazyce Python a využívá modulů, které firma ESRI nabízí pro snadný přístup k datům ve své aplikaci. Díky tomu je možné pracovat právě s aktuálními daty stavebního pasportu MU.

Práce s tímto nástrojem umožňuje snížení časové náročnosti a pracnosti tvorby kót. To je velkým přínosem zejména při velkém množství nových podkladů, které je potřeba okótovat. Tak tomu bylo například při přebírání nových budov Univerzitního kampusu Bohunice do užívání. Výsledkem běhu nástroje není optimální okótování (definice optimálnosti se ostatně liší v závislosti na profesi i na konkrétních lidech), a to zejména



Obrázek 5: Příklad výstupu nástroje I.



Obrázek 6: Příklad výstupu nástroje II.

proto, že některé kóty je možné odebrat a výsledek zůstane pro uživatele čitelný. Tyto přebytečné kóty (jedná se o velmi malé procento) je snadné při zběžné kontrole odstranit.

Výsledek běhu nástroje v několika příkladech ilustrují obrázky 5, 6.

6 Shrnutí

Data stavebního pasportu obohacená o kóty umožňují generovat výkresy jako podklady pro různé rekonstrukce, rozvrhování nábytku na pracovišti v případě stěhování atd. Výkresy a plány jsme schopni dodávat v požadovaném formátu. Zaměstnanci Masarykovy univerzity tak mají přístup k aktuálním datům bez nutnosti dalekosáhle prohledávat archivy s často neaktuálními daty, ať už ve formě svazku papírových výkresů nebo ve formě digitálních dat.

7 Výhled

V současné době poskytujeme výstupy ze stavebního pasportu na požádání. Chtěli bychom však vybudovat portál pro automatizované poskytování dokumentace ve zvoleném formátu na základě autentizace uživatele. Tento přístup by ušetřil čas jak nám, tak uživatelům stavebního pasportu MU.

Literatura

[1] Petr Kroutil. Stavební pasport MU v současnosti. Zpravodaj ÚVT MU, 2009, `http://www.ics.muni.cz/bulletin/articles/619.html`

[2] Martin Vytrhlík. Automatizované generování kót stavebních objektů. Diplomová práce FI MU, 2009, `http://is.muni.cz/th/134576/fi_m/Diplomova_prace.pdf` □

DNSSEC

Bohuslav Moučka, Radim Peša, ÚVT MU

Jednou z klíčových součástí dnešní internetové infrastruktury je systém doménových jmen (DNS – Domain Name System). Jde o hierarchickou databázi umožňující vzájemný převod textových jmen uzlů počítačové sítě a číselných IP adres.

DNS pro překlad adres používají prakticky všechny internetové služby. O to víc zarážející je fakt, že dodnes používaný systém DNS postrádá jakékoli bezpečnostní mechanismy. Uživatel DNS nemá možnost si ověřit pravdivost nebo původ získaných informací, protože protokol neobsahuje mechanismus pro kontrolu přenášených dat.

Bylo již popsáno několik způsobů útoku (např. v [1]) na důvěryhodnost dat poskytovaných systémem DNS. Použité techniky se různí, ale ve výsledku získává klient podvržené údaje. Například když chce klient přistoupit www prohlížečem na stránky svého oblíbeného internetového bankovnictví www.nejakabanka.cz, musí dojít k převodu jména `www.nejakabanka.cz` na příslušnou IP adresu. To zprostředkovává dotazem na přednastavený DNS server DNS klient v operačním systému. Na dotaz odpoví buď přímo předdefinovaný a dotazovaný DNS server nebo pokud odpověď nezná, dotazuje se dalších

DNS serverů v DNS infrastruktuře. Jak již bylo řečeno, současný způsob DNS komunikace nenabízí prostředky, které by umožnily ověřit, zda výsledně získaná IP adresa opravdu přísluší původně dotazovanému DNS jménu. Pokud někde v infrastruktuře DNS serverů dojde k úspěšnému podvržení IP adresy internetového bankovnictví `www.nejakabanka.cz` nemá ani předávající DNS server a ani DNS klient žádnou možnost ověřit si, zda je IP adresa, kterou obdržel, správná. Internetový prohlížeč následně může být přesměrován například na počítač útočníka, kde může probíhat další etapa útoku třeba v podobě pokusu o sběr hesel, zneužití chyby v internetovém prohlížeči atd.

Jako příklad úspěšného útoku na DNS je možné uvést mediálně známý případ podvržení DNS údajů, kdy v roce 1997 využil Eugene Kashpureff chybu v DNS serverech k přesměrování stránek registrátora InterNIC na svůj server AlterNIC.

1 Přichází DNSSEC

Jako obrana proti možnému podvržení dat poskytovaných DNS infrastrukturou bylo po řadu let vyvíjeno rozšíření DNS pojmenované DNSSEC (*Domain Name System Security Extensions*). Jeho příprava nebyla jednoduchá, za počátek vývoje se dá považovat RFC 2065 vydané už v roce 1997. Tato původní představa byla dále upravována a rozpracována a v roce 1999 vychází RFC 2535, které již mělo být základem pro funkční implementaci a nasazení DNSSEC v systému DNS. Bohužel specifikace se ukázala jako neživotaschopná, především kvůli problémům se škálovatelností. Proto byla v následujících letech připravena výrazně změněná specifikace. Pro odlišení od předchozí verze byla označována jako DNSSEC-bis. Její vývoj byl v roce 2005 završen standardizací v podobě dokumentů RFC 4033, RFC 4034 a RFC 4035. Ani specifikace DNSSEC-bis však nebyla dokonalá. Je pikantní, že přestože se jedná o protokol definovaný primárně pro zvýšení bezpečnosti, přinesl novou bezpečnostní zranitelnost v podobě možnosti vylistování celého doménového prostoru (zonewalking). Tento problém byl vyřešen v roce 2008 vydáním RFC 5155, které definuje nový druh záznamu pojmenovaný NSEC3.

Vzhledem k popsané historii vývoje specifikace protokolu DNSSEC není velkým překvapením, že používání protokolu DNSSEC není ani dnes zdaleka standardem. Možná se ale blýská na lepší časy. Ke zrychlení šnečího tempa šíření DNESSEC technologie by mohlo výrazně přispět podepsání kořenové domény, ke kterému došlo 15. července 2010. Podepsání kořenové domény výrazně zjednodušuje řešení problémů s údržbou pevných bodů důvěry a vytváření řetězu důvěry (viz dále). Věřme, že spolu s vyřešením dětských nemocí předchozích verzí specifikace se podpis kořenové domény stane akcelerátorem reálného využití DNSSECu.

2 Jak DNSSEC funguje?

DNSSEC zajišťuje kontrolu původu a pravosti dat, ale jeho cílem není zajištění důvěrnosti dat (přenášená data nejsou šifrována) a ani přímo nechrání před útoky na dostupnost služby. Pro zajištění kontroly integrity přenášených informací využívá DNSSEC nástroje asymetrické kryptografie. Zjednodušeně řečeno je vlastně každý DNS záznam podepsán a autenticitu záznamu je možné zjistit ověřením příslušného podpisu. Samotná realizace je však komplikovanější. Mimo jiné přibylo několik nových typů DNS záznamů:

- RRSIG (Resource Record Signature) – obsahuje digitální podpis příslušné množiny DNS záznamů.
- DNSKEY (DNSSEC public key) – obsahuje veřejný klíč, jehož odpovídajícím privátním klíčem jsou podepsány DNS záznamy této domény.
- DS (Delegation Signer) – je umístěn v nadřazené DNS doméně a obsahuje otisk veřejného klíče uloženého v DNSKEY záznamu podepsané domény. Pomocí DS záznamů se vytváří řetěz důvěry do nadřazených domén.
- NSEC (Next Secure) – využívá se pro informaci o neexistenci dotazovaného záznamu.
- NSEC3 (Next Secure v.3) – využívá se pro informaci o neexistenci dotazovaného záznamu. Na rozdíl od NSEC záznamu neobsahuje jména, ale jen jejich otisky.

Do hlaviček DNS zpráv byly zavedeny nové příznaky:

– AD (Authenticated Data) – indikuje, že všechna data v sekcích odpověď a autorita byla ověřena a jsou správná.
– DO (DNSSEC OK) – v dotazu určuje, že server požaduje validaci dat pomocí DNSSEC.
– CD (Checking Disabled) – určuje, že server má vrátit data, i když validace nebyla úspěšná.

Pro ověření libovolného digitálního podpisu je nezbytné znát z důvěryhodného zdroje veřejný klíč podepisující entity. V případě DNS je samozřejmě nereálné, aby dotazující se klient (případně ověřující DNS server) znal veřejné klíče všech DNS domén, se kterými komunikuje. Proto DNSSEC používá systém pevných bodů důvěry a řetězu důvěry. DNS klient zná veřejné klíče pouze několika vybraných DNS domén – pevných bodů důvěry. Veřejné klíče jejich poddomén může získat zřetězením otisků klíčů z DS záznamů jednotlivých poddomén, které jsou uloženy v podepsané doméně, a příslušných veřejných klíčů jednotlivých poddomén obsažených v jejich DNSKEY záznamech. Tímto zřetězením DS a DNSKEY záznamů vzniká tzv. *řetěz důvěry*, který umožňuje DNS klientu získat důvěryhodným způsobem veřejné klíče libovolné podepsané poddomény. Letošní podpis kořenové domény umožní využít tuto doménu jako nejvyšší pevný bod důvěry a ulehčí DNS serverům, protože si nebudou muset udržovat seznam různých bodů důvěry. Klíč kořenové domény je publikován na serveru `www.iana.org`.

3 Ověřování (validace) DNS záznamů

Ověřování (validace) DNS záznamů se obvykle provádí na úrovni tzv. rekurzního DNS serveru, který dostává dotaz od DNS klienta a zajišťuje veškerou komunikaci s ostatními DNS servery. Na klienta se vrací až výsledek dotazu.

Rekurzivní DNS server si při DNSSEC validaci nejprve ověří pravost DS a DNSKEY záznamů v kořenové doméně pomocí veřejného klíče kořenové domény, který má zapsán ve své konfiguraci. V následujících krocích dostane vždy kromě IP adres autoritativních DNS serverů také DS záznam podřízené domény a pomocí něj si ověří DNSKEY záznam v podřízené doméně. V posledním kroku získá kromě původně hledaného DNS záznamu také RRSIG záznam, kterým ověří původně hledaný záznam. Pokud je vše v pořádku, rekurzivní server v DNS zprávě pro dotazujícího se klienta nastaví příznak AD (Authenticated Data), v opačném případě se zpráva vrátí s příznakem SERVFAIL a klient špatnou odpověď vůbec nedostane. Jestliže dotazovaná doména DNSSEC nepodporuje, server nedostane žádné DS, DNSKEY ani RRSIG záznamy z této domény a vrací obvyklou DNS odpověď, která není ověřena pomocí DNSSEC.

Pokud chceme, aby náš DNS server ověřoval záznamy z cizích domén, musíme na něm mít zapnutou validaci. Server BIND verze 9.5 a vyšší má validaci implicitně zapnutou. Aby server mohl ověřovat pravost záznamů, musí mít k dispozici klíč kořenové domény. Ten zapíšeme do konfiguračního souboru serveru verze BIND-9.6 příkazem:

```
trusted-keys {
. 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQb
SEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RS
tIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9Vn
MVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68Lsv
PVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA
2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ5
7relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1d
fwhYB4N7knNnulqQxA+Uk1ihz0=";
}
```

V případě verze BIND-9.7 můžeme použít příkaz, který zajistí automatickou aktualizaci klíče, bude-li změněn:

```
managed-keys {
"." initial-key 257 3 8
"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQb
SEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RS
tIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9Vn
MVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68Lsv
PVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA
2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ5
7relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1d
fwhYB4N7knNnulqQxA+Uk1ihz0=";
};
```

4 Podpis DNS zóny

Majitel domény, která má být zabezpečena, vygeneruje privátní a veřejný klíč. Privátním klíčem podepíše záznamy uložené v DNS a musí jej chránit před zneužitím, veřejný klíč slouží k ověření pravosti těchto podpisů. Je doporučeno pro

každou doménu vygenerovat 2 dvojice klíčů. Klíč ZSK (Zone Signing Key) podepisuje jednotlivé záznamy v doméně, je kryptograficky slabší a bývá častěji měněn. Klíč KSK (Key Signing Key) by měl být kryptograficky silnější a slouží k podpisu záznamů obsahujících ZSK. Při použití serveru BIND můžeme klíče vygenerovat například pro doménu muni.cz příkazy:

```
dnssec-keygen -a NSEC3RSASHA1 -b 1024 \
     -r /dev/urandom -f KSK muni.cz

dnssec-keygen -a NSEC3RSASHA1 -b 1024 \
     -r /dev/urandom  muni.cz
```

Oba příkazy vygenerují dva soubory, v souboru s příponou .key je veřejný klíč ve tvaru DNSKEY záznamu a v souboru s příponou .private je soukromý klíč.Veřejné klíče je třeba přidat do zónového souboru domény, kterou podepisujeme. Potom můžeme doménu podepsat příkazem:

```
dnssec-signzone muni.cz
```

Po spuštění tohoto příkazu vznikne nový soubor `muni.cz.signed`, který bude kromě původních informací obsahovat záznamy RRSIG a NSEC3. Záznamy typu RRSIG jsou přidány za každý RRSet, což je skupina záznamů stejného názvu a typu a slouží ke kontrole pravosti předchozích záznamů. Záznam obsahuje také data začátku a konce platnosti podpisu, která můžeme zadat při podpisu domény. Záznam NSEC3 obsahuje informaci o následujícím záznamu v setříděné doméně a informaci o všech existujících typech tohoto záznamu. Pokud se dotážeme na neexistující jméno, vrací DNS server NSEC3 záznam, který je před a za dotazovaným jménem. Záznamy NSEC3 neobsahují jména, ale jen otisky, takže je nelze použít ke získání seznamu všech záznamů v doméně, což je považováno za bezpečnostní problém. Při podpisu domény vznikne také soubor s názvem dsset-muni.cz obsahující DS záznamy, které je třeba umístit do nadřazené domény (cz). V souboru keyset-muni.cz je zapsán KSK klíč, který byl použit pro podpis domény. Tyto dva soubory jsou ekvivalentní v tom smyslu, že DS záznam se vypočítává z klíče a názvu domény. DS záznamy je možné umístit do domény cz prostřednictvím registrátora (pokud podporuje DNSSEC), kterému předáme KSK klíč.Vzhledem k tomu, že kořenová doména je již podepsána a klíč domény cz je v ní zaregistrován, vznikl tak řetěz důvěry. Pokud všechny sekundární DNS servery naší domény podporují DNSSEC, mohou všechny DNS servery, které jsou nakonfigurovány tak, že validují DNSSEC záznamy, ověřovat platnost záznamů z naší domény.

5 DNSSEC na MU

Doména muni.cz byla v návaznosti na podpis kořenové domény a domény .cz podepsána v srpnu 2010. V listopadu byla experimentálně zapnuta validace DNSSECu na serverech `ns.muni.cz` a `ns1.muni.cz`. Během dvou dnů však servery nahlásily chyby při validaci záznamů u 258 domén, z toho 88 v doméně cz. V mnoha případech existuje pro danou doménu DS záznam v nadřazené doméně, ale doména není podepsaná. Tento stav vede k tomu, že validující DNS server dostane informaci, že doména je podepsaná, ale podpis jejích záznamů není možné ověřit a vrací chybu. Následkem toho se záznamy v těchto doménách jeví jako nedostupné. Vzhledem k možnému dopadu na uživatele byla validace na těchto serverech pozastavena. Věřme, že ne na dlouho.

Literatura

[1] Suranjith Ariyapperuma, Chris J. Mitchell. *ARES '07 Proceedings of the Second International Conference on Availability, Reliability and Security*. ISBN:0-7695-2775-2 □

Inovační vouchery

Tomáš Pitner, FI MU a Jan Pavlovič, CTT MU

1 Kdo zaplatí aplikovaný výzkum?

V posledních letech se hodně mluví o reformě vědy směřující k podpoře inovací, tedy procesu, kdy z nápadů vznikají produkty přinášející zisk. Viditelným výsledkem je vyšší podpora aplikovaného výzkumu prostřednictvím nových grantových struktur, jako je Technologická agentura ČR (TAČR), v očích řady vědců spatřovaná spíše

jako nepřímá podpora firem a nikoli vysokoškolské vědy. Ucházet se rovnou o velký projekt typu TAČR navíc není pro vysokoškolské pracoviště vůbec triviální a vyžaduje průmyslového partnera s delší zkušeností ze vzájemné spolupráce a velkou vzájemnou důvěrou.

Bariér bránících rozběhu inovační spolupráce mezi vysokou školou a firmou je ale více. Je známým faktem, že nejvíce inovací vzniká v menších firmách, často zakládaných studenty právě proto, aby zhodnotili vlastní nápad. V Česku ještě léta potrvá, než budeme mít kromě nápadů také rizikový kapitál, který do takových firem do začátku investuje. Proto to bez veřejných zdrojů jde zpočátku špatně.

V rozpačité situaci ohledně spolupráce s výzkumnými institucemi ale stojí i firmy větší a kapitálově silné, které s vysokou školou spolupracovat chtějí, nemají ale dosud žádné zkušenosti ani dostatečnou důvěru ve funkčnost spolupráce. Všem těmto zájemcům se město Brno snaží v posledních dvou letech pomoci programem tzv. *inovačních voucherů* [1], který nabízí úhradu za inovativní služby poskytnuté vysokou školou firmě.

2 Přihlášky a výběr

Program voucherů je vyhlašován jednou ročně prostřednictvím *Jihomoravského inovačního centra* (JIC), vloni trval sběr žádostí do 25. září, letos končil již 17. června. Informace o výzvách najdete vždy na webu [1].

Proces je výrazně méně administrativně náročný než běžné grantové programy. Firma se dohodne s konkrétním týmem na vysoké škole (ne libovolné; součástí výzvy je seznam zapojených škol a ústavů Akademie věd) a zformuluje objednávku služeb pro podporu inovací. Předmět inovace není shora nijak dán ani omezen, záleží na dohodě obou stran – firmy a výzkumného pracoviště. Návrh je skutečně jednoduchý, postačí 1 strana A4 textu návrhu + rámcový rozpočet projektu. Výzva shora omezuje finanční objem zakázky – letos 200 tis. Kč, z čehož firma musí sama vložit 25% a zbylých 75% (tedy max. 150 tis.) dává město Brno. Jedna společnost smí v jedné výzvě požádat o nejvýše jeden inovační voucher. Na Masarykově univerzitě pomáhá s administrativou, ale i s vyhledáváním příležitostí a s formulací návrhů *Centrum pro transfer technologií*.

JIC na podaných žádostech prověří kritéria přijatelnosti, jež mohou návrh vyřadit kvůli nedostatku inovativnosti nebo pro nesplnění kvalifikačních předpokladů (např. v letošním roce byla podpora omezena na podnikající právnické osoby vč. družstev; živnostníci se účastnit nemohli). Vyhovující návrhy jdou následně do slosování. Vylosovaní příjemci – firmy – uzavřou v dané lhůtě (např. letos od konce června do října) s partnerským univerzitním týmem smlouvu, kde je plnění podrobně rozepsáno vč. plateb a časového rámce, který je sice v zásadě na dohodě firmy a výzkumného týmu, ale je současně ohraničen podmínkami výzvy. Letos vybrané vouchery musí být v každém případě hotové do června 2011 a firmám s dosud neukončenými projekty se nedovoluje podávání žádostí v dalším kole.

Podle dělby zodpovědností uzavírá smlouvu s firmou příslušné hospodářské středisko (HS) univerzity – tzn. fakulta, samostatné centrum nebo ústav, kde působí řešitelský tým. Dané hospodářské středisko zakázku následně garantuje. Dílčí vnitřní subdodávky od jiných ústavů a fakult jsou nicméně možné a v případě, že partnerských HS spolupracuje více, řeší se další vnitrouniverzitní smlouvou nebo sérií smluv na řešení projektu.

3 Zapojení MU v oblasti IT

Na Fakultě informatiky a Ústavu výpočetní techniky bylo v minulém (prvním) kole řešeno prostřednictvím voucherů několik projektů zaměřených na inovace v oblasti správy dokumentů (práce s novými formáty MS Office, vyhledávání v úložištích, metadata), dále byl podpořen systém Takeplace.eu poskytující kompletní servis pořadatelům odborných akcí, byly prováděny procesní analýzy menší firmy. Do procesu se letos zapojují i větší společnosti jako Microsoft a Aponia. V letošní výzvě uspěly z MU v oblasti IT konkrétně tyto projekty:

- *Návrh a implementace pokročilých funkcí pro komplexní systém podporující organizaci odborných akcí.* Žadatel: ACEMCEE, s.r.o., poskytovatel znalostí: FI MU, tým Tomáše Pitnera;
- *Metodiky a standardy pro postupy bezpečnostních týmů CSIRT.* Žadatel: AdvaICT, a.s., poskytovatel znalostí: ÚVT MU, oddělení bezpečnosti datové sítě;
- *Studie portovatelnosti mobilních aplikací v jazyce C na platformu Android.* Žadatel: Aponia Software, s.r.o., poskytovatel znalostí: FI MU, laboratoř Lasaris;
- *Adresářový systém pro integraci heterogenních videokonferenčních prostředí.* Žadatel: AV MEDIA, a.s., poskytovatel znalostí: ÚVT MU;
- *Optimalizace a evaluace algoritmů pro inhibiční zóny antibiotik.* Žadatel: LABMEDIASERVIS, s.r.o., poskytovatel znalostí: Mikrobiologický ústav LF MU;
- *Studie využitelnosti technologií MS Azure v oblasti enterprise integrace.* Žadatel: Microsoft, s.r.o., poskytovatel znalostí: ÚVT MU, tým Lukáše Rychnovského;
- *Transformace účtovacího modelu u inteligentních výdejních automatů.* Žadatel: PETROV Group, s.r.o., poskytovatel znalostí: ÚVT MU, tým Lukáše Rychnovského;
- *Analýza standardů a současného vývoje v oblasti Complex Event Processing.* Žadatel: MycroftMind, a.s., poskytovatel znalostí: FI MU, tým Tomáše Pitnera.

4 Závěrem

Inovační vouchery se ukazují jako vhodná, administrativně nenáročná cesta, jak podpořit nejen zaběhlou spolupráci s firmami, ale především vzájemného poznávání, neboť prostředky třetí strany eliminují nedůvěru ze strany firem a případná rizika. *Rižská deklarace o inovačních voucherech* [3] brněnskou zkušenost mezinárodně potvrzuje.

Výsledkem je prospěch obou stran. Firma pozná, co vysoká škola nabízí, který tým je dostatečně pružný, schopný reagovat na požadavky a přenášet univerzitní know-how do praxe. Pro vysokoškolským tým je to nezřídka první střet s komerčním světem, s jeho procesy i požadavky. V každém případě je získaný voucher přínosem pro obě strany. Odbourají se předsudky, získají první zkušenosti a v ideálním případě vybudují dlouhodobá partnerství pro řešení dalších společných projektů. Aplikovaný výzkum totiž nelze provádět bez odběratelů, jimiž bývají především firmy, a grantové programy (TAČR, Ministerstvo průmyslu, CzechInvest) jejich zapojení tvrdě vyžadují.

Pravděpodobně největší praktické zkušenosti v tomto ohledu mají kromě zmíněného Centra pro transfer technologií týmy *Laboratoře softwarových architektur (Lasaris)* [2] na Fakultě informatiky MU a *Oddělení vývoje systémových služeb* [4] na Ústavu výpočetní techniky MU. Firmám vouchery v některých případech pomohly i ke strategickému rozhodnutí přijít do Brna, do blízkosti univerzitních pracovišť. Celkově byly vouchery přiděleny již 90 firmám.

Z hlediska podaných žádostí bylo vloni z akademické sféry nejaktivnější VUT (97 žádostí), přičemž MU a Mendelova univerzita nabídly každá cca poloviční počet projektů. Letos s 80 nabídkami opět vede VUT, MU vložila do osudí 28 nabídek. Novinkou tohoto roku byla širší účast Akademie věd, nejaktivnější byl Ústav přístrojové techniky. Celkově se letos hrálo o 7,2 mil. Kč. Není důvod to příště nezkusit také!

Literatura

[1] Jihomoravské inovační centrum. Inovační vouchery. `http://www.inovacnivouchery.cz`

[2] T. Pitner a kol. Projekty Laboratoře softwarových architektur FI, `http://lasaris.fi.muni.cz/research-projects`

[3] Rižská deklarace o inovačních voucherech. `http://www.europe-innova.eu/c/document_library/get_file?folderId=132988&name=DLFE-9801.pdf`

[4] L. Rychnovský, M. Osovský. Služby Oddělení vývoje systémových služeb. Zpravodaj ÚVT MU. ISSN 1212-0901, 2010, roč. XX, č. 4, s. 3–7. □

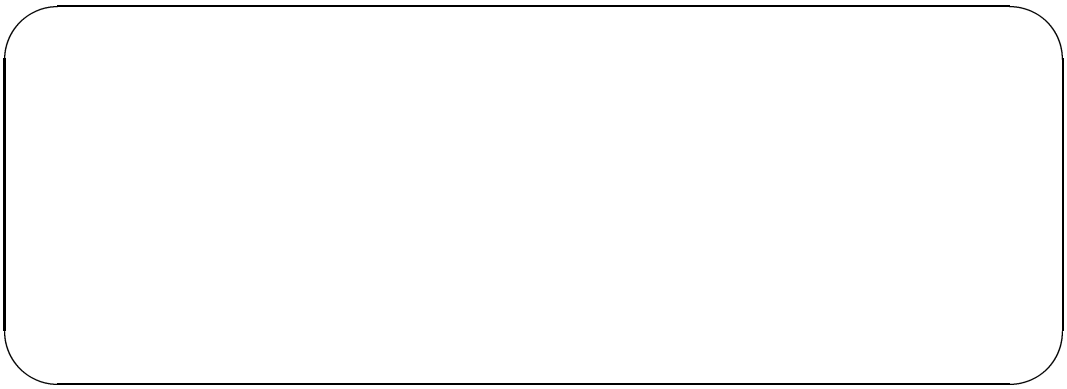
Vyzkoušejte: ebrary Academic Complete

Miroslav Bartošek, ÚVT MU

Jedním z letošních přírůstků na MU v oblasti elektronických informačních zdrojů je rozsáhlá kolekce elektronických knih *ebrary Academic Complete*, `http://site.ebrary.com/lib/masaryk`. Tato kolekce obsahuje na 50 tisíc odborných knih ze všech vědních oborů z produkce 300 nejvýznamnějších světových vydavatelů odborné a vědecké literatury. Pokud se podíváme jenom na oblast počítačů a informačních technologií, najdeme zde na 3 000 knih týkajících se programování, operačních systémů, software, zpracování dat a dalších témat. Uživatelé mohou knihy nejen vyhledávat, číst či tisknout jejich části. Po vytvoření osobního účtu mohou sestavovat svou osobní knihovničku, ve které lze knihy opatřovat elektronickými poznámkami, zvýrazňovat si části textu, připojovat ke slovům v textu hypertextové odkazy na externí zdroje na Internetu, sdílet své okomentované knihy s dalšími kolegy. Po instalaci speciálního čtecího programu ebrary Reader se repertoár funkcí ještě dále rozšíří – je například možné převádět texty z knih na hlasový výstup.

Další možnosti jsou již na vás, ebrary Academic Complete rozhodně stojí za vyzkoušení. Podrobnější informace ke zdroji naleznete na Portálu EIZ-MU, `http://ezdroje.muni.cz/prehled/zdroj.php?id=294`. □

Obsah



Editor: Miroslav Bartošek • Vydavatel: Masarykova univerzita • Žerotínovo náměstí 9, 601 77 Brno, CZ
tel.: 549 492 100 • e-mail: zpravodaj@muni.cz • WWW: http://www.ics.muni.cz/zpravodaj/
Sazba systémem LaTeX 2ε písmem LucidaBright • Tisk: Tribun EU s. r. o. • *Neprodejné* • ISSN: 1212–0901