Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

Bakalářská práce

Tomáš Rejnek

Technologie vzdáleného přístupu a jejich implementace na Univerzitě Karlově v Praze

Remote access technologies and their implementation at Charles University in Prague

Praha 2010

Vedoucí práce: Ing. Jiří Pavlík

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

V Praze, dne 12. 8. 2010

……..

podpis studenta

Identifikační záznam:

REJNEK, Tomáš. *Technologie vzdáleného přístupu a jejich implementace na UK = Remote access technologies and their implementation at Charles University in Prague.* Praha, 2010-08-12. 68 s. Bakalářská práce (Bc.). Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí bakalářské práce Jiří Pavlík.

Abstrakt (česky)

Bakalářská práce se zabývá problematikou vzdáleného přístupu k elektronickým informačním zdrojům. A to zejména ve vztahu k řešení dané problematiky na Univerzitě Karlově v Praze.

Práce se postupně věnuje následujícím aspektům dané problematiky. Nejprve stručně popisuje současný stav zpřístupňování elektronických informačních zdrojů na Univerzitě Karlově. Dále se práce zabývá teoretickými aspekty správy identit a přístupů, jež se stará o to, aby se k požadovaným zdrojům dostali oprávněné osoby. To také zahrnuje hlavní metody autentizace uživatelů, federační model a další. Samotná část je věnována Centrální autentizační službě, která má na Univerzitě Karlově správu identit a přístupů na starosti. Velký důraz je kladen na popis a zhodnocení hlavních technologií umožňujících vzdálený přístup jako VPN, Proxy servery, Shibboleth a další.

Závěr práce je věnován vyhodnocení průzkumu, který se zabýval oblíbeností a využitím jednotlivých metod vzdáleného přístupu studenty a zaměstnanci Univerzity Karlovy.

[Autorský abstrakt]

Klíčová slova (česky)

vzdálený přístup, autentizace, vpn, Shibboleth, proxy, elektronické informační zdroje, federace identit, ezproxy

Abstrakt (anglicky)

The bachelor thesis deals with the issue of remote access to electronic information resources and its solution at Charles University at Prague.

The bachelor thesis describes the following topics. Firstly, it describes the current state of electronic resources at Charles University. Then it provides some basic information about identity and access management, mainly focused on user authentication. Identity and access management ensures that right people access right resources. It involves federation identity management as well as main methods of user authentication. There is also described Charles University Central Authentication Service. Then comes the main part that describes the most important remote access technologies such as VPN, Proxy servers, Shibboleth and others.

The last part includes the evaluation of survey that was focused on popularity of individual remote access technologies. The survey has been done among the stuff and students of Charles University at Prague.

[Authors‘ abstract]

Klíčová slova (anglicky):

remote access, access management, authentication, vpn, Shibboleth, proxy, electronic information resources, federation identity management, EZproxy

OBSAH

PŘEDMLUVA

Tématem bakalářské práce jsou technologie vzdáleného přístupu k elektronickým informačním zdrojům a to především s ohledem na jejich implementaci na Univerzitě Karlově v Praze. Poskytnutí uživatelsky příjemného a zároveň bezpečného vzdáleného přístupu k elektronickým informačním zdrojům potřebných pro vědu a výzkum je v současnosti velkou výzvou nejen pro univerzity, ale pro celou knihovnickou sféru jako takovou.

Cílem práce je popsat a zhodnotit základní technologie vzdáleného přístupu. V práci budou také popsaný základní procesy, které jsou nutné k poskytnutí vzdáleného přístupu k elektronickým informačním zdrojům osobám, které na tyto služby mají nárok. Součástí bakalářské práce je vyhodnocení průzkumu, který se zaměřil na využití a oblíbenost jednotlivých technologií na Univerzitě Karlově (UK).

Práce je rozdělena do 7 hlavních kapitol (včetně závěru). Jednotlivé kapitoly se postupně věnují všem důležitým aspektům pro vzdálený přístup. Nejprve jsou popsány elektronické zdroje na UK, dále jsou popsány základní principy ověřování uživatelů, jejich implementace na UK v podobě Centrální autentizační služby, samotné technologie umožňující vzdálený přístup, implementace těchto metod do Portálu elektronických informačních zdrojů a na závěr je vyhodnocen výše zmíněný průzkum.

Pro zpracování bakalářské práce byly použity články českých i zahraničních odborných periodik, stejně tak monografií a dalších zdrojů převážně dostupných v síti Internet. Vycházel jsem také ze znalostí nabytých během konzultací s vedoucím práce.

Rozsah práce překračuje doporučené množství z důvodu použití mnoha grafů pro vyhodnocení průzkumu v závěrečné části. Všechny zdroje použité v práci jsou citovány dle norem ISO 690 a ISO 690-2 a jsou uvedeny v seznamu použité literatury na konci práci. V textu bylo použito tzv. Harvardského stylu citováni, kdy v hranaté závorce je nejprve uveden první údaj záznamu a poté rok vydání.

Na závěr bych chtěl především poděkovat vedoucímu práce Ing. Jiřímu Pavlíkovi, za věnovaný čas a potřebné znalosti k napsání této práce.

1 Elektronické informační zdroje na UK

Univerzita Karlova pro své studenty a zaměstnance zpřístupňuje obrovské množství elektronických zdrojů z oblasti vědy a výzkumu. Nejprve si objasníme, co se pojmem elektronické informační zdroje (dále jako EIZ) rozumí.

1.1 Definice a charakteristika EIZ

Nejprve si vymezme, co je **informační zdroj**. Informační zdroj (někdy se také používá výraz pramen) je objekt, který obsahuje dostupné informace odpovídající informačním potřebám uživatele. Informační zdroje můžeme dělit dle formátu na tištěný, zvukový, obrazový nebo elektronický (včetně zdrojů dostupných online). [Celbová, 2005a].

Elektronický informační zdroji je tedy informační zdroj, který je uchováván v elektronické (digitální) podobě a je dostupný v prostředí počítačových sítí nebo prostřednictvím jiných technologií distribuce digitálních dat. [Celbová, 2005b].

V této práci se budeme zabývat přístupem ke vzdáleným informačním zdrojům, které umožňují získat požadovanou informaci přímou interaktivní komunikací v reálném čase a to v prostředí celosvětové sítě Internet. Tyto EIZ se také dají označovat jednoduše jako **online zdroje** [Kučerová, 2005]**.**

Pod pojmem EIZ můžeme rozumět samotné dokumenty nebo také celé kolekce jednotlivých dokumentů, které mohou být zprostředkovány přes profesionální online databázové systémy.

Elektronické informační zdroje oproti svým klasickým předlohám mají mnohé výhody. Předně nejsou omezeny svojí fyzickou podstatou. Stačí si představit exemplář klasické knihy. Oproti její elektronické variantě může být k dispozici v jeden okamžik pouze jedné osobě. V elektronické verzi (tedy pokud je dostupná online) může být k dispozici v jeden moment neomezenému počtu uživatelů, kteří se mohou fyzicky nacházet po celém světě. S elektronickými informačními zdroji lze také mnohem efektivněji pracovat (viz funkce jako fulltextové vyhledávání apod.).

1.2 Typologie

Podle **typu informace** lze rozlišovat zdroje na primární, které nesou původní informaci, sekundární, které informují o primárních zdrojích a terciární, které logicky nesou informaci o zdrojích sekundárních.

Dalším možným dělením EIZ je na základě podmínek jejich **zpřístupňování**.

Licencované – zdroje, ke kterým lze získat přístup zakoupením licence. Licence může být formou předplatného, kdy je zdroj nakupován pouze na **omezené** časové období. To se týká zejména zdrojů, jejichž obsah je neustále doplňován. Druhá možnost je licence **trvalá**, po jejímž zakoupení je možné zdroj využívat po neomezenou dobu [Svršek, 2004].

Volně dostupné – zdroje, jejichž dostupnost není omezena žádnou licencí nebo jsou dostupné pod licencí, která umožňuje jejich využívání. A to pro jakékoliv nebo nekomerční využití, případně jinak specifikované. To umožňují například licence Creative Commons a další.

Free-trial (zkušební verze) – Zdroje, které jsou k užívání poskytnuty na omezenou dobu, ve které je možné zdroj testovat a rozhodnout se, zda se koupí licence.

Databázové elektronické informační zdroje můžeme dělit dle druhů dokumentů, které zpřístupňují:

Full-textové – zdroje obsahující plné texty dokumentů.

Bibliografické – zdroje, které neobsahují plné texty dokumentů, ale pouze informace o nich (název, autor, abstrakt, klíčová slova apod.). Plného textu je někdy možné dosáhnout pomocí nadstavbových služeb jako je např. SFX.

Faktografické – obsahují konkrétní údaje, např. statistické databáze.

1.2.1 Shrnutí

Dále v textu bude používáno termínů zdroj, informační zdroj, elektronický informační zdroj (EIZ) pro zastřešení jakékoliv výše zmíněného druhu, detailní rozlišování v rámci textu není třeba.

1.3 Akvizice EIZ na UK

Akvizice EIZ na UK probíhá na několika úrovních. Hlavním koordinátorem nákupu komerčních bibliografických, faktografických a fulltextových informačních zdrojů je **Ústřední knihovna**, která od roku 1996 slouží jako manažerské pracoviště pro oblast knihovnicko-informačního servisu na UK[Univerzita Karlova v Praze, 2004]. Většina zdrojů je pořizována na celo-univerzitní úrovni a to často také v rámci různých konsorcií. Konsorcia jsou seskupení několika subjektů (např. univerzit a vel-kých knihoven), které si dohromady koupí licenci k informačnímu zdroji. Takto pořízená licence vyjde pochopitelně pro jednotlivé subjekty podstatně levněji, než kdyby si každý licenci pořídil samostatně.

Dále se o nákup EIZ stará každá fakulta (případně na úrovni kateder a ústavů) dle svých konkrétních potřeb. To zejména pokud se jedná např. o nákup samostatných elektronických časopisů apod.

1.4 Správa EIZ na UK

Pro správu elektronických informačních zdrojů na UK je využíván software **Verde**, který je produkován společností ExLibris. Ve Verde jsou centrálně ukládány všechny podklady pro zpřístupnění elektronických zdrojů na UK- evidence předplatného a také využívání EIZ na UK. Pro správu EIZ je důležité, že se informace o jednotlivých zdrojích ukládají přesně a strukturovaně na jednom místě a jsou tedy lehce dosažitelné [Pavlík, 2008]. Podle těchto údajů jsou zpřístupňovány elektronické časopisy a knihy v Centrálním katalogu UK, v SFX UK, MetaLib UK a na Portálu elektronických zdrojů UK [Beitlová, 2010].

Pro obyčejné uživatele je tento nástroj prakticky neviditelný.

1.5 Dostupnost EIZ na UK

Univerzita Karlova zpřístupňuje svým studentům a zaměstnancům obrovské množství EIZ. Pro výuku a výzkum je dostupných 33 852 elektronických časopisů (údaj z června 2010) ve více než 100 databázích [PEZ, 2007]. Prostřednictvím databází předních světových vydavatelů (Thomson Reuters, Ovid a další) jsou dostupné také sborníky z vědeckých konferencí, kolekce elektronických knih, časopisů atd.

Ne všechny licencované zdroje jsou dostupné pro každého. Mnohdy také **zaleží na příslušnosti** ke konkrétní fakultě, oboru apod. Například pro studenty a zaměstnance Ústavu informačních studií a knihovnictví Filosofické fakulty je v současnosti dostupných 117 elektronických zdrojů.

Vzhledem k velkému množství nejrůznějších EIZ může být pro uživatele náročné se v nabídce zdrojů zorientovat. Tuto situaci se snaží řešit různé seznamy a **portály EIZ**, které jsou provozovány jako knihovní služby UK. Ty jsou zajišťovány Oddělením knihovnických aplikací Ústavu výpočetní techniky ve spolupráci s knihovnami UK. Některé z nich si stručně přiblížíme na následujících řádcích. Nejprve však rozlišíme způsoby přístupu k EIZ.

1.5.1 Přímý přístup X vzdálený přístup

Přístup k licencovaným EIZ na UK můžeme rozdělit na dva způsoby- **přímý** a **vzdálený**. Prvním a bezproblémovým způsobem je přístup přímý. **Přímý přístup** znamená, že k EIZ přistupujeme z počítače, který je **připojen na síť UK**. V takovém případě má uživatel přístup **ke všem zdrojům**, na které má nárok dle své příslušnosti k určité fakultě apod. Tento přístup je umožněn z veřejných PC stanic i registrovaným uživatelům jednotlivých knihoven. Přímý přístup je umožněn na základě IP adresy počítače (či dalšího koncového zařízení) a to neumožňuje přístup ke všem zdrojům (k většině však ano), bude vysvětleno dále v textu.

Vzdálený přístup je tedy logicky takový přístup, kdy se uživatel připojuje ke zdroji a **není** v danou chvíli **připojen** na síť UK. To je typicky případ, kdy chce uživatel pracovat z domova, internetové kavárny nebo prostě odkudkoliv, kde se může připojit na Internet. Přístup vzdálený je pouze pro studenty a zaměstnance UK[PEZ, 2007].

1.5.2 Portál elektronických informačních zdrojů

Portál elektronických zdrojů (PEZ, dostupný z http://pez.cuni.cz) je patrně nejdůležitějším místem pro přístup k EIZ. Odsud lze přistupovat ke **všem** licencovaným i volně přístupným zdrojům dostupných v rámci UK i jednotlivých fakult. Je to ideální místo pro vzdálené připojení k EIZ, které si ale více přiblížíme v 6. kapitole této práce.

1.5.3 Centrální knihovně-informační systém UK

Centrální knihovně-informační systém (CKIS, dostupný z http://ckis.cuni.cz/) je centrální katalog všech knihoven fakult a dalších součástí. Kromě klasických dokumentů lze centrální katalog použít také pro vyhledávání elektronických knih a elektronických časopisů a přímo z něj je také možné se dostat k plnému textu po přihlášení ke svému účtu [Baranayová, 2010].

1.5.4 Digitální univerzitní repozitář

Digitální univerzitní repozitář UK (dostupný z http://digitool.is.cuni.cz) je provozován v systému DigiTool společnosti ExLibris, který umožňuje dlouhodobou archivaci, správu a zpřístupňování elektronických dokumentů v nejrůznějších formátech. V současné chvíli obsahuje vysokoškolské kvalifikační práce a historické dokumenty Archivu UK. Na doplňování obsahu se však stále pracuje [Fojtů, 2007].

1.5.5 Portál elektronických časopisů

Portál elektronických časopisů (PEC) UK (dostupný z http://pec.cuni.cz) slouží k vyhledání časopisů dostupných v licencovaných i volně dostupných on-line databází. Je součástí služeb SFX serveru Univerzity Karlovy. SFX je technologie, která mimo jiné je schopna zprostředkovat plné texty dokumentů či vytvářet seznamy elektronických časopisů, což je funkce využita pro tvorbu PEC [Zach, 2010].

1.5.6 Metalib

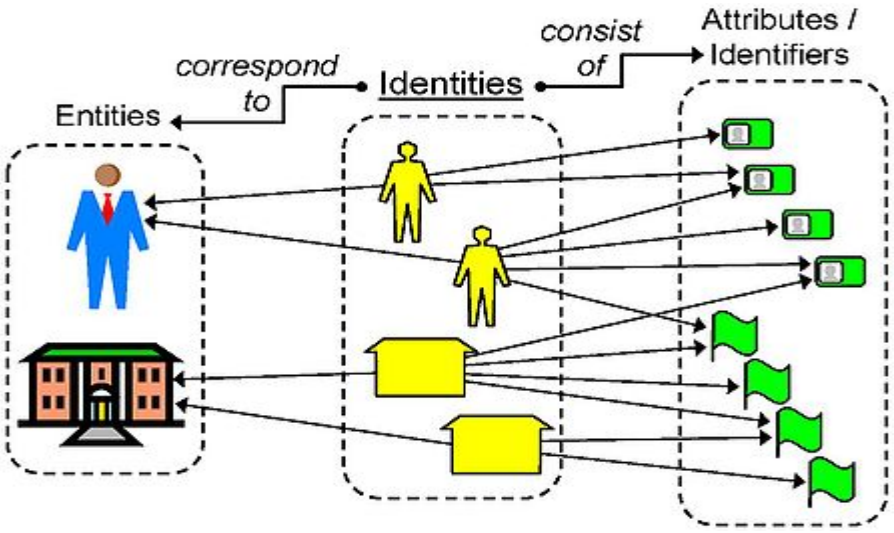
Metalib (dostupný z http://metalib.cuni.cz) je komerčním produktem firmy Ex Libris (stejně jako výše zmíněné SFX). Jedná se o tzv. federativní vyhledávač. To znamená, že je schopen paralelně prohledávat několik informačních zdrojů najednou. Jeho implementace na UK je v současnosti schopna prohledávat katalogy knihoven UK a některé předplácené databáze.

2 Správa identit a přístupů

Nedílnou součástí poskytnutí vzdáleného přístupu k elektronickým informačním zdrojům oprávněným uživatelům je kvalitní **správa identit** (v cizojazyčné odborné literatuře se označuje jako Identity and Access Management, IAM). Pojmem **správa identit a přístupů** se označuje komplex služeb, který poskytuje na základě definovaných politik bezpečné a automatizované řešení správních úkonů efektivně řešících **přístup** velké a trvale rostoucí komunity **uživatelů** (např. studenti či zaměstnanci univerzity) **k licencovaným** a mnohdy citlivým informačním zdrojům [Hanáček, 2005]. IAM je rozsáhlá disciplína, ve které se uplatňuje mnoho rozdílných přístupů k dané problematice. My si zde představíme jen některé nejdůležitější termíny a procesy úzce se vážící k tématu této práce.

2.1 Identita uživatele

Uživatel je entita (označována také jako **subjekt**) existující v reálném (fyzickém) světě. Entita nemusí být omezena pouze na lidi, ale může to být také instituce, počítačový software nebo cokoliv jiného, co může vyžadovat přístup k informačnímu zdroji. Pro získání přístupu ke zdroji se **entita odvolává na** svoji **identitu**. **Identita** je souborem informací o entitě, které se často označují jako **atributy**. **Atributy** jsou prvky, kterými se může entita jednoznačně prokázat. Zde pochopitelně hovoříme o digitální identitě, která se skládá z elektronicky zapsaných atributů [Windley, 2005]. Vztahy jsou názorně vyjádřeny na obrázku č.1.



Obrázek č.1: Vztah mezi entitami, identitami a atributy

Záznam uživatele (respektive atributů jeho identity) může být uložen v tzv. adresářové službě. **Adresářová služba** je aplikace **shromažďující** a **poskytující informace** o entitách (v našem případě uživatelé). Takovou službou může být **LDAP** (Lightweight Directory Access Protocol).

2.1.1 LDAP

LDAP byl původně pouze protokol používaný pro přístup k adresářům na vzdáleném serveru, který byl odlehčenou verzí protokolu X.500.

LDAP Protokol může být využit pro 3 základní operace:

- **Dotazovací operace** – pro vyhledávání v adresáři
- **Aktualizační operace** – pro úpravu záznamů v adresáři
- **Autentizační operace** – pro ověření identity

Nicméně postupem času se LDAP vyvinul v regulérní adresářovou službu (lze označit jako LDAP server[1]). Informace na LDAP serveru jsou uloženy v hierarchické stromové struktuře pomocí záznamu. Záznam v LDAP se skládá ze tří základních prvků:

- **Rozlišovací jméno** (Distinguished name)
- **Atributů**
- **Objektových tříd** [Howes, 2003].

Každý záznam je jednoznačně identifikovatelný pomocí svého rozlišovacího jména. **Záznam** je složen z jednotlivých **atributů** (vlastností popisované entity). Záznamy musí odpovídat povolenému schématu, což je soubor objektových tříd. Takovou třídou může být např. inetOrgPerson, což je obecná třída pro zápis atributů o uživatelích (resp. lidech obecně) [LDAP, 2006].

LDAP tedy může sloužit jako **adresář uživatelů**, vůči kterému se **uživatelé** mohou **autentizovat**. Své uplatnění našel i na Univerzitě Karlově v rámci Centrálních autentizačních služeb, které budou popsaný dále v textu.

[1] To je pochopitelně značné zjednodušení, avšak v rámci této práce dostatečné

2.2 Autentizace

Autentizace[2] je proces vedoucí k **ověření identity** uživatele (vymezení může být mnohem širší, ale zde se budeme zabývat právě autentizací uživatelů) [Huntington Ventures, 2006a].

Proces autentizace sestává z těchto dvou prvků: **získání autentizační informace** od uživatele a následně analýza těchto informací vedoucí k ověření, že skutečně náleží uživateli. Ověření probíhá vůči záznamu uživatele uloženého v adresářové službě.

Po procesu autentizace následuje obvykle **autorizace**, což je proces při kterém dojde k ověření, zda má uživatel právo dosáhnout požadovaných zdrojů či služeb.

Autentizační metody se nejčastěji rozdělují na 4 typy a to dle toho:

- co uživatel **zná**
- co uživatel **vlastní**
- čím uživatel **je**
- kde se uživatel **nachází** [Apelbaum, 2004].

V prvním případě se jedná o **abstraktní znalost**, kterou lze snadno zadat do počítače. Tou může být **heslo**, **PIN** (personal indetification number, osobní identifikační číslo) či přístupová **fráze**. Toto je metoda velice častá, ale také má značná bezpečnostní rizika.

V druhém případě se jedná o fyzické či digitální „předměty“, které se často označují jako **tokeny**. Těmi mohou být například **digitální certifikát** nebo čipová karta. Tato metoda je výhodná z bezpečnostního hlediska. Nevýhodou je, že uživatel musí mít token vždy v dosahu, aby se mohl autentizovat. Také zavádění do praxe bývá u této metody finančně náročné.

Třetí metoda je využití **biometriky**, tedy statického měření biologických vlastností, které můžou být kontrolované technickými prostředky. V praxi to znamená třeba skenování oční sítnice nebo kontrola otisků prstů (viz nové cestovní

[2] (totožný s termíny autentifikace a autentikace, proč je termín autentizace nejvhodnější se můžeme dočíst například zde [Behún, 2004])

pasy vydávané v České republice od 1. května 2009). Jeden z rozdílů oproti ostatním metodám je to, že nedává zcela konkrétní odpovědi (takové heslo platí nebo ne), ale pouze říká s jakou pravděpodobností se jedná o daného uživatele. Výhodou je, že ze strany uživatele nemůže dojít ke ztrátě (jako u tokenů) nebo k zapomenutí (jako u hesel) potřebných údajů [Krhovják, 2007].

Čtvrtou a poslední metodou je autentizace na základě IP adresy, kterou si více přiblížíme dále.

Aby se při současném zachování výhod těchto metod co možná nejvíce eliminovaly jejich nevýhody, je častým řešením jejich vhodná vzájemná kombinace. Použití metod ze dvou výše uvedených skupin se pak označuje jako **dvoufaktorová autentizace** a použití metod ze všech tří skupin jako **třífaktorová** autentizace [Krhovják, 2007].

Teorie kolem autentizace by vydala na samostatnou práci. Podrobněji si zde představíme pouze základní způsoby autentizace, které jsou nejčastěji využívány k ověření uživatelů vzdáleného přístupu k licencovaným elektronickým zdrojům v akademickém (či knihovnickém) prostředí. To je autentizace pomocí přihlašovacího jména (login) a hesla a autentizace na základě IP adresy, případně kombinace obojího.

2.3 Autentizace loginem a heslem

Nejjednodušší a také nejrozšířenější způsob autentizace. Kromě toho je to však také způsob nejméně bezpečný. S autentizací pomocí loginu a hesla se dnes setkáváme naprosto běžně. Přihlašovací jméno je údaj, který může být uživateli přiděleno nebo si ho může sám vybrat. Stejné je to s heslem s tím, že heslo přidělené náhodně systémem se obvykle musí změnit a to hlavně z důvodu zapamatovatelnosti.

Uživatel předkládá systému heslo (sdílené tajemství) společně se svou identifikací - uživatelským jménem (loginem). Systém tyto autentizační údaje kontroluje s daty uloženými k danému uživateli. Prokázání znalosti tajemství je vyhodnoceno systémem jako korektní prokázání identity.

Heslo je **řetězec znaků**, v ideálním případě netriviální, ale uživatelem snadno zapamatovatelný [Krhovják, 2007]. Netriviální znamená kombinaci různých znaků jako malá a velká písmena, číslice či další speciální znaky. **Důležitost** netriviálnosti

spočívá hlavně v **bezpečnosti**. V dnešní době existuje nespočet softwarových i hardwarových způsobů používaných k získání uživatelova hesla. Jmenujme alespoň tzv. brutální útok, kdy útočník zkouší (samozřejmě automaticky za pomocí softwaru, kterých lze třeba na Internetu nalézt celá řada) náhodně různé kombinace znaků či slovníkový útok, kdy jsou zkoušeny celé řetězce znaků z vlastní databáze útočníka. Čím méně triviální heslo, tím déle trvá jeho prolomení.

Hlavním bezpečnostním rizikem však bývá samotný uživatel. Instituce spravující přístupy by měla mít dobrou bezpečnostní politiku týkající se právě vytváření vlastních hesel uživateli [Apelbaum, 2004].

Autentizace **loginem** a **heslem** se většinou provádí **na straně instituce**, která svým uživatelům umožňuje přistup k licencovaným zdrojům. Méně často se provádí autentizace pouze pomocí institucionálního hesla (případně jména a hesla) na straně poskytovatele zdroje a to především z bezpečnostních hledisek. Není těžké si představit, jaká rizika nese sdílení jednoho hesla velikou skupinou uživatelů. Nicméně i tak se najdou poskytovatelé, kteří pro přístup k jim nabízeným zdrojům autentizaci za pomoci **institucionálního loginu** a hesla vyžadují. Tyto údaje pak nejsou přímo svěřované uživatelům, ale řeší to technologie pro vzdálený přístup jako např. EZproxy, ale o tom až dále v textu.

Naopak na **straně poskytovatele zdroje** je **nejčastěji** prováděna **autentizace pomocí IP adresy**, kterou si představíme níže. Někdy je také použito autentizace za pomoci kombinace institucionálního jména a hesla spolu s IP adresou.

2.4 IP Autentizace

Jeden ze způsobů autentizace uživatelů je **pomocí IP adresy** počítače, ze kterého k EIZ přistupují.

2.4.1 IP adresa

Všechna koncová zařízení připojená k Internetu mají IP (Internet Protocol) adresu. IP adresa je 32-bitové číslo, které je přiřazeno každému počítači (a dalším prvkům) připojenému do sítě postavené na IP (např. Internet) [IP address, 2001]. Obvyklá konvence pro zapsání IP adresy je taková: celé 32-bitové číslo, představující konkrétní IP adresu, se rozdělí na 4 části, odpovídající jednotlivým 8-bitovým bytům. Obsah každé z těchto čtyř částí (bytů) se pak vyjádří samostatně

jako desítkové číslo, a čtyři takto vzniklá čísla se zapíší za sebe, oddělená tečkami. Výsledek může vypadat takto: 94.143.168.233. [Peterka, 2000]. V současnosti vedle sebe paralelně existují dvě verze IP adres: IPv4 (Internet Protocol verze 4, ta je výše popsána) a IPv6. IPv6 řeší některé problémy spojené s IPv4. V rámci této práce je důležité pouze to, že adresy IPv4 jsou již skoro vyčerpané, vzhledem k obrovskému množství nejrůznějších koncových zařízení připojovaných k Internetu.

Dalším důležitým termín je **blok IP adres**. IP adresy jsou organizovány tak, že lehce identifikují celé sítě. Např. všechny IP adresy počítačů v UK začínají 159.23[3] takže pomocí zkratky 159.23.*.* reprezentujeme všechna koncová zařízení v síti. Tedy 159.23.*.* je jeden blok IP adres.

2.4.2 Jak to funguje

Když se uživatel přihlásí ke zdroji, tak systém jednoduše zkontroluje, zda je jeho IP adresa na seznamu. Pokud tam je, tak uživatel získá přístup a v opačném případě je mu odepřen.

Seznam IP adres je vlastníkovi EIZ dodáván institucí, která si ke zdroji platí přístup. K vytvoření seznamu není však třeba vypisovat jednu IP adresu po druhé. Obvykle se poskytují bloky síťových adres. Vlastník EIZ si tedy na své straně buduje seznam všech IP adres, které mají ke zdrojům přístup. Problém tedy nenastává ve chvíli, kdy uživatel, který chce dosáhnout vzdáleného zdroje, pracuje z počítače, který je připojen přímo do počítačové sítě instituce, která má přístup ke zdrojům zaplacen. Pokud uživatel přistupuje ke zdroji z počítače, který nemá povolenou IP adresu, tak musí využít nějakou z metod vzdáleného přístupu.

Tato metoda je používaná hlavně pro **autentizaci** přístupu **velkých skupin** (např. studenti univerzity) **uživatelů** k licencovaným zdrojům. Poskytovatelé EIZ nepotřebují znát přesnou identitu uživatelů, stačí jim, že uživatel byl autorizován na straně domovské instituce. Starost o to, aby z povolených rozsahů IP adres přistupovali pouze oprávnění uživatelé je na straně kupujícího licence.

[3] Nejedná se o skutečnou hodnotu IP adres UK.

2.4.3 Výhody a nevýhody

Výhodou autentizace pomocí IP adres je, že uživatelé nejsou nuceni se přihlašovat na straně poskytovatele zdroje (to je však obvykle vyžadováno na straně instituce, ze které ke zdroji přistupují).

I když to je v současnosti patrně nejrozšířenější způsob přístupu k licencovaným zdrojům v akademickém prostředí, tak má více úskalí než výhod. Na příkladu Univerzity Karlovy si můžeme některé problémy blíže vysvětlit. Předně seznamy IP adres je **komplikované udržovat**. Stačí jakákoliv změna IP adres (což není nic neobvyklého) a je nutno, z principu fungování autentizace na základě IP adres, změnu ohlásit dodavateli EIZ. To je, vzhledem k obrovskému počtu EIZ na UK, poměrně náročná záležitost.

Dalším problémem je, že ne každá část UK (např. katedra psychologie) má svůj vlastní blok IP adres (počítačové učebny bývají obvykle společné pro několik oborů), tak nemůže být takto vyřešen přístup do EIZ zakoupených pouze pro konkrétní část. Poslední problém, který zde zmíníme se týka výše uvedené problematiky IPv4 a IPv6. Adresy IPv4 jsou takřka vyčerpány, ale adresy IPv6 nejsou podporovány pro autentizaci ze strany poskytovatelů EIZ.

2.5 Synchronizace hesel

Cílem synchronizace hesel je umožnit uživatelům, aby při interakci s více aplikacemi mohli **používat** stále **jediné heslo** a usnadnilo se jim dodržovat zásady stanovené autentizační politikou. Model synchronizace hesel, na rozdíl od řešení pomocí dále popsaného modelu single sign-on, požaduje zadávání přihlašovacího jména uživatele a hesla pro každý přístup ke každé aplikaci (systému) [Hanáček, 2005].

2.6 Single sign-on

Tradičně, softwarové aplikace, které vyžadují uživatelské účty si autentizaci a autorizaci zpracovávají interně. Pro jejich využití se uživatel musí ke každé aplikaci přihlásit odděleně. Pro uživatele to znamená nutnost pamatovat si **mnoho přihlašovacích údajů**, což obvykle vede ke **snižování bezpečnosti**. Uživatele to navádí k nastavování co nejjednoduššího hesla, aby bylo lehce pamatovatelné.

Single sign-on (volně přeloženo jako jednotné přihlášení, SSO) je autentizační proces, který umožňuje uživateli přístup pomocí jediného přihlášení k více aplikacím či zdrojům [Huntington Ventures, 2006b]. A to tak, že po prvním přihlášení se již pro využití dalších služeb nemusí uživatel opakovaně přihlašovat. Tím odpadá pro uživatele nutnost si pamatovat hesla pro každou aplikaci zvlášť. Uživatel se přihlašuje u nějaké autentizační autority (např. LDAP server), na kterou jsou napojeny všechny služby v rámci SSO infrastruktury.

Existují dva základní scénáře pro přihlášení.

- Uživatel se **nejprve přihlásí** u autentizační autority a následně se může volně „pohybovat“ v rámci SSO prostředí a vstupovat do zdrojů a aplikací dle svých potřeb.
- Uživatel si **nejprve vybere zdroj** či aplikaci, kterou chce využít. Ta zjistí, že uživatel není přihlášen, a tak je přesměrován k autentizační autoritě [Novakov, 2006].

Zavedení single sign-on prostředí je však poměrně komplikovaná věc. Z principu je zřejmé, že proces autentizace musí být veden mimo aplikace, které jsou integrovány do single sign-on prostředí. Je tedy nutná jistá důvěra mezi zúčastněnými stranami. Ta je zajištěna zabezpečením přenášených dat nutných k autentizaci.

2.7 Šifrování

Pro zabezpečení přenášených dat pro autentizaci (a nejen) je třeba využít nějakého šifrovacího mechanismu. Existují mnohá řešení, ale zde si představíme pouze základní technologie. Jednou z takových technologií jsou protokoly **TLS** a **SSL**.

2.7.1 Protokoly TLS/SSL

Protokol TLS (Transport Layer Security) je následovníkem protokolu SSL (Secure Socket Layer), na jehož třetí verzi byl postaven V zásadě jde o to, že umožňují bezpečnou komunikaci vzdáleného uživatele přes veřejnou síť. Slouží k zabezpečení aplikací typu klient-server (tedy např. komunikaci webového prohlížeče s webovou stránkou) [Pužmanová, 2006].

2.8 Federační model

Hlavní myšlenkou federačního uspořádání je, že každý uživatel spadá pod nějakou "domovskou" organizaci, která o něm spravuje informace ve svém systému. Domovská organizace se stará o aktuálnost spravovaných dat o svých uživatelů. Federační model umožňuje využít informace spravované domovskou institucí i informačními systémy, které nejsou s touto institucí přímo propojeny, ale které jsou zapojeny v infrastruktuře pro výměnu dat o uživatelích - "federaci" [Kouřil, 2007].

Federace sdružuje organizace, které souhlasí se spoluprácí v rámci vymezených pravidel. Tato pravidla musí definovat několik oblastí: od komunikačních protokolů a datových formátů přes sémantiku předávaných dat až po provozní a organizační pravidla [Sova, 2005].

Federace tedy umožňuje uživatelům z různých organizací přistupovat k externím zdrojům s využitím svých „domovských“ přihlašovacích údajů. Uživatelům stačí si pamatovat pouze jediné přihlašovací údaje. Samotná autentizace pak probíhá pouze na přihlašovacím serveru domovské organizace a citlivé údaje jsou ve větším bezpečí. [EduId.cz, 2009]

Organizace sdružené ve federaci se dají rozdělit do dvou skupin. Jedna poskytuje informace o svých uživatelích (Identity Provider) a druhá poskytuje služby (Service Provider). Obecně platí, že každá organizace participující v rámci federace může vystupovat jako jeden poskytovatel identit a zároveň provozovat několik poskytovatelů služeb

Zapojené instituce si musí zvolit jednotný způsob, kterým budou data mezi sebou komunikovat. Takovým standardem může být například SAML (Security Assertion Markup Language), jehož implementací je např. Shibboleth.

2.8.1 Security Assertion Markup Language

SAML (Security Asssertion Markup Languague) je protokol fungující jako standard pro výměnu autentizačních a autorizačních dat mezi účastníky komunikace. Tedy mezi poskytovateli identity a poskytovateli služeb [SAML, 2008]. SAML je vyvíjen Technickým výborem pro bezpečnostní služby (Security Services Technical Committee) konsorcia OASIS (Organization for the Advancement of Structured

Information Standards). První verze SAML byla přijata v listopadu roku 2002. V současnosti je SAML ve verzi 2.0 [OASIS, 1993].

SAML je postaven na bázi XML (eXtensible Markup Language, volně přeložitelné jako rozšiřitelný značkovací jazyk). XML je metajazyk, v rámci něhož je možné vytvářet vlastní jazyky. Používá se především pro snadnou výměnu informací v elektronickém formátu a komunikaci nezávislou na konkrétních počítačových platformách [Kosek, 2000].

Jedním z hlavních problémů, který se SAML snaží vyřešit je vytvoření single sign-on ve webovém prostředí (tzv. web single sign-on). Single sign-on je poměrně snadno dostupné řešení v rámci intranetu (soukromá počítačová síť fungující v rámci jedné organizace, která používá stejné technologie jako Internet). Rozšíření těchto řešení mimo intranet je problematické, protože každá zúčastněná strana komunikace obvykle používá svá vlastní proprietární řešení, která nebývají kompatibilní. Tento problém právě řeší SAML, který je schopen komunikaci zajistit. [SAML, 2008].

Komponenty ze kterých se SAML skládá jsou tvrzení (assertions), protokoly (protocols), vazby (bindings) a profily (profiles).

Pro nás jsou nejzajímavější právě **tvrzení**. Tvrzení jsou balíky informací, které obsahují nějaké prohlášení tzv. **SAML autority** (poskytovatel identity nebo naopak poskytoval služeb) o nějaké třetí straně (typicky nějaký uživatel, ale záleží čistě na konkrétním použití). Prohlášení mohou být tří typů:

- **Autentizační** – prohlášení směrované k poskytovateli služeb. Specifikovaný subjekt (např. uživatel) byl autentizován poskytovatelem identity v určitý čas, určitou metodou.
- **Prohlášení o vlastnostech** (atributech) – prohlášení o vlastnostech, které se váží k danému subjektu
- **Rozhodnutí o autorizaci** – prohlášení o tom, zda požadavek pro povolení přístupu k danému zdroji specifikovanému subjektu bylo uděleno nebo ne [OASIS, 1993].

Kromě Shibbolethu je SAMLu využíváno v dalších projektech jako třeba Liberty Aliance (která přesla pod iniciativu Kantara) [OASIS, 1993].

Hlavní výhody protokolu SAML jsou:

- **Nezávislost na platformě** – odděluje bezpečnostní prvky od konkrétních aplikací, což vede k větší bezpečnosti komunikace
- **Volné propojení adresářů** – není nutné, aby správci identit měli data uživatelů synchronizována
- **Vytvoření single sign-on** – komfortnější prostředí pro koncového uživatele
- **Snížení administrativních nákladů** – to zejména na straně poskytovatelů služeb, kteří nemusí spravovat účty uživatelů

Kromě Shibbolethu je SAMLu využíváno v dalších projektech jako třeba Liberty Aliance (která nyní přesla pod iniciativu Kantara) [OASIS, 1993].

2.9 Česká akademická federace identit eduID.cz

2.9.1 Historie federace

Česká národní akademická federace je provozována sdružením CESNET (sdružení vysokých škol a Akademie věd, které od roku 1996 mimo jiné rozvíjí a provozuje páteřní akademickou počítačovou síť). Počátky federace eduID.cz se datují k roku 2006, kdy byla založena pracovní skupina pro přípravu federace. Pracovní skupina byla složena z 9 zástupců akademických institucí (Univerzita Karlova, Masarykova Univerzita, CESNET a další). Hlavním úkolem skupiny byl **rozvoj lokálních systémů správy identit a přístupů**, **sjednocení schématu atributů a především výběr federačního softwaru.**

Pro roli federačního softwaru byli dva kandidáti. Nizozemský systém A-Select, který původně vznikal jako lokální autentizační systém, jež byl o podporu federací rozšířen později. A-Select však nepodporoval snadné předávání atributů a v některých dalších ohledech byl celkově příliš robustní. Druhým a hlavně nakonec vybraným kandidátem byl software Shibboleth vyvíjený americkým konsorciem Internet2.

Pro potřeby federace byla vybrána **objektová třída eduPerson**, která byla vytvořena konsorciem Internet2 pro potřeby vzdělávacích institucí. Jeden z hlavních důvodů výběru bylo, že je to schéma používané v rámci většiny národních

akademických federací identit po celém světě [CESNET, 2007]. V současnosti se pracuje na přípravě schématu czEduPerson.

Příklad atributu dle schématu eduPerson může být například eduPersonAffiliation. Tento atribut popisuje vzat osoby k organizaci. Může nabývat více hodnot (faculty, student, staff, alum, member, affiliate, employee), které se mohou mezi sebou různě kombinovat pro získání podrobnějšího popisu [EduId.cz, 2009].

2.9.2 Současnost

Federace eduID.cz byla do ostrého provozu spuštěna 1. ledna 2009. Cílem České akademické federace identit je poskytnout svým členům rámce pro vzájemné využívání identit uživatelů při řízení přístupu k síťovým službám při respektování ochrany osobních údajů.

Česká národní federace eduID.cz má v současné době **15 členů** na straně **poskytovatelů identit**. Kromě CESNETU se jedná pouze o univerzity. Nicméně podle plánu by se k federaci během tohoto léta (2010) měly přidat další instituce a to zejména velké knihovny (Národní knihovna v Praze, Národní technická knihovna), ale i kulturní instituce (Národní galerie, Galerie výtvarných umění v Ostravě a další).

Poskytovatelů služeb je v současnosti více, protože se jedná o samostatné aplikace jako **EZproxy UK**, výukový portál **Mefanet** lékařských fakult a zejména přední poskytovatelé elektronických informačních zdrojů. Těmi jsou EBSCO, Cambridge University Press, Thomson Reuters a Ovid [EduID.cz, 2009].

3 Centrální autentizační služby Univerzity Karlovy

Centrální autentizační služby UK (dále jen CAS, dostupné z adresy http://ldap.cuni.cz) slouží k ověření totožnosti uživatele při přístupu k online databázím a aplikacím. Cílem je vytvoření **jedinečné elektronické identity** uživatele, která sestává z jeho přihlašovacího jména (také označováno jako login) a hesla. Uživatel si tedy nemusí pamatovat přihlašovací jména a hesla pro každou aplikaci a databázi zvlášť. CAS shromažďuje informace o uživateli potřebné k jeho autentizaci. Zdrojem těchto informací je Informační systém UK.

Účelem CAS je dále také zaručit poskytovatelům elektronických služeb metody bezpečného (chráněný pomocí SSL protokolu) ověření identity uživatele, administrátorům poskytnout prostředky pro správu uživatelských účtů a autorizačním systémům základní prostředky pro identifikaci skupin uživatelů [CAS, 2010].

3.1 Jak to funguje

Proces autentizace skrze CAS zahrnuje minimálně tři zúčastněné strany. Uživatele (respektive jeho webový prohlížeč, který vystupuje jako klient), webovou aplikaci, která vyžaduje autentikaci uživatele a CAS server.

Uživatel se přihlašuje k aplikaci. Ta vyžaduje autentizaci a uživatele přesměruje k CAS serveru, vůči kterému se uživatel autentizuje. Pokud se autentizace podaří, tak je uživatel poslán zpět k aplikaci, do které má nyní povolen přístup [CAS,2010].

3.2 Uživatelé

Uživateli CAS jsou studenti, pracovníci a externí uživatelé (např. účastníci programů celoživotního vzdělávání nebo externí uživatelé knihoven UK) Univerzity Karlovy. Tedy každý, kdo má nárok na vydání průkazu UK a je veden v informačním systému UK.

3.3 Přihlašovací údaje

Uživatelé se tedy vůči CAS identifikují pomocí svého přihlašovacího jména a hesla. Přihlašovací jméno je standardně 8-místné číslo osoby, které lze nalézt pod fotografií na průkazu UK, případně přihlašovací jméno používané v rámci nějaké lokální domény (např. doména JINONICE, která slouží pro autentizaci uživatelů UK v lokální síti areálu Jinonice) nebo také přihlašovací jméno, které je automaticky vygenerováno CAS po přijetí ke studiu.

V rámci CAS se rozlišují dva typy hesel: **ověřené** a **neověřené**. Ověřené heslo může uživatel získat v některém z výdejních center průkazů. Ve výdejním centru dostane automaticky vygenerované heslo, které má nastavenou omezenou dobu platnosti na 10 dnů, během kterých si ho uživatel musí změnit, aby jím vymyšlené heslo bylo dále považováno za ověřené. S ověřeným heslem si může nastavit heslo do domény JINONICE nebo pro připojení k eduroam (bezdrátová síť v prostorách UK). Heslo nastavené uživatelem musí splňovat určitá **kritéria bezpečnosti**. Těmi jsou **omezená doba platnosti**, která je nastavena na 365 dní, **minimální rozsah** hesla je 6 znaků, musí obsahovat alespoň jedno velké písmeno, malé písmeno a speciální znak (např. číslice) a zároveň nesmí obsahovat sekvenci delší než tři znaky, která se objevuje ve jméně nebo e-mailové adrese uživatele. Kvalitní bezpečnostní politika tvorby hesel je velice důležité, protože **poskytovatelé** zdrojů často **vyžadují garance**, že hesla uživatelů nejsou lehce prolomitelná [Voců, 2007].

3.4 Technické detaily

Pro ukládání a přístup k záznamům uživatelů je využíváno adresářových služeb **LDAP**. Záznamy jsou uchovávány v obecné objektové třídě inetOrgPerson, třídě cuniPerson (vytvořené speciálně pro potřeby CAS UK) a třídě eduPerson, která je používána v rámci federace eduID.cz. CAS UK tedy také slouží také jako zdroj informací pro shibbolethovou komponentu poskytovatele identit, která je implementována na UK.

4 Technologie vzdáleného přístupu

4.1 Obecně o metodách vzdáleného přístupu

Technologie vzdáleného přístupu řeší problém, kdy chce uživatel využívat elektronické informační zdroje a nachází se mimo budovu své domovské instituce (univerzita, knihovna apod.), která má přístup ke zdrojům pro své uživatele zakoupen. Na technologie vzdáleného přístupu jsou kladeny velké požadavky, které ne každá zcela splňuje.

Začněme obecnými požadavky. Technologie vzdáleného přístupu by měly být především jednoduché a to tak, aby byly jednoduše použitelné uživateli a zároveň lehce implementovatelné do provozu správci vzdáleného přístupu.

Z hlediska uživatele to znamená především, aby se mohl pro používání vzdáleného přístupu obejít bez instalace doplňků do svého webového prohlížeče nebo nutnost instalace jakéhokoliv speciálního softwaru. Uživatel by neměl být omezen tím, jaký používá operační software (ať už MS Windows, Linux nebo Mac OS případně další), webový prohlížeč (tedy alespoň pokud se jedná o nějakou aktuálnější verzi) a neměl by být omezen ani samotným typem koncového zařízení, kterých dnes existuje celá řada (kromě osobního počítače to jsou notebooky, netbooky, mobilní telefony s přístupem k Internetu atd.). Z uživatelova hlediska je také důležitá ochrana jeho osobních údajů. Třetí strana, tedy poskytovatel zdroje, nepotřebuje znát jméno uživatele ani další osobní údaje, obvykle stačí jenom informace o tom, že uživatel je členem nějaké instituce. Důležitým aspektem je také podpora single sign-on prostředí.

Z hlediska správce (tedy domovské organizace uživatele) vzdáleného přístupu jsou důležité aspekty jako možnost monitorovat využívání vzdáleného přístupu pro vedení statistik. Důležitá je také zda je technologie stále vyvíjena, aby dokázala reflektovat požadavky dané technickým vývojem apod. Z tohoto pohledu se asi nejlépe jeví technologie s otevřeným zdrojovým kódem, které mají širokou uživatelskou základnu starající se o vývoj. Vzhledem k tomu, že musí být technologie implementovatelná mezi různorodými systémy je také vhodné, aby byla založena na otevřených mezinárodních standardech [Pavlík, 2009] .

V této kapitole si blíže představíme v současnosti nejrozšířenější technologie vzdáleného přístupu.

4.2 Terminálový přístup

4.2.1 Základní charakteristika

Vzdálený přístup pomocí terminálového serveru funguje na principu klient-server. Klient je software, který umožňuje uživateli z jeho vlastního počítače (či jiného koncového zařízení) ovládat počítač vzdálený (server), jako kdyby byl u něj fyzicky přítomen. Základní rozdělení vzdáleného přístupu pomocí terminálového serveru lze do dvou kategorií dle grafického rozhraní a to na textový výstup a obrazový výstup [Vašek, 2009].

Pravděpodobně nejčastěji používaným typem terminálového přístupu je tzv. vzdálená plocha, které spadá do druhé kategorie. Uživatel vidí na svém počítači plochu vzdáleného počítače, kterou může ovládat pomocí svých kontrolních zařízení (např. myš a klávesnice). Uživatel má tedy potenciálně (záleží také na nastavení administrátorem) k dispozici veškeré softwarové vybavení vzdáleného serveru.

Jakožto konkrétní příklad si můžeme uvést klienta a server pro vytvoření vzdáleného plochy, který je obsažen jako jedna ze základních komponent v operačním systému MS Windows. Tato komponenta se nazývá Služby vzdálené plochy (volný překlad Remote Desktop Services), fungující dle protokolu RDP (Remote Desktop Protocol), který byl vyvinut přímo firmou Microsoft [Remote Desktop Services, 2004].

4.2.2 Terminálový přístup na UK

Na Univerzitě Karlově je terminálový přístup používán pouze okrajově a to pro zaměstnance s účtem v doméně UVTUK (počítačová síť Ústavu výpočetní techniky Univerzity Karlovy). Využívá se pro přístup k pracovní poště a souborům na síťových discích.

4.2.3 Shrnutí

Výhody: - není omezeno operačním systémem
- není náročný na správu

Nevýhody: - hardwarově náročné (na serverové straně)

- chybí statistiky

4.3 Portálová řešení

4.3.1 Základní charakteristika

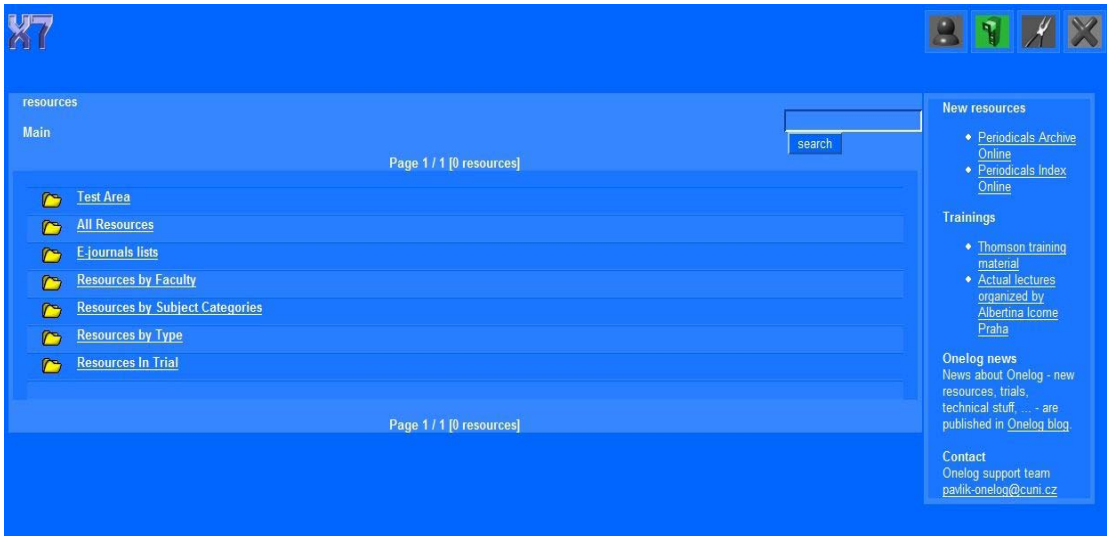
Portálová řešení se vyznačují jednotným rozhraním pro přístup k EIZ. Jedná se o jakési brány, které sjednocují přístup k dostupným aplikacím a informačním zdrojům. Obvykle poskytují také širokou škálu různých nadstavbových funkcí. Podrobněji si ukážeme portál **OneLog**, který byl v minulých letech používán jako jedna z možných metod vzdáleného přístupu na Univerzitě Karlově. Odstaven byl v neděli 8. března 2009, kdy byl plně nahrazen Portálem elektronických zdrojů a EZproxy. Dalším možným představitelem této skupiny je softwarový produkt HAN (Hidden Automatic Navigator) německé společnosti H+H Software.

4.3.2 Onelog

Onelog je jedním z produktů britské společnosti Info Technology Supply Ltd. Onelog nabízí řadu funkcí. Nejedná se o "pouhý" nástroj pro vzdálený přístup k EIZ. Spíše se jedná o komplexní **nástroj pro správu elektronických zdrojů** (ERM, Electronic resource management). Uživatelům umožňuje vzdálený přístup pomocí jediného přihlášení a zároveň poskytuje informace o informačních zdrojích. Administrátorům na druhou stranu nabízí možnost sledovat statistiky o využívání jednotlivých zdrojů (kdo zdroj používal, jak dlouho setrval apod.) [Info Technology Supply, 2009].

Pro své fungování Onelog vyžaduje instalace některých komponent a to jak na straně uživatele, tak na straně instituce, která Onelog provozuje. Více si přiblížíme Onelog dle toho, jak fungoval na Univerzitě Karlově z pohledu uživatele.

4.3.3 Onelog na UK



obrázek č.2: uživatelské rozhraní Onelogu na UK

Zprovoznění Onelogu nebylo z pohledu uživatele úplně jednoduché. Existovaly 2 hlavní možnosti v závislosti na operačním systému (OS) uživatele. Uživatelé OS Windows si pro přístup pomocí Onelogu museli stáhnout plug-in (doplňkový modul rozšiřující funkce dané aplikace) do svého webového prohlížeče. Uživatelé jiných OS si museli stáhnout Citrix klienta, který vyžadoval podporu Javy (programovací jazyk). Uživatel byl pak ke zdrojům připojován skrze Citrix server, což bylo pomalejší než první možnost. Druhá možnost byla také hardwarově náročnější a obsahovala větší bezpečnostní rizika (jako vyšší riziko nákazy počítačovým virem). Druhá možnost však poskytovala přístup ke všem elektronickým zdrojům, protože některé zdroje byly přístupné pouze prostřednictvím Citrix serveru.

Po zdárné instalaci však nabízel poměrně příjemné uživatelské prostředí. Pro uživatele nabízel možnost různých „kosmetických“ změn grafického rozhraní, výběr svých oblíbených elektronických časopisů či databází, které mohl mít „připravené“ hned po přihlášení v úvodním menu rozhraní Onelog [Kubeš, 2007].

Nakonec se od používání Onelogu odstoupilo. To především z důvodů vysoké ceny (v řádech sta tisíců za roční licenci), častým problémům uživatelů způsobených používanými zásuvnými moduly.

4.3.4 Shrnutí

Výhody: - uživatelsky komfortní prostředí
- modifikovatelnost
- možnost vedení statistik

Nevýhody - vysoké pořizovací náklady
- nutnost instalace doplňků

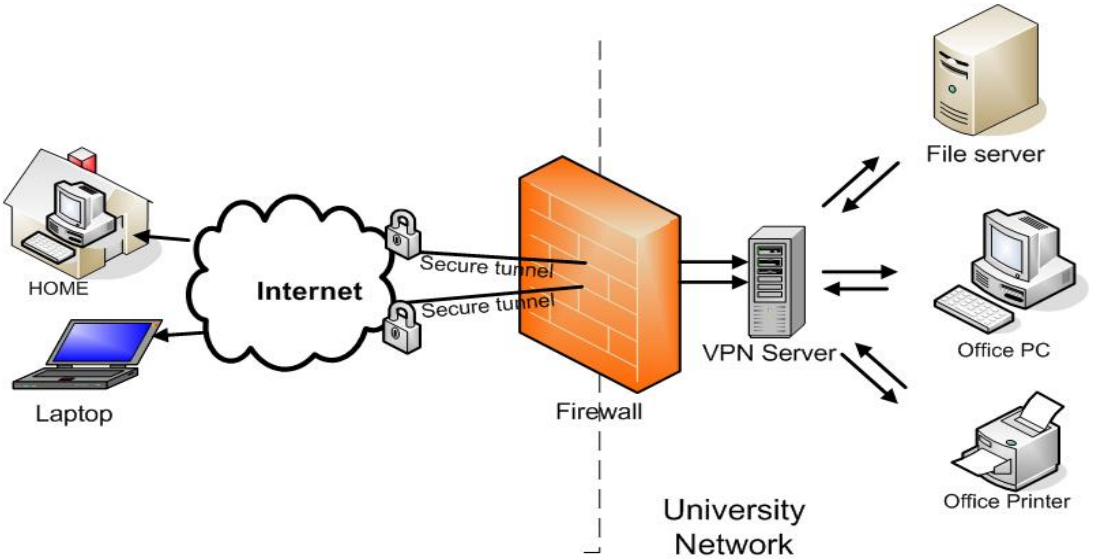
4.4 Virtualní privátní sítě

4.4.1 Základní charakteristika

Virtuální privátní sítě (Virtual private networks, dále jen VPN) využívají **veřejnou (sdílenou) infrastrukturu**, kterou může být například **Internet,** pro vytvoření uzavřeného bezpečného komunikačního prostředí [Luhový, 2003]. Pod pojmem VPN můžeme nalézt široké spektrum mnohdy i značně rozdílných technologií. VPN tedy nejsou specifické svou technologií, ale právě způsobem efektivního využití veřejných sítí a komunikačních služeb [Pužmanová, 2006]. Cílem VPN je propojení vzdáleného počítače (případně celých počítačových sítí) do lokální sítě organizace, který se tak vůči okolí jeví, jako by v dané lokální síti byl fyzicky přítomen (má její IP adresu).

-**Virtuální**, protože neexistuje žádné **přímé** síťové spojení mezi dvěma (nebo více) komunikačními partnery.

-**Privátní**, protože pouze účastníci komunikace, kteří jsou propojeni pomocí VPN, se mohou dostat k přenášeným informacím. [Feilner, 2006]



Obrázek č. 3: Schéma propojení pomocí VPN

4.4.2 Typologie

VPN lze rozdělit na **2 základní typy**.

- 1, VPN je vytvořena mezi jednou koncovou vzdálenou stanicí (např. osobní počítač) a lokální (privátní) sítí (LAN, Local Area Network). Tento typ se označuje jako „client-to-server“ nebo „user-to-LAN“ .
- 2, VPN je vytvořena mezi dvěma lokálními sítěmi. Tento typ se označuje jako „site-to-site“. [Petri, 2001]

4.4.3 Jak to funguje

První typ vyžaduje přítomnost nějakého VPN klienta na stanici vzdáleného uživatele a na druhé straně (například LAN nějaké organizace, univerzity apod.) VPN server (někdy se označuje jako brána). Klient naváže spojení se serverem a vytvoří mezi sebou zabezpečený šifrovaný tunel. Takto připojený vzdálený uživatel pak vystupuje na síti pod IP adresou sítě, do které se připojil. K vytvoření komunikačního tunelu je obvykle vyžadováno heslo.

Pro vytvoření bezpečného spojení se používají ruzné síťové protokoly. Nejčastější je využíváno protokolů IPsec (IP security), L2TP (Layer 2 Tunneling Protocol), PPTP (Point to Point Tunneling Protocol).

Druhý typ vyžaduje přítomnost serverů na obou stranách účastníků komunikace. [Petri, 2009]

Klient VPN je standardně nějaký software. Dnes je defaultně součástí naprosté většiny operačních systému (např. MS Windows). Komerčních řešení existuje celá řada (CISCO je jedno z nejznámějších), ale k dispozici jsou i open-sourcová řešení (např. OpenVPN).

Technologie VPN vyžaduje správné nastavení firewallů (bezpečnostních prvků na síti) a není možné ji vždy použít, protože bývá blokována poskytovateli internetového připojení.

4.4.4 VPN na Univerzitě Karlově

Jedním z protokolů pro realizaci virtuální privátní sítě Univerzity Karlovy byl zvolen protokol **PPTP**, který je podporován ve většině operačních systémů (MS Windows 95/98/NT/2000/XP, Linux, aj.). Operační systémy MS Windows, které jsou mezi uživateli nejrozšířenější, obsahují klienta pro použití tohoto protokolu, takže odpadají problémy se sháněním instalací a složitou konfigurací. Společnost Microsoft se podílí na specifikaci PPTP protokolu [Morávek, 2003].

Problémem VPN je, že uživatelovi v podstatě zprostředkovává připojením do sítě UK uživateli přímý přístup k EIZ, který nedokáže zajistit přístup k EIZ vyžadujících autentizaci na základě institucionálního loginu a hesla.

4.4.5 Shrnutí

Výhody: - jednoduchá správa ze strany provozovatele
- lehce dostupná technologie

Nevýhody: - pro uživatele náročnější instalace
- nemusí vždy fungovat

4.5 Proxy server

4.5.1 Základní charakteristika

Proxy server je počítač případně specializovaný software, který vystupuje jako **prostředník mezi klientem** (např. webový prohlížeč uživatele) **a serverem** (např. požadovaný cílový elektronický informační zdroj). Proxy server přijímá požadavky od klienta a předává je cílovému serveru. A stejně tak opačným směrem vrací odpovědi serveru klientovi. Pro cílový server tedy proxy vystupuje jako klient [Blansit, 2007].

Možných využití proxy serverů je celá řada. Kromě využití pro přístup ke vzdáleným zdrojům jmenujme rychlejší „načítání“ webových stránek, kdy proxy slouží jako tzv. cache (vyrovnávací paměť), kde se ukládají data směřující ze serveru ke klientovi. Ta se při každém dalším přístupu mohou tedy načíst přímo z proxy a nemusí se znova stahovat ze serveru, což bývá pomalejší. Další výhodou je anonymita uživatele, který je „schován“ za proxy serverem a není tedy cílovým zdrojem vidět (resp. cílový zdroj nezná jeho IP adresu).

V rámci vzdáleného přístupu je hlavním smyslem to, že **uživatel** přistupující k cílovému zdroji skrze proxy **dostává IP adresu** právě **proxy serveru**. Z hlediska autentizace pak stačí, aby byla všechna oprávnění na straně cílového informačního zdroje nastavena pouze pro daný proxy server, např. na základě jeho IP adresy nebo jména a hesla [Pokorný, 2007].

Jedním z hlavních problému proxy serverů je nemožnost jejich škálovatelnosti. Tedy rozlišování skupin uživatelů. Ve chvíli, kdy se uživatel k proxy připojí, tak má automaticky přístup ke všem zdrojům dostupných na základě IP adresy.

Proxy servery můžeme rozdělit jednoduše na dva typy. **HTTP proxy** a **Rewrite proxy** (typů však existuje celá řada a terminologie není nijak dogmaticky ustálená). Největším rozdílem ze strany uživatele je to, že pro použití prvního typu si musí přenastavit vlastnosti webového prohlížeče a u druhého nemusí [Mikesell, 2004]

4.5.2 HTTP proxy

Jedna ze základních metod využití proxy služby vyžaduje po uživateli změnu nastavení webového prohlížeče, tak aby směřoval na adresu proxy serveru. To je záležitost pouhého vložení URL (Uniform Resource Locator, je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací, ve smyslu dokument nebo služba, na Internetu [Uniform Resource Locator, 2004]) proxy serveru na patřičné místo v menu pro nastavení webového prohlížeče. Tady však nastává problém v tom, že každý webový prohlížeč má menu pro nastavení odlišné a také jsou rozdíly v tom, jaký typ připojení k Internetu uživatel používá. Proxy není tolik citlivá na nastavení firewallů (např. proti VPN), ale je méně pohodlná na používání. Není možné ji použít v případě, kdy se již přes nějakou jinou proxy připojujete do internetu [Mikesell, 2004]

Tento typ proxy serveru představuje známý open-sourcový software Squid.

4.5.3 Rewrite proxy

Druhým typem proxy serveru jsou tzv. rewrite proxy. Ty ze strany uživatele nevyžadují žádné nastavování. Tento typ proxy si představíme na konkrétním produktu EZproxy.

4.5.4 Shrnutí

Výhody: - nízké pořizovací náklady
- lehce zvládnutelné pro uživatele (u rewrite proxy)
- možnost vedení statistik

Nevýhody: - nutnost úprav nastavení webového prohlížeče (u http proxy)
- není rozlišení skupin uživatelů

4.6 EZproxy

EZProxy je jedna z nejrozšířenějších aplikací pro vzdálený přístup k elektronickým informačním zdrojům v knihovnickém prostředí. Uvádí se, že jí implementovalo již cca 2500 institucí ve více než 60 zemích světa. EZproxy bylo původně vyvíjeno od roku 1999 firmou The Useful Utilities, kterou vedl Chris Zagar. V roce 2008 bylo EZproxy odkoupeno americkou organizací OCLC (Online Computer Library Center), která nyní poskytuje technickou podporu a stará se o další vývoj. Jedná se o komerční produkt, ale jeho cena je poměrně únosná – roční licence vyjde na něco málo pod 500 dolarů. [OCLC, 2010]

EZproxy je momentálně jedna z metod pro vzdálený přístup na Univerzitě Karlově a nahradila dříve používaný OneLog (viz. výše). EZproxy bylo do reálného provozu nasazeno ve školním roce 2008-2009. Kromě UK je EZproxy implementováno také v následujících institucích v ČR: Národní technická knihovna, Masarykova Univerzita v Brně, Vysoká škola ekonomická v Praze a mnohé další.

EZproxy patří do skupiny tzv. rewrite proxy. Rewrite proxy se vyznačují tím, že mění URL zdroje takovým způsobem, že cílovému serveru se uživatelův klient jeví, jako by „přísel“ z IP adresy proxy serveru.

Ukázka modifikace URL:

- http://www.databaze.com/index.html

EZproxy ji však modifikuje takto:

- http://www.databaze.com.ezproxy.domaciinstituce.cz/index.html [OCLC, 2010b]

Kromě ceny má EZproxy spoustu dalších výhod, které vedly k tomu, že je to momentálně jedna z metod pro vzdálený přístup na UK.

EZproxy není limitovaná operačním systémem uživatele a funguje na všech webových prohlížečích (tedy minimálně, co se jejich aktuálních verzí týká). Nepožaduje po uživateli instalaci žádných doplňků do webových prohlížečů nebo speciálního softwaru. Oproti klasickým proxy také nevyžaduje žádné úpravy v nastavení webových prohlížečů. EZproxy funguje na standardních portech (80 – http, 443 – https), což eliminuje problémy s firewally, se kterými si klasická proxy řešení často neuměla poradit.

EZproxy také umožňuje zaznamenávat uživatelské aktivity. To lze použít pro vyhodnocení využívanosti jednotlivých informačních zdrojů, případně také pro identifikování případného porušování podmínek užívání informačních zdrojů.

Další důležitou vlastností EZproxy je kompatibilnost s mnohými nadstavbovými nástroji pro využívání EIZ jako Metalib či SFX a v neposlední řadě je možná jeho integrace se Shibbolethem, který si představíme dále [Pavlík, 2008b].

4.7 Shibboleth

4.7.1 Základní charakteristika

Shibboleth je volně dostupný software s otevřeným zdrojovým kódem implementující federační model, který se používá pro zabezpečení přístupu k webovým aplikacím a vytvoření webového single sign-on prostředí [Kouřil, 2007]. A to jak mezi zdroji a aplikacemi v rámci jedné instituce, tak za jejím hranicemi.

Shibboleth je postaven na protokolu SAML (Security Assertion Markup Language). První verze Shibbolethu byla vypuštěna v červnu roku 2003. Za vývojem Shibbolethu stojí americký projekt Internet2, konkrétně jeho podskupina MACE (Middleware Architecture Committe for Education), která je podporována korporací IBM (International Bussiness Machines). S Shibbolethem se často spojuje termín middleware, což je software, který umožňuje komunikaci mezi různými softwarovými aplikacemi [Internet2, 2010].

Shibboleth se skládá ze tří hlavních komponent a to poskytoval identit, poskytovatel služeb (souhrně označovány jako entity) a vyhledávací služby (Discovery service). První komponenta obsahuje funkce pro identifikaci uživatelů a poskytování informací (atributů) o uživatelích komponentě druhé. Komponenta poskytovatel služeb je umístěna na webovém serveru, kde sídlí požadovaný

informační zdroj (případně jakákoliv aplikace), která provádí autorizaci uživatelů na základě atributů poskytnutých poskytovatelem identit.

Celá architektura Shibbolethu závisí důvěře mezi poskytovateli identit a služeb. Pro usnadnění komunikace mezi servery během autentizačního procesu používá Shibboleth protokol SAML pro předávání informací o identitě uživatele a služby. Jako primární zdroj důvěry mezi poskytovateli identit a služeb slouží metadata. Obsahují totiž veřejné klíče, které slouží k ověření podpisů jednotlivých entit, k jejich autentizaci či k zašifrování zpráv, jejichž formát je také definován protokolem SAML [Internet2, 2010].

Správa metadat je obvykle starostí národních federací. Do druhé verze Shibbolethu byla metadata obvykle spravována manuálně. Správce entity připravil novou verzi svých metadat, předal ji správci metadat federace, ten ji zkontroloval, zařadil do souboru metadat federace, který elektronicky podepsal a publikoval na předem dohodnutém URL. Odtud si pak soubor zkopírovaly všechny entity. Tento způsob správy byl náročný na lidské kapacity a byl poměrně zdlouhavý. To způsobovalo problémy v případech, kdy bylo potřeba rychle změnit např. informace o klíčích některé z entit. Od verze 2.0 Shibboleth obsahuje nástroje na automatické stahování, kontrolu a údržbu federačních metadat. Některé údaje je však stále třeba nastavovat manuálně [CESNET, 2006].

V současnosti je aktuální (a zároveň stabilní) verze Shibbolethu 2.1 pro komponentu poskytovatele identit a 2.3.1. pro poskytovatele služeb.

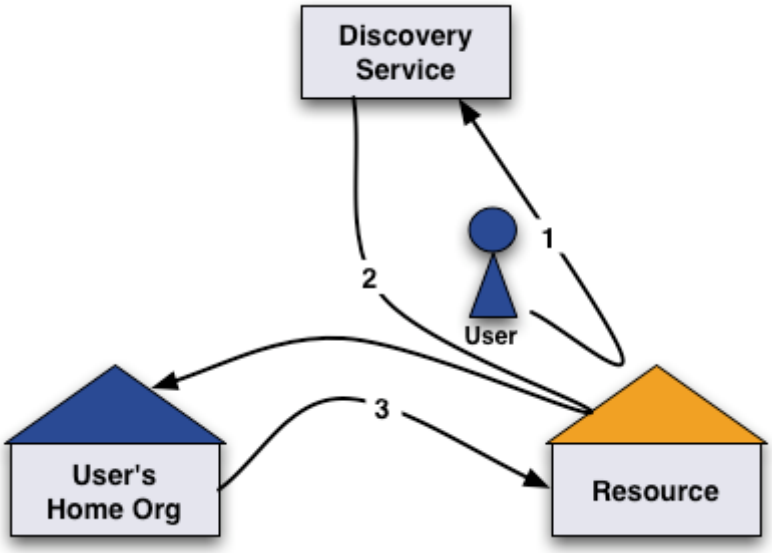
4.7.2 Obecné schéma fungování

Představme si modelovou situaci, kdy uživatel, v tomto případě student univerzity, se chce dostat k elektronickému informačnímu zdroji, umístěnému na serveru www.zdroj.com. A to z vlastního počítače mimo síť jeho domovské organizace. Zdroj je ovšem licencovaný, takže se k němu mohou dostat jen oprávnění uživatelé. Naštěstí pro uživatele k němu má však zakoupena práva univerzita, jejímž je studentem. Univerzita i informační zdroj (respektive jeho poskytovatel) jsou členy federace používající shibbolethovou autentizaci.

1. **fáze – Uživatel se přihlašuje ke zdroji a je přesměrován**: Uživatel zadá adresu serveru (www.zdroj.com) do svého webového prohlížeče, který

pošle požadavek o přístup k webu. Server zjistí, že uživatel není dosud autentizován a odpoví tak, že automaticky přesměruje uživatele na „Vyhledávací službu“ („Discovery service“, od verze 2.0 nahradila službu „Where Are You From“, WAYF[4]), která je umístěna třeba na serveru www.wayf.com.

2. **fáze – výběr domovské organizace**: Nyní se uživatel nachází na webu Vyhledávací služby, která nabídne uživateli seznam možných domovských institucí (resp. poskytovatelů identity), ze kterých si vybere tu svou. Z vyhledávací služby je uživatel přesměrován na autentizační stránky své domovské organizace.
3. **fáze - Autentizace**: Uživatel se pomocí přihlašovacích údajů autentizuje u své domovské organizace. Následně je vysláno tvrzení (viz. popis protokolu SAML), které obsahuje informace (tzv. atributy) o uživateli.
4. **fáze - Autorizace**: Po úspěšné autentizaci u své domovské organizace je na zdroji, zda uživateli poskytne přístup nebo ne a to na základě tvrzení, které vyslala domovská organizace. Domovská organizace poskytla zdroji nejmenší potřebné množství uživatelových atributů, které je třeba aby zdroj uživatele autorizoval nebo ne [Switch, 2010].



Obrázek č.4: Obecné schéma fungování Shibbolethu

[4] Došlo ke změně technologie, ale z pohledu uživatele se nemění nic. „Discovery service“ je tak stále často označována jako „WAYF“

Když je jednou uživatel autentizován, tak může využívat služby všech dalších shibboletizovaných aplikací a zdrojů, ke kterým má přistup díky své domovské organizaci, bez nutnosti další autentizace. Tedy autentizace probíhá vždy, ale na pozadí (uživatel se nemusí opětovně přihlašovat). A to do doby než vypne uživatel svůj webový prohlížeč nebo dokud neskončí relace připojení k Shibbolethu, která je standardně nastavena na 60 minut. V současnosti chybí podpora jednoduchého odhlášení z kontextu Shibbolethu.

4.7.3 Shibboleth na UK

Technologie Shibboleth zajišťuje veškerý vzdálený přístup ke zdrojům dostupných na Univerzitě Karlově. Některé zdroje v současnosti podporují připojení pomocí Shibbolethu přimo (databáze členů federace eduID.cz na straně poskytovatelů služeb- Ovid, EBSCO, Thomson Reuters). Ostatní zdroje jsou dostupné přes Shibboleth pomocí brány, kterou vytváří EZproxy [Pavlík, 2010].

EZproxy je na UK nastaveno jako shibbolethový poskytovatel služeb. To má výhodu v tom, že je tak vytvořeno SSO prostředí i pro zdroje, které nejsou dostupné přímo přes Shibboleth. Uživatel se přihlásí přes CAS, v jehož rámci je instalována i komponenta shibbolethového poskytovatele identit. Shibboleth následně poskytuje atributy EZproxy, které je na jejich základě schopno rozhodnout, zda má uživatel ke zdroji přístup.

4.7.4 Shrnutí

Aby mohlo být Shibbolethu využito je třeba mít dobře zvládnutou centrální správu identit a přístupů v rámci instituce, to mimo jiné znamená dodržování patřičných standardů v rámci federace. To je poměrně náročný proces, ale vyplatí se všem zúčastněným. Pro uživatele to znamená pohodlné SSO prostředí nejen v rámci zdrojů domácí instituce, ale i vnějších zdrojů externích poskytovatelů služeb.

Uživatelům také nabízí „bezbariérový“ přístup – nejsou omezeni svým koncovým zařízením, operačním systémem a ani webovým prohlížečem. Kromě toho také Shibboleth poskytuje velkou míru soukromí svým uživatelům, což je založeno na již zmíněné autentizaci na základě atributů, kterých jde ze strany poskytovatelů identit k poskytovatelům služeb pouze minimální potřebné množství.

5 Implementace vzdáleného přístupu v Portále elektronických informačních zdrojů

Cílem této kapitoly je popsat, jak vypadá implementace technologií vzdáleného přístupu z **uživatelova** hlediska. Konkrétně při přístupu ke vzdálenému zdroji z Portálu Elektronických informačních zdrojů Univerzity Karlovy.

Portál elektronických informačních zdrojů (dále jen jako PEZ) je hlavním výchozím bodem pro přístup k elektronickým informačním zdrojům zpřístupňovaných na Univerzitě Karlově. Původně byl vytvořen na půdě Masarykovy Univerzity v Brně, ale postupně ho začaly používat i další univerzity [Zach, 2010].

PEZ plní několik základních funkcí:

- poskytuje seznam a základní informace o všech dostupných EIZ na UK
- **zpřístupňuje všechny zdroje**
- informuje o novinkách souvisejících s EIZ
- obsahuje návody

Nás v rámci této práce zajímá pouze jedna funkce PEZ a tou je právě zpřístupňování EIZ. Pro přístup k EIZ z PEZ je možno využít dva způsoby. Buď přímo z **PEZ** nebo lze využít **portál EZproxy**. Začneme popisem přístupu z druhého.

Portál EZproxy je uživateli poněkud skryt. Dostat se k němu lze přes odkaz „vzdálený přístup“ v menu v levé části webu PEZ. Zde se k portálu EZproxy dostane uživatel přes další odkaz, tentokrát již nazván „Portál EZproxy“. Následně je uživatel vyzván k přihlášení pomocí svého univerzitního učtu, tato výzva zároveň slouží jako odkaz, ze kterého je uživatel přesměrován k CAS, kde se přihlásí. Výsledkem je, že se uživatel dostane k nabídce všech zdrojů, ke kterým má přístup. Po kliknutí na odkaz[5], vybraného zdroje je k němu přesměrován.

[5] jehož konstrukce byla popsána v kapitole 4

Ve spodní části portálu EZproxy je možnost se odhlásit. To však ve skutečnosti nefunguje, což je dáno výše zmíněným propojením EZproxy se Shibbolethem, který tento způsob odhlášení momentálně nepodporuje.

Druhým způsobem přístupu je přímo skrze PEZ. Zde si uživatel nejprve vybere, jakým způsobem bude zdroji procházet. Může si vybrat mezi zdroji seřazenými abecedně, dle institucí (fakulty a části UK, které mají zdroj předplacený), případně zdroje zkušební nebo volné. Uživatel si vybere abecední seznam. Zde vidí jednotlivé zdroje seřazené ve sloupci podle názvu. Vedle názvu v hranatých závorkách může najít tři odkazy: „**přímý přístup“**, „**vzdálený přístup“** nebo „**Shibboleth“**. Přímý přístup je možné využít v případě, že pracuje z počítače napojeného do sítě UK, nebo je do sítě UK připojen pomocí VPN. Zdroje, které nenabízí přímé přihlášení vyžadují institucionální heslo, což nedokáže přímý přístup zařídit.

„Vzdálený přístup“ je odkaz využívající EZproxy (jako shibbolethovou bránu, což je popsáno v kapitole 4). Odkaz Shibboleth je pro zdroje, které ho podporují nativně. Při výběru odkazu „vzdálený přístup“ se, v případě, že zdroj není pro celou fakultu, objeví nabídka fakult a částí, které přístup mají. Po výběru instituce je uživatel přesměrován na přihlašovací stránku EZproxy portálu, odkud je přesměrován na službu CAS a pak dále ke zdroji.

Při výběru odkazu „Shibboleth“ je uživatel přesměrován přímo na CAS, kde se přihlásí a je přesměrován ke zdroji, který rozhodne o jeho autorizaci. Zvláštnost odkazu „Shibboleth“ je v tom, že se jedná o tzv. **WAYFless** odkaz. To znamená, že je přeskočena fáze výběru domovské instituce (viz obecné schéma fungováni Shibbolethu v kapitole 4.7.2).

Ať si vybereme jakýkoliv způsob vzdáleného přístupu, který se na Portále elektronických informačních zdrojů nabízí, tak po prvním přihlášení je možné se dostat k dalším zdrojům bez dalšího přihlašování. Využití EZproxy jako shibbolethového poskytovatele služeb poskytuje příjemné SSO prostředí (detailněji v kapitole 4.7.3).

6 Průzkum

Závěrečná část bakalářské práce je věnována vyhodnocení průzkumu využívání jednotlivých technologií vzdáleného přístupu na Univerzitě Karlově. Průzkum probíhal po dobu 10 dnů a to od 25. července do 3. srpna 2010. Za tuto dobu se podařilo získat odpovědi od **164 respondentů**.

6.1 Cíle dotazníku

Dotazník byl vypracován za účelem zjištění oblíbenosti a využití jednotlivých technologií vzdáleného přístupu a v orientaci v nabízených službách. Cílovou skupinou byli studenti a vyučující z Ústavu informačních studií a knihovnictví. Konečná cílová skupina však byla nakonec nejspíše poněkud širší, protože šíření dotazníku nešlo úplně kontrolovat a na konec byl propagován v podstatě v rámci celé univerzity.

6.2 Metodologie

Sběr dat probíhal pouze v prostředí **Internetu**. Konkrétně jsem využil služeb webového serveru „**Vyplňto.cz**“ (dostupný z http://www.vyplnto.cz/), kde si lze sestavit vlastní dotazník, který plně vyhovoval potřebám průzkumu.

Dotazník byl anonymní. Byl nastaven pouze limit na jedno hlasování z jedné IP adresy, aby bylo zamezeno případnému opakovanému hlasování jednoho uživatele.

Uživatelům bylo položeno maximálně 17 z celkově 18 vypracovaných otázek a to v závislosti na odpovědích.

6.3 Propagace dotazníku

Propagace dotazníku proběhla simultánně několika způsoby.

První způsob byl využití **e-mailové konference UISK118**, která se používá pro komunikaci v rámci Ústavu informačních služeb a knihovnictví.

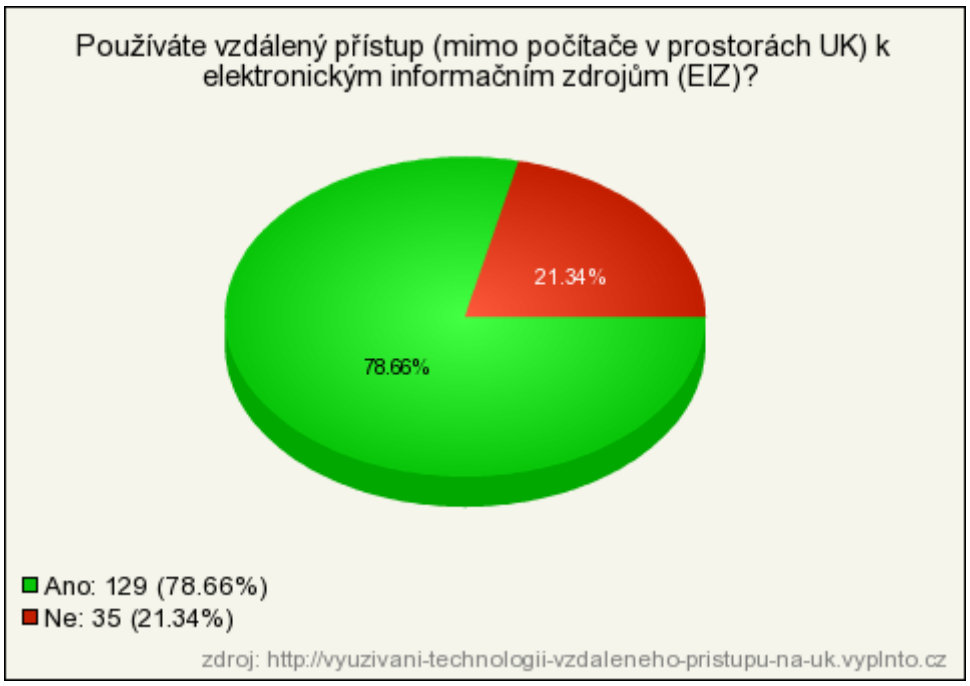
Druhý způsob byl pomocí v současné době velice populární sociální sítě **Facebook**, kde byla vytvořena tzv. událost, která byla rozeslána kontaktům z řad spolužáků a ti zase poslali údalost svým kontaktům atd.

Třetí způsob šíření dotazníku bylo zveřejnění žádosti o vyplnění **na Portále elektronických zdrojů UK**, konkrétně v jeho propagační části (konkrétně též přes sociální síť **Facebook** a zároveň přes blogovací službu **Twitter**).

6.4 Vyhodnocení dotazníku

V následující části budou postupně rozebrány jednotlivé otázky. Ke každé otázce je přiložen graf pro lepší přehlednost a zároveň je výsledek také doplněn v textové podobě. Vysvětlen je účel otázky, ačkoliv ten by snad měl být zřejmý ze samotného znění. Připojen je také autorův komentář. Jako poslední je uvedeno celkové shrnutí průzkumu.

- **Otázka č. 1: Používáte vzdálený přístup (mimo počítače v prostorech UK) k EIZ?**



Graf č.1: Graf k otázce č.1

- **Účel otázky** – rozdělit uživatele na ty, kteří vzdálený přístup používají a na ty, kteří tak nedělají. Druhá skupina v dotazníku postupuje na otázku č.2, první skupina přistupuje k otázce č.3.

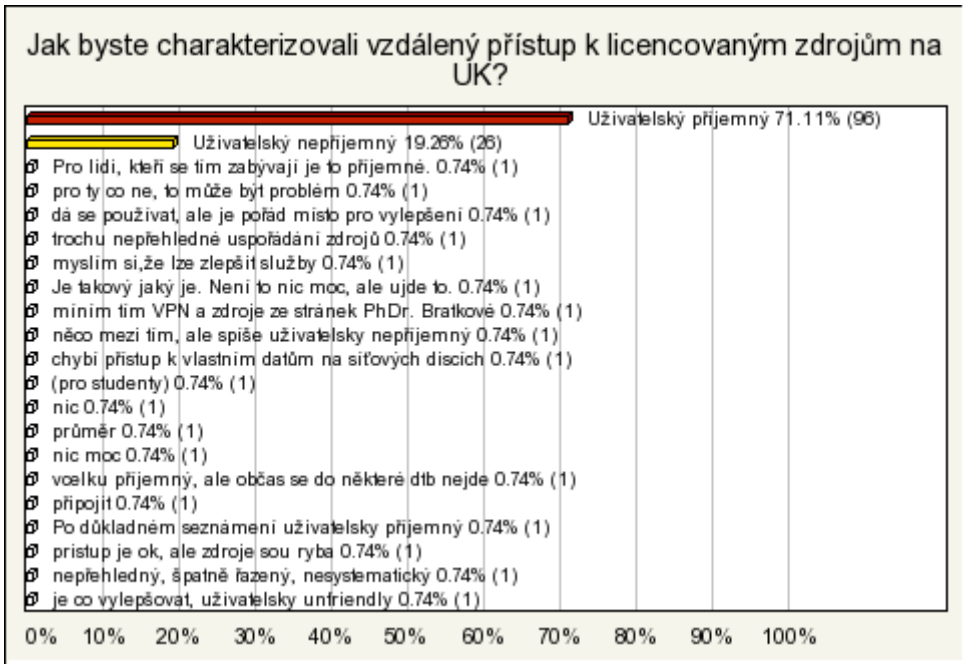
- **Výsledek -** Z celkového počtu 164 respondentů používá vzdálený přístup k elektronickým informačním zdrojům 129 (78,66%) respondentů. Zbylých 35 (21,34%) respondentů vzdálený přístup nevyužívá.

- **Otázka č.2: Proč nevyužíváte vzdálený přístup?**

Graf č.2: Graf k otázce č.2

- **Účel otázky** – Zjistit důvody, které uživatele vedou k tomu, že nepoužívají vzdálený přístup. Na výběr byly tři předem stanovené možnosti (v grafu první tři), případně vlastní odpověď. Respondenti zodpovídající tuto otázku v dotazníku dále nepokračovali.
- **Výsledek -** Z celkového počtu 35 respondentů byl jako nejčastější důvod vybrána odpověď: „Nepotřebuji používat vzdálený přístup k el. zdrojům“, kterou uvedlo 21(60%) respondentů.
- **Komentář –** Zde by patrně bylo vhodné zjistit, zda uživatelé vůbec využívají přístup k elektronickým informačním zdrojům.

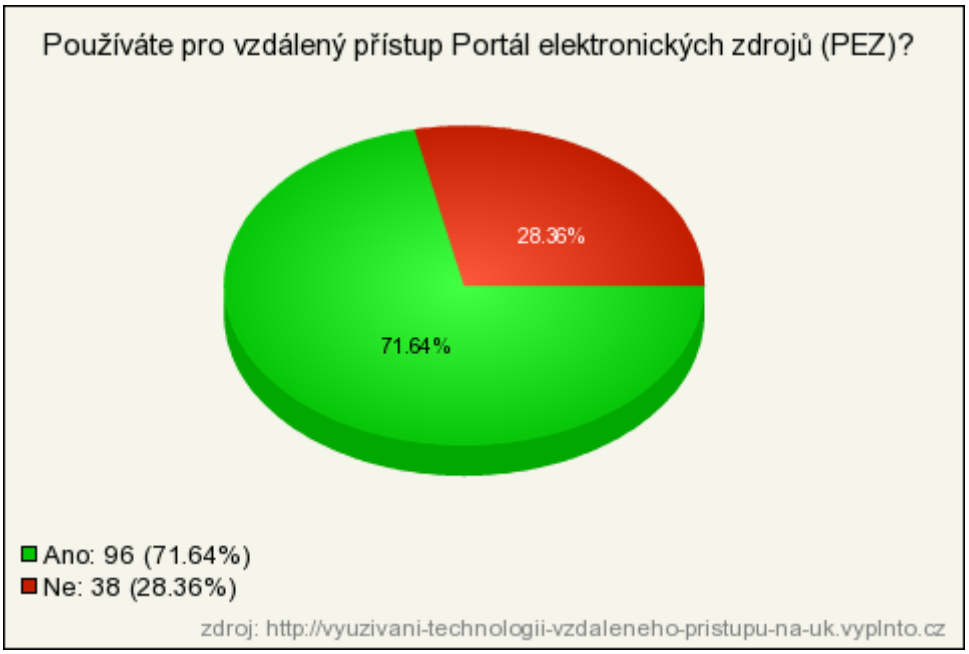
- **Otázka č. 3: Jak byste charakterizovali vzdálený přístup k licen-covaným zdrojům na UK?**



Graf. č3: Graf k otázce č.3

- **Účel otázky** – Cílem otázky bylo zjistit, zda respondentům vyhovuje celkové řešení vzdáleného přístupu na UK z uživatelského hlediska. Na výběr byly dvě možnosti (příjemný nebo nepříjemný) nebo vlastní vyjádření respondentů.
- **Výsledek –** Většina (71,11%) respondentů považuje vzdálený přístup na UK za uživatelsky příjemný. Přímo za uživatelsky nepříjemný ho označilo necelých 20%. Vlastní komentáře uživatelů se však z větší části jeví také jako negativní.
- **Komentář –** Vzhledem k vlastním odpovědím respondetům se zdá, že otázka nebyla položena zcela ideálně. Patrně došlo k představě, že se otázka týká především Portálu elektronických informačních zdrojů.

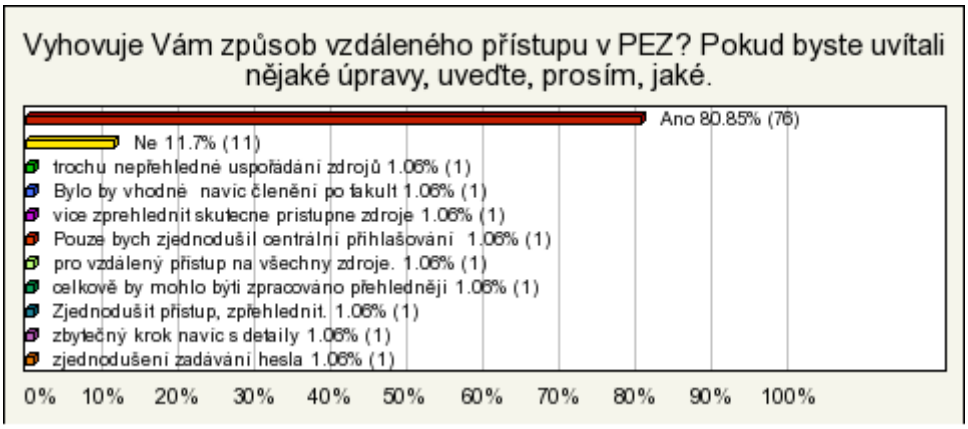
- **Otázka č.4: Používáte pro vzdálený přístup Portál elektronických zdrojů (PEZ)?**



Graf č.4: Graf k otázce č.4

- **Účel otázky** – Cílem otázky bylo zjistit, zda respondenti využívají pro vzdálený přístup Portál elektronických zdrojů. Respondenti, kteří odpověděli kladně přešli k otázce č. 5. Ostatní přešli rovnou k otázce č. 6.
- **Výsledek** – Většina 96(71,64%) respondentů používá PEZ, zbylých 38(28,36%) tak nečiní.
- **Komentář** – Počet uživatelů, kteří ke el. zdrojům přistupují z PEZ je poměrně vysoký, druhá skupina je však větší než bylo očekáváno. Dotazník způsob jejich přístup k el. zdrojům tedy neřeší.

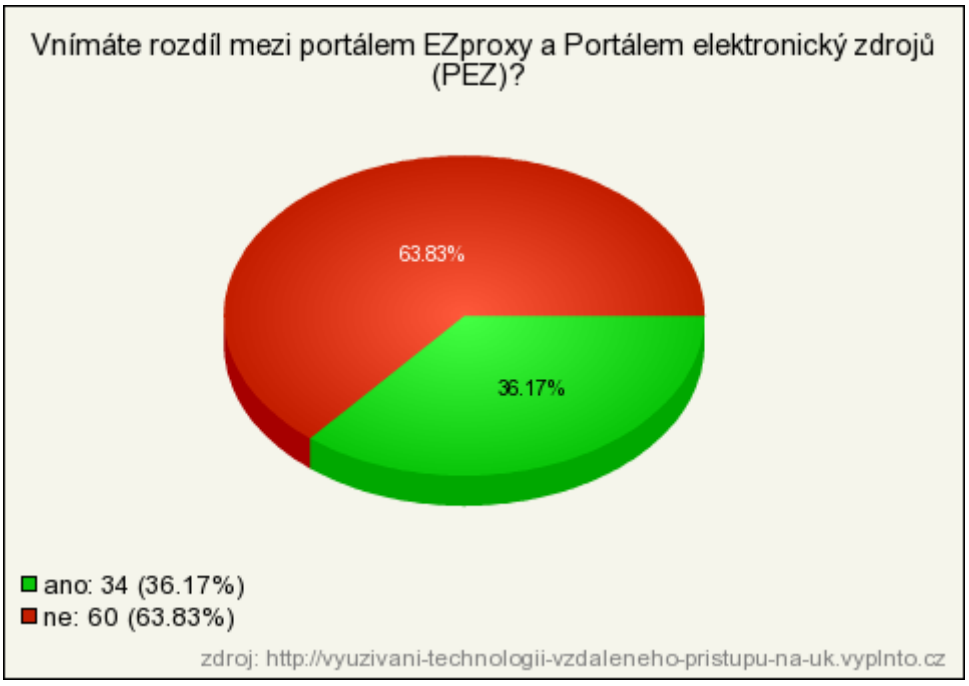
- **Otázka č.5: Vyhovuje Vám způsob vzdáleného přístupu v PEZ? Pokud byste uvítali nějaké úpravy, uveďte, prosím, jaké.**



Graf č.5: Graf k otázce č.5

- **Účel otázky** – Cílem otázky bylo zjistit, zda jsou respondenti spokojeni se způsobem, jakým je v PEZ řešena možnost vzdáleného připojení. Respondenti mohli uvést i vlastní názor.
- **Výsledek –** Většina 76(80,85%) shledává současný stav za vyhovující. Opačný názor má 20(19,15%) respondentů.
- **Komentář –** Respondenti nejčastěji „volají“ po změně přihlašování a lepším zpřehlednění dostupných zdrojů.

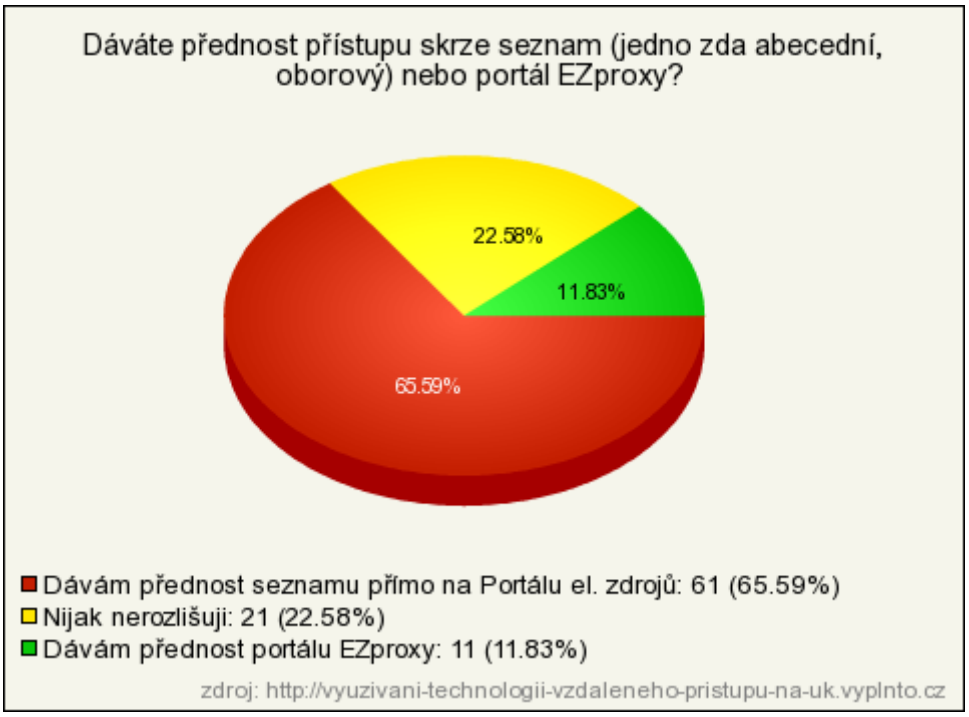
- **Otázka č.6: Vnímáte rozdíl mezi portálem EZproxy a Portálem elektronických zdrojů (PEZ)?**



Graf č.6: Graf k otázce č.6

- **Účel otázky** – Cílem otázky bylo zjistit, zda respondenti rozlišují mezi Portálem elektronických informačních zdrojů a EZproxy portálem.
- **Výsledek** – Většina 60(63,83%) respondentů mezi dvěma portály nerozlišuje. Rozdíl vnímá zbylých 34(36,17%).
- **Komentář** – Portál EZproxy není z úvodní stránky PEZ dostupný přímým linkem. Je tedy možné, že mnozí si jeho existence nejsou vědomi.

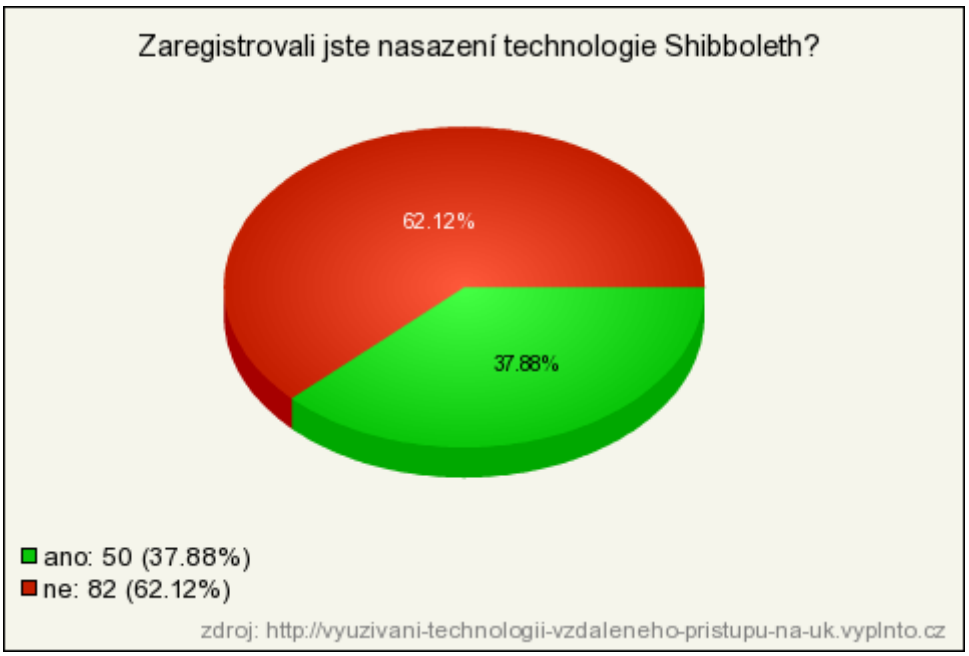
- **Otázka č.7: Dáváte přednost přístupu skrze seznam (jedno zda abecední, oborový) nebo portál EZproxy?**



Graf č.7: Graf k otázce č.7

- **Účel otázky** – Cílem otázky bylo zjistit, jaký z dvou výše uvedených portálů preferují.
- **Výsledek** – Většina 61(65,59%) respondentů upřednostňuje Portál elektronických informačních zdrojů. Portálu EZproxy dává přednost 11(11,83%) respondentů. Nerozlišuje 21(22,58%) respondentů.
- **Komentář** – Vzhledem k tomu, že uživatelé nerozlišují mezi oběma portály není výsledek překvapivý. Portál EZproxy, jak již bylo zmíněno, není dostupný přímým linkem z úvodní stránky PEZu, což může vést k tomu, že jeho přítomnost mnohý uživatel ani nezaregistruje, natož aby ho více využíval.

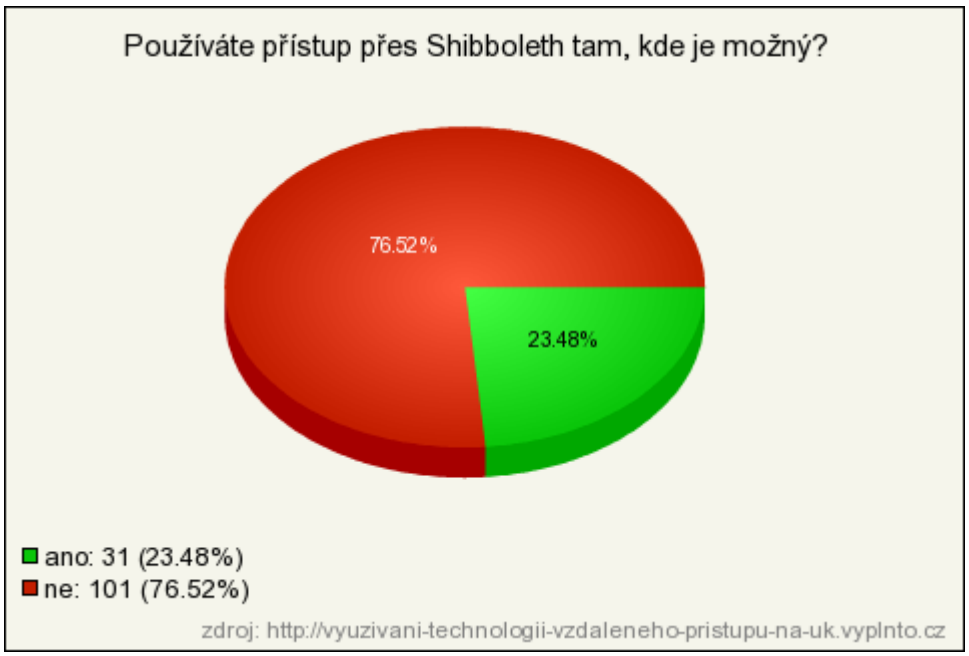
- **Otázka č.8: Zaregistrovali jste nasazení technologie Shibboleth?**



Graf č.4: Graf k otázce č.4

- **Účel otázky** – Cílem otázky bylo zjistit, zda respondenti zaregistrovali nasazení technologie Shibboleth.
- **Výsledek** – Většina 82(62,12%) respondentů nasazení technologie Shibboleth nezaregistrovala. Opačně hlasovalo 50(37,88%) respondentů.
- **Komentář** – Vzhledem k tomu, že Shibboleth byl na UK zprovozněn v květnu 2010 není výsledek zvláště překvapivý.

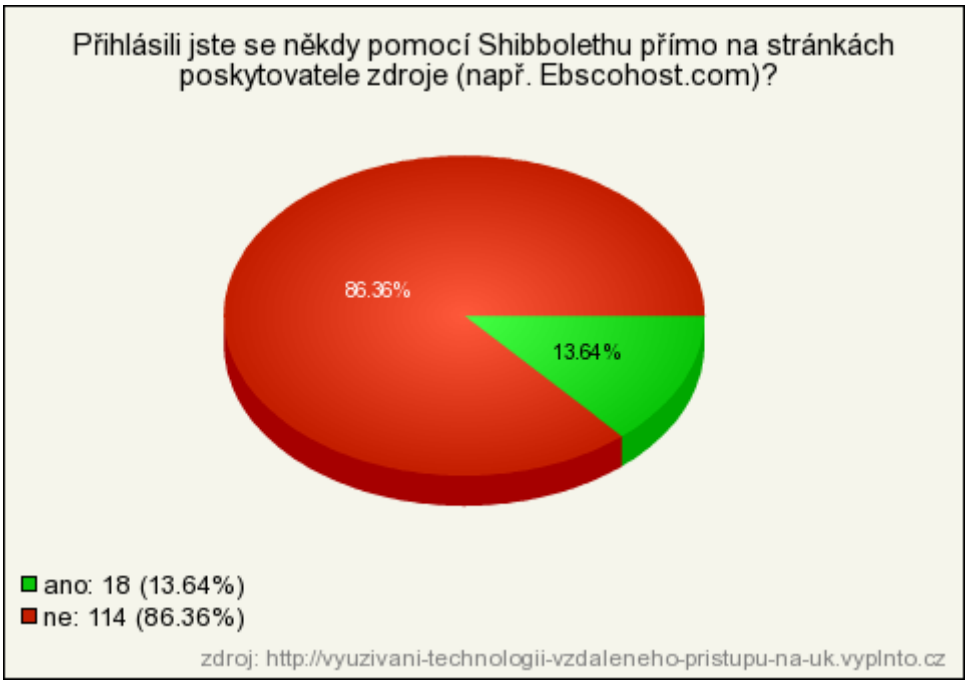
- **Otázka č.9: Používáte přístup přes Shibboleth tam, kde je možný?**



Graf č.9: Graf k otázce č.9

- **Účel otázky** – Cílem otázky bylo zjistit, zda respondenti využijí možnost přihlášení přes Shibboleth, když se jim ona možnost nabízí.
- **Výsledek** – Většina 101(76,52%) respondentů Shibboleth nepoužije. Opačně hlasovalo 31(23,48%) respondentů.
- **Komentář** – Uživatelé patrně raději využijí možnost, na kterou jsou zvyklí.

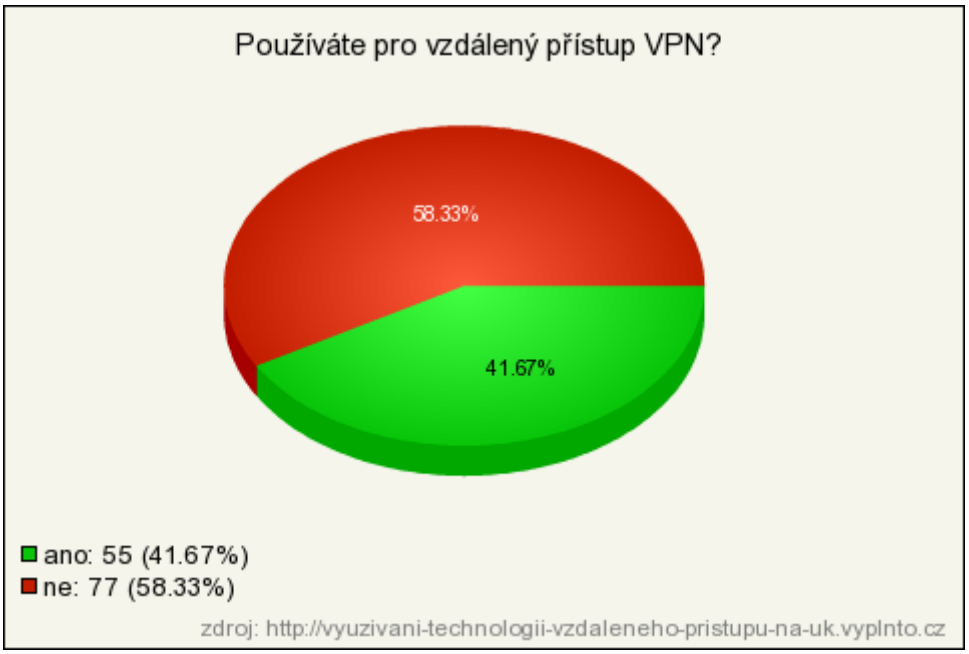
- **Otázka č.10: Přihlásili jste se někdy pomocí Shibbolethu přímo na stránkách poskytovatele zdroje (např. Ebscohost.com)?**



Graf č.4: Graf k otázce č.4

- **Účel otázky** – Zjistit, zda respondenti někdy využili možnosti přímého přihlášení za pomoci technologie Shibboleth na stránkách poskytovatele zdroje.
- **Výsledek** – Většina 114(86,36%) respondentů tuto možnost dosud nepoužila. Tento způsob přihlášení použilo 18(13,64%) dotázaných.
- **Komentář** – Z pohledu uživatelů patrně krajní možnost použití Shibbolethu. Vzhledem k odpovědím na předešlé dvě otázky však zcela logický výsledek.

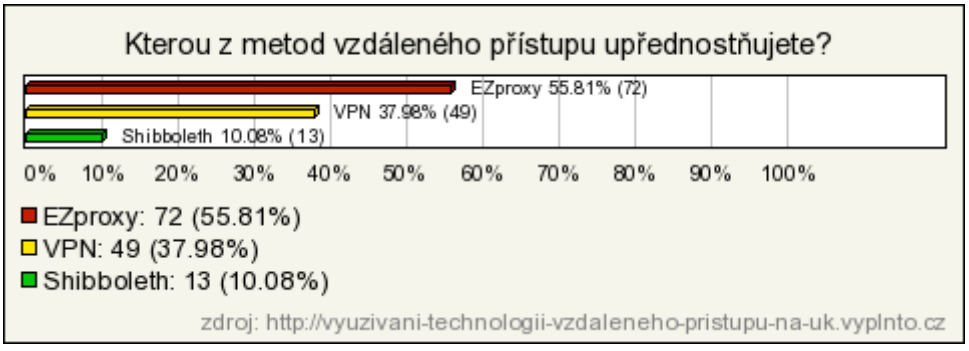
- **Otázka č.11: Používáte pro vzdálený přístup VPN?**



Graf č.11: Graf k otázce č.11

- **Účel otázky** – Zjistit, zda respondenti využívají možnost připojení ke vzdáleným zdrojům pomocí VPN.
- **Výsledek** –Většina 77(86,36%) respondentů VPN nepoužívá, zbylých 55(41,67%) však ano.
- **Komentář –** Zde je vidět, že VPN i když jedna z historicky nejstarších metod na UK je stále hojně využívána.

- **Otázka č.12: Kterou z metod vzdáleného přístupu upřednostňujete? VPN x EZproxy x Shibboleth**

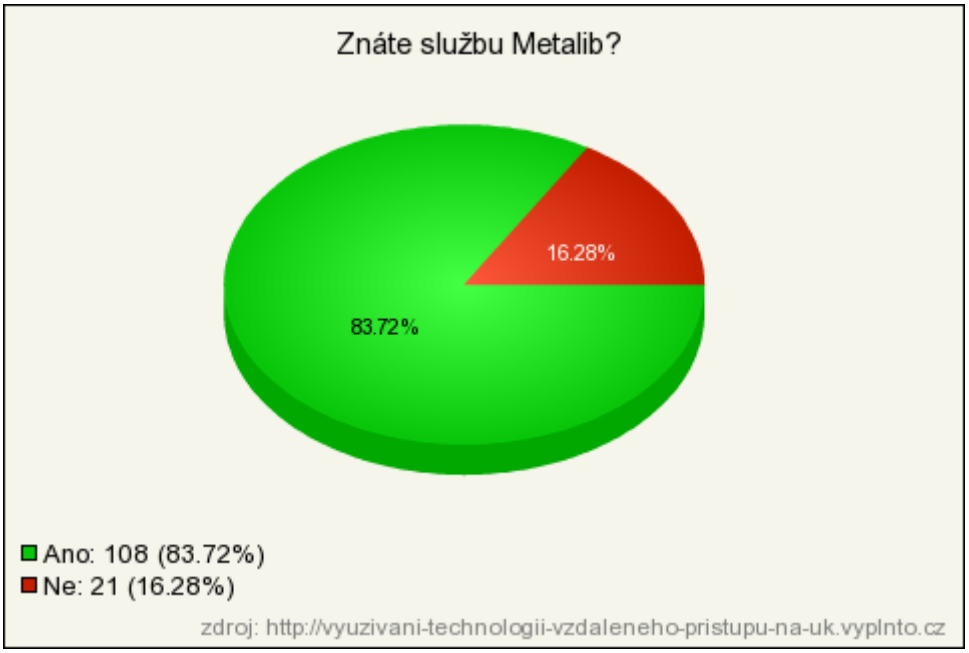


Graf č.12: Graf k otázce č.12

- **Účel otázky** – Zjistit, které z metod vzdáleného připojení uživatelé preferují.

- **Výsledek –** V pomyslném souboji metod zvítězilo EZproxy s 72(55,81%) hlasy, na druhém místě se umístilo VPN s 49(37,98%) a poslední pozici obsadil Shibboleth s 13(10,08%) hlasy.
- **Komentář –** Výsledky odpovídají předchozím odpovědím respondentů. Snad jen, že patrně 5 respondentů používajících VPN upřednostní EZproxy nebo Shibboleth.

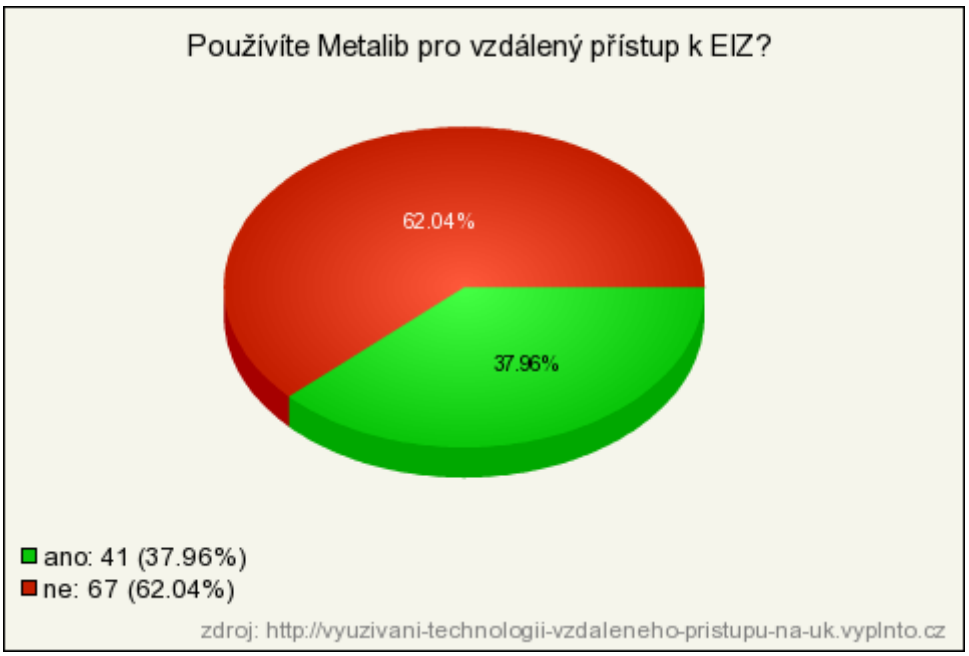
- **Otázka č.13: Znáte službu Metalib?**



Graf č.13: Graf k otázce č.13

- **Účel otázky** – Zjistit, zda uživatelé znají službu Metalib. Otázka byla použita pro selekci těch, kteří ji znají. Ti pak následně odpovídali na otázku č.14. Ostatní přešli k otázce č.15.
- **Výsledek –** Znalost potvrdilo 108(83,72%) respondentů. Službu nezná 21(16,28%) respondentů.
- **Komentář –** Z výsledků vyplývá, že služba Metalib je poměrně známá, přesto by patrně neškodila její větší propagace.

- **Otázka č.14: Používáte Metalib pro vzdálený přístup k EIZ?**



Graf č.14: Graf k otázce č.14

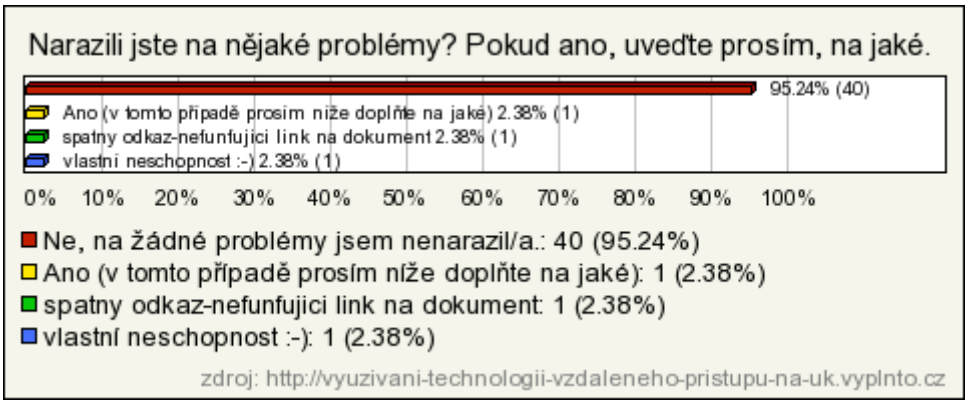
- **Účel otázky** – Zjistit, zda uživatelé používají službu Metalib pro vzdálený přístup k elektronickým informačním zdrojům.
- **Výsledek –** Více 67(62,42%) uživatelů službu Metalib pro vzdálený přístup nepoužívá než používá 41(37,96)
- **Komentář –** S dostupnými daty lze o důvodech nevyužívání pouze spekulovat, ale mohlo by za tím být poměrně náročnější uživatelské prostředí.

- **Otázka č.15: Používáte vzdálený přístup při linkování z výsledků vyhledávání v Google Scholar?**

Graf č.15: Graf k otázce č.15

  - **Účel otázky** – Zjistit, zda uživatelé využívávají možnost vzdáleného přístupu pro linkování z výsledků vyhledávání v Google Scholar. Uživatelé, kteří si vybrali kladnou odpověď, přešli k otázce č. 16. Ostatní přešli k otázce č. 17.
  - **Výsledek –** 87(67,44%) respondentů tuto možnost nevyužívá, menšina 42(32,56%) respondentů ano.
  - **Komentář –** Z mého pohledu překvapivý výsledek, protože tím uživatelé přicházejí o dostupnost značné části plných textů.

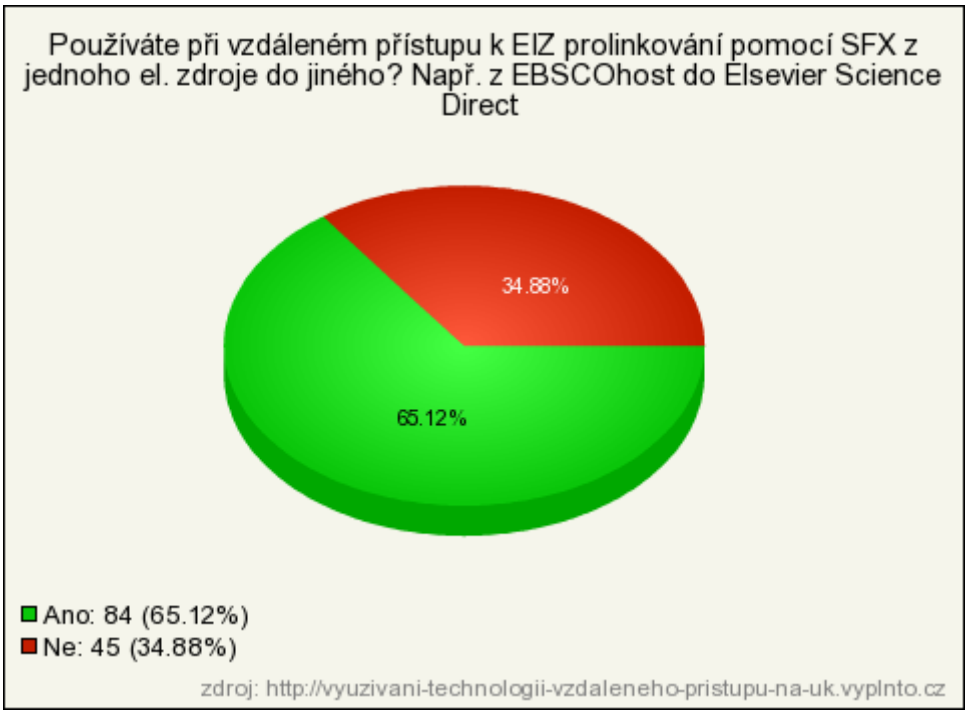
- **Otázka č. 16: Narazili jste na nějaké problémy? Pokud ano, uveďte prosím, na jaké.**



Graf č.16: Graf k otázce č.16

- **Účel otázky** – Zjistit, zda uživatelé při používání vzdáleného přístupu pro linkování z výsledků vyhledávání v Google Scholar narazili na nějaké problémy.
- **Výsledek** – 40(95,24)% respondentů na žádné problémy nenarazilo, pouze 3(4,76%) ano.
- **Komentář –** Značně positivní výsledek.

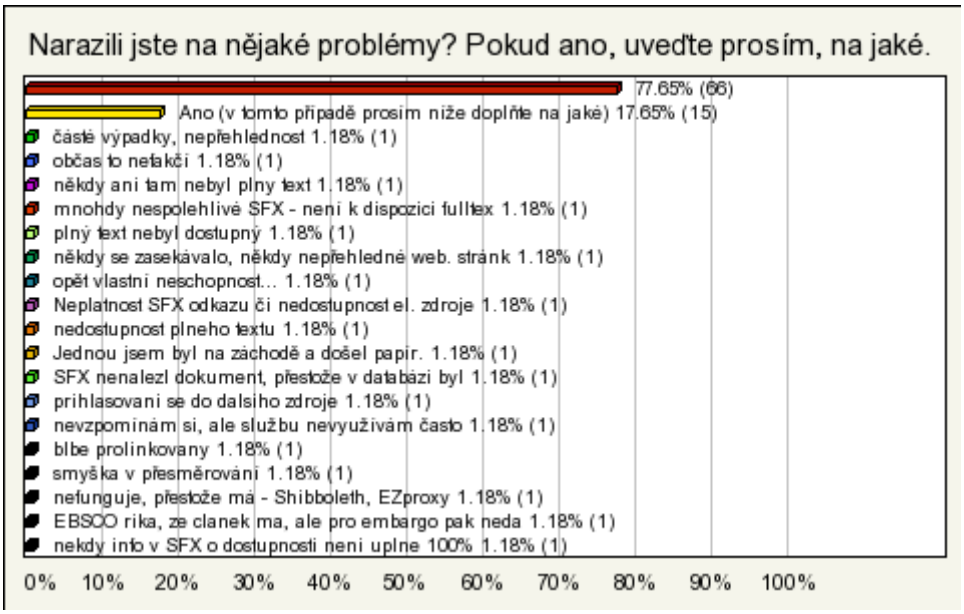
- **Otázka č.17: Používáte při vzdáleném přístupu k EIZ prolinkování pomocí SFX z jednoho el. zdroje do jiného? Např. z EBSCOhost do Elsevier Science Direct**



Graf č.17: Graf k otázce č.17

- **Účel otázky** – Cílem bylo zjistit, zda respondenti používají při vzdáleném přístupu k EIZ prolinkování pomocí SFX z jednoho elektrického zdroje do jiného. Uživatelé, kteří si vybrali kladnou odpověď, přešli k otázce č. 18. Pro zbytek dotazník skončil.
- **Výsledek** – 84(65,12%) respondentů tuto možnost využívá, 45(34,8%) respondentů ne.
- **Komentář** – Vzhledem k užitečnosti dané služby se nelze kladnému výsledku divit.

- **Otázka č. 18: Narazili jste na nějaké problémy? Pokud ano, uveďte prosím, na jaké.**



Graf č.18: Graf k otázce č.18

- **Účel otázky** – Zjistit, zda uživatelé, kteří odpověděli kladně na minulou otázku narazili na nějaké problémy. Poslední otázka dotazníku
- **Výsledek –** 66(77,65%) respondentů na problémy nenarazilo, zbylých 32(22,35%) ano.
- **Komentář –** SFX není vždy úplně spolehlivé, ale to je vcelku známý fakt.

6.5 Celkové shrnutí

6.5.1 Pozitiva a nedostatky dotazníku jako takového

Následující shrnutí vychází z výsledků dotazníků a především z autorovy osobní interpretace daných výsledků.

Nejprve začnu nedostatky dotazníku. Ty zpětně shledávám v tom, že dotazník nerozlišoval, zda se jedná o studenta či vyučujícího (případně z vlastního hlediska uživatele, zda se jedná o profesionála nebo amatéra). Druhým nedostatkem byla neobjevená chyba technického rázu, kdy patrně došlo ke špatnému nastavení dotazníku a někteří respondenti (celkem 5), kteří odpověděli, že nepoužívají vzdálený přístup přesto mohli pokračovat v dalším vyplňování dotazníku.

Nepodařilo se však vypátrat, zda se jedná o chybu systému vyplňto.cz nebo chybu autorovu.

Naopak značné pozitivum je, že i přes probíhající prázdniny se podařilo shromáždit odpovědi celých 164 respondentů. V tomto však nelze opominout značnou kolegiálnost lidí z Ústavu informačních studií a knihovnictví, kteří ochotně dotazník vyplňovali (cca 80 respondentů odpovědělo doslova pár hodin po odeslání emailu do konference UISK118) a také pracovníků z Ústavu výpočetní techniky UK, kteří iniciativně dotazník vystavili na Portále elektronických informačních zdrojích.

K samotným výsledkům průzkumu. Počet lidí, kteří odpověděli, že vůbec nevyužívají vzdálený přístup je z mého pohledu velmi vysoký. A to z důvodu, že ke studiu na ÚISKu je minimálně v rámci některých předmětů vzdálený přístup třeba a v případě respondentů mimo ÚISK je zvláštní, že dotazník objevili (viz kanály jeho propagace). Na druhou to se týká pouze těch, kteří odpověděli, že ho nepotřebují. Ostatní k tomu patrně mají vážnější důvod.

Dále bych zhodnotil z mého pohledu nejdůležitější body průzkumu. Vyberu nejproblematičtější části vyplívající z průzkumu a navrhnu jejich řešení (bez ohledu na technologickou řešitelnost).

6.5.2 Portál elektronických informačních zdrojů

Převažující část (71%) respondentů pro vzdálený přístup k el. zdrojům PEZ využívá. Z toho celých 80% respondentů jsou se stávajícím stavem PEZ spokojeni. Nedá se však opomíjet hlas zbylých 20%, kteří nějakým způsobem spokojeni nejsou. Hlavními problémy, které respondenti zmiňují jsou způsob přihlašování a nepřehlednost nabízených zdrojů.

Možným řešením prvního problému by mohlo být přihlášení již při vstupu na PEZ a dále se pohybovat v rámci SSO prostředí (tak jak to nyní funguje po přihlášení se k prvnímu zdroji). V současnosti musí uživatel podniknout až 5 „kroků“ než se dostane k požadovanému zdroji.

Druhý problém by snad částečně mohla řešit možnost individuálního nastavení, kdy by si uživatel mohl přizpůsobit portál tak, aby měl možnost si zobrazit pouze své oblíbené zdroje (to je technologicky pravděpodobně velice komplikovaně řešitelné). Tento problém patrně také trochu řeší portál EZproxy, který je však v PEZ

schován „až“ za odkazem na vzdálený přístup. Ostatně většina respondentů (63,83%) portál EZproxy nerozlišuje od PEZ.

6.5.3 Shibboleth

Nadpoloviční většina (62,12%) respondentů nezaregistrovala nasazení technologie Shibboleth. To samo o sobě bude pravděpodobně hlavním důvodem toho, že většina (76,52%) respondentů nevyužívá možnost přístupu pomocí Shibbolethu. Vzhledem ke krátké době, kdy je Shibboleth na UK implementován je však stále dostatek prostoru k seznamování uživatelů s použitím. Např. pomocí výukových videí, jako je tomu u technologie SFX.

6.5.4 VPN

Jak ukázal průzkum technologie VPN je stále hojně využívána. Přihlásilo se k ní 41,67% respondentů. Svým způsobem to je zcela pochopitelné. VPN na UK funguje již dlouho, takže mnozí jsou na ní zvyklí. Po přihlášení může člověk volně „brouzdat“ internetem a jsou mu zpřístupňovány rovnou funkce, na které má z daného rozsahu IP adres právo. Zde se také ukazuje, že překážka v podobě dodatečného nastavování zvláštního připojení není pro velkou část uživatelů problém.

Nutno podotknout, že VPN servery budou výhledově končit, vzhledem k přecházení na adresy IPv6. Když nic, tak toto je dalším důvodem k seznamování uživatelů s technologií Shibboleth.

6.5.5 Oblíbenost jednotlivých technologií

Zde se patrně nekonalo žádné překvapení. Nejpoužívanější technologií je EZproxy, která funguje také již nějakou chvíli. Nenutí uživatele k instalaci žádných doplňků a je podporována v rámci PEZ, v němž jsou přímo zabudovány EZproxy linky, které až do příchodu technologie Shibboleth neměly „konkurenci“. Tedy pokud uživatelé nebyli připojení do lokální sítě Jinonice pomocí VPN, které je druhou nejpoužívanější metodou. Ti však mohli využívat přímého přístupu, jak z PEZ, tak odjinud.

6.5.6 Nadstavbové služby Metalib a SFX

Metalib, ač znám celým 83% respondentů, není pro vzdálený přístup příliš využíván. K tomu ho používá 38% respondentů. Důvody nelze z průzkumu zjistit, tak lze pouze spekulovat. Domnívám se, že to bude způsobeno vyšší uživatelskou náročností, která může být překážkou jinak velice „šikovné“ službě.

SFX je služba, která je mezi respondenty používána více, a to při využití k prolinkování z jedno zdroje do druhého, takto činí 65% respondentů. Ačkoliv většina uživatelů (77%) hlásí bezproblémové fungování služby SFX, tak z vlastních reakcí respondentů se dá vyčíst, že tomu tak vždy není. Spravovat databáze SFX je však poměrně náročná činnost a nelze se tomu divit.

6.5.7 Závěr

Obecně se dá říci, že uživatelé jsou spíše spokojeni. Za uživatelsky příjemné bylo řešení vzdáleného přístupu na UK označeno 71% respondenty. Přesto existují oblasti, ve kterých je stále, co zlepšovat. Ty jsem se na základě výsledků pokusil přiblížit výše. Z mého pohledu je strategie řešení vzdáleného přístupu dána dlouholetými zkušenostmi odpovědných osob a nezbývá než postupovat dále potřebnou „mravenčí prací“.

7 Závěr

Vzdálený přístup k elektronickým informačním zdrojům, zvláště těch pro vědu a výzkum, je jednou ze základních služeb, kterou by měly poskytovat (a také

tak dnes již ve velké míře dělají) jak větší odborné knihovny, tak akademické instituce. Cílem této práce bylo popsat a zhodnotit jednotlivé technologie, které to umožňují. Problematika vzdáleného přístupu je popisována ve vztahu k Univerzitě Karlově, aby práce nebyla pouhým teoretizováním.

Úvodní část práce stručně popisuje stav přístupnosti elektronických informačních zdrojů na Univerzitě Karlově a definuje některé základní pojmy, jako rozlišení vzdáleného a přímého přístupu.

Ve druhé kapitole se řeší problematika správy identit a přístupů. Ta je nezbytným procesem k umožnění vzdáleného přístupu takovým uživatelům, kteří na něj mají nárok. Popsány jsou základní metody využívaných pro autentizaci uživatelů a to jak na straně jejich domácí instituce, tak na straně elektronického informačního zdroje, ke kterému přistupují. Pozornost je věnována také federacím, konkrétně České akademické federaci identit EduID.cz, která umožňuje uživatelům z různých organizací přistupovat k externím zdrojům s využitím svých domovských přihlašovacích údajů, jejímž členem je právě Univerzita Karlova.

Třetí kapitola se věnuje popisu Centrálních autentizačních služeb, které slouží jako centrální správa identit a přístupů na Univerzitě Karlově. A zároveň poskytuje potřebné informace pro přihlašování v rámci federace.

Čtvrtá kapitola je popisem a zhodnocením jednotlivých technologií vzdáleného přístupu, které jsou nebo byly používány na Univerzitě Karlově. Jako nejvhodnější se jeví využití technologie Shibboleth.

Pátá kapitola je popisem implementace technologií vzdáleného přístupu z uživatelova pohledu v Portále elektronických informačních zdrojů, který je hlavním bodem Univerzity Karlovy pro přístup k elektronickým informačním zdrojům

Šestá a poslední kapitola je vyhodnocením průzkumu oblíbenosti a využití jednotlivých metod vzdáleného přístupu Univerzitě Karlově. Ten poukázal na některé dílčí nedostatky, jako malou známost technologie Shibboleth mezi uživateli, ale zároveň spíše celkovou spokojenost uživatelů s řešením vzdáleného přístupu na Univerzitě Karlově.

Seznam použité literatury

- APELBAUM, Jacob. *User Authentication Principles, Theory and Practice*. [New York, USA] : Fuji Technology, 2004. 228 s. ISBN 978-0-980-00000-9.
- BARANAYOVÁ, Irena. *Univerzita Karlova v Praze* [online]. Praha : Univerzita Karlova, Ústav výpočetní techniky, 2010 [cit. 2010-07-11]. Centrální knihovně-informační systém UK . Dostupné z WWW: <http://alephuk.cuni.cz/>.
- BEHÚN, Dalibor. *Interval.cz* [online]. 25.11.2004 [cit. 2010-07-21]. Hříchy pro šíleného korektora - autentizace, autentikace nebo autentifikace?. Dostupné z WWW: <http://interval.cz/clanky/hrichy-pro-sileneho-korektora-autentizace-autentikace-nebo-autentifikace/>.
- BEITLOVÁ, Michaela. *Univerzita Karlova v Praze* [online]. Praha : Univerzita Karlova, Ústav výpočetní techniky, 2010, poslední změna 9. 7. 2010 [cit. 2010-08-11]. Verde. Dostupné z WWW: <http://verde.cuni.cz/>.
- BLANSIT, Douglas B. Beyond Password Protection : Methods for Remote Patron Authentication. *Journal of Electronic Resources in Medical Libraries*. 2007, 4, 1/2, s. 185-193. ISSN 1542-4065.
- *CAS : Centrální autentizační služby UK* [online]. Stránka generována 16.07.2010 [cit. 2010-07-16]. Informace o autentizační službě. Dostupné z WWW: <https://ldap.cuni.cz/info.php>.
- CELBOVÁ, Ludmila. 2005a. Informační zdroj. In *KTD : Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online databáze]. Praha : Národní knihovna České republiky, 2003- [cit. 2010-05-07]. Dostupné z WWW: <http://sigma.nkp.cz/cze/ktd>.
- CELBOVÁ, Ludmila. 2005b. Elektronický zdroj. In *KTD : Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online databáze]. Praha : Národní knihovna České republiky, 2003- [cit. 2010-05-07]. Dostupné z WWW: <http://sigma.nkp.cz/cze/ktd>.
- CESNET. *CESNET* [online]. Praha : 2007 [cit. 2010-07-30]. Záměr 2006: AAI a mobilita. Dostupné z WWW: <http://www.cesnet.cz/doc/2006/zprava/aai.html>.
- *EduID.cz : Česká akademická federace identit* [online]. Praha : CESNET, 2009, oslední úprava 2009-04-30 [cit. 2010-08-11]. Dostupné z WWW: <http://www.eduid.cz/wiki/eduid/index>.
- FEILNER, Markus. *OpenVPN : Building and Integrating Virtual Private Networks*. 1st published. Birmingham : Packt, 2006. 258 s. ISBN 1-904811-85-X.

- FOJTŮ, Andrea. *Univerzita Karlova v Praze* [online]. Praha : Univerzita Karlova, Ústav výpočetní techniky, 2007 [cit. 2010-07-11]. Digitool. Dostupné z WWW: <http://digitool.cuni.cz/>.
- HANÁČEK, Petr; STAUDEK, Jan. Správa identity. In HRUŠKA, Tomáš. DATAKON 2005 : Brno, 22.-25. 10. 2005. [s.l.] : [s.n.], 2005. s 123-146. Dostupné z WWW: <http://www.fi.muni.cz/usr/staudek/vyuka/security/stud_lit/d05_idm_tutorial_text.pdf>. ISBN 80-210-3813-6.
- HOWES, Timothy A.; SMITH, Mark C.; GOOD, Gordon S. *Understanding and deploying LDAP directory services*. 2nd ed. Boston (Massachussets) : Pearson Education, 2003. 899 s. ISBN 0-672-32316-8.
- HUNTIGTON VENTURES. *AuthenticationWorld.com : The business of authentication* [online]. c2006a [cit. 2010-07-24]. User Authentication. Dostupné z WWW: <http://www.authenticationworld.com/Authentication-User/>.
- HUNTIGTON VENTURES. *AuthenticationWorld.com : The business of authentication* [online]. c2006b [cit. 2010-07-24]. Single Sign On. Dostupné z WWW: <http://www.authenticationworld.com/Single-Sign-On-Authentication/>.
- Info Technology Supply. *ITS : Essential IT solutions for the Education, Public and Corporate sectors* [online]. c2009 [cit. 2010-07-30]. ITS:Onelog. Dostupné z WWW: <http://www.itsltduk.co.uk/Our_offerings/Access_Management/Onelog_Landing_Page.aspx>.
- Internet2. *Shibboleth : A Project of Internet2 Middleware Initiative* [online]. c2010 [cit. 2010-08-11]. Dostupné z WWW: <http://shibboleth.internet2.edu/>.
- IP address. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 25 August 2001, last modified on 6 August 2010 [cit. 2010-08-06]. Dostupné z WWW: <http://en.wikipedia.org/wiki/IP_address>.
- KENNEDY, David. Authentication and Authorization in Libraries. In COURTNEY, Nancy. *More Technology for the Rest of Us : A Second Primer on*

Computing for the Non-IT Librarian. Santa Barbara (California) : ABC-Clio, 2010. s. 55-67. ISBN 978-1-59158-939-6.

- KOUŘIL, Daniel, et al. Federace identit : aneb spolčení totožností. *Zpravodaj ÚVT MU*. 2007, roč. 18, č. 2, s. 1-7. Dostupný také z WWW: <http://www.ics.muni.cz/zpravodaj/articles/566.html>. ISSN 1212-0901.
- Kučerová. 2005. Elektronický zdroj. In *KTD : Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online databáze]. Praha : Národní knihovna České republiky, 2003- [cit. 2010-05-07]. Dostupné z WWW: <http://sigma.nkp.cz/cze/ktd>.
- KOSEK, Jiří. *XML pro každého* [online]. c2000-2004 [cit. 2010-07-29]. Dostupné z WWW: <http://www.kosek.cz/xml/index.html>.
- KUBEŠ, Radim. *Ústav vědeckých informací 2. lékařské fakulty* [online]. verze 1.0.1. 2007 [cit. 2010-07-30]. OneLog : Vzdálený přístup k e-zdrojům. Dostupné z WWW: <http://knihovna.lf2.cuni.cz/vyhledavani/navodonelog.pdf>.
- KRHOVJÁK, Jan; MATYÁŠ, Václav. Autentizace a identifikace uživatelů. *Zpravodaj ÚVT MU*. 2007, 13, 1, s. 1-5. Dostupný také z WWW: <http://www.ics.muni.cz/zpravodaj/articles/560.html>. ISSN 1212-0901.
- LDAP. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 12. 3. 2006, last modified on 9. 8. 2010 [cit. 2010-08-11]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/LDAP>.
- LUHOVÝ, Karel. Virtuální privátní sítě VPN. *Svět sítí* [online]. 2003, [cit. 2010-06-28]. Dostupný z WWW: <http://www.svetsiti.cz>.
- MIKESELL, Brian L. . Anything, Anytime, Anywhere : Proxy Servers, Shibboleth, and the Dream of the Digital Library. *Journal of Library Administration*. 2004, 41, 1/2, s. 315-326. ISSN 0193-0826.
- Novakov, Ivan. *Web Single Sign On Systems*. Praha : CESNET, 2006. Technical report number 21/2006. Dostupný také z WWW: <http://www.cesnet.cz/doc/techzpravy/2006/web-sso/>.
- OCLC. 2010a. EZproxy [OCLC – Management Services and systems]. [online]. [cit. 2010-07-27]. Dostupný z WWW: <http://www.oclc.org/us/en/ezproxy/default.htm>.
- MORÁVEK, Jakub; PEŠA, Radim. VPN server Masarykovy univerzity. *Zpravodaj ÚVT MU*. 2003, roč. 14, č. 2, s. 10-12. Dostupný také z WWW: <http://www.ics.muni.cz/zpravodaj/articles/292.html>. ISSN 1212-0901.

- OCLC. 2010b. URL Rewriting [OCLC – Documentation]. [online]. [cit. 2010-07-27]. Dostupný z WWW: <http://www.oclc.org/us/en/support/documentation/ezproxy/rewrite.htm>.
- PAVLÍK, Jiří. *EIZ UK* [online]. 2010 [cit. 2010-08-11]. Co jste možná nevěděli k Shibboleth na UK. Dostupné z WWW: <http://eizuk.blogspot.com/2010/06/co-jste-mozna-nevedeli-k-shibboleth-na.html>.
- PAVLÍK, Jiří. SFX, Verde a MetaLib ve službách Univerzity Karlovy v Praze. *Ikaros* [online]. 2008a, roč. 12, č. 5 [cit. 22.07.2010]. Dostupný na World Wide Web: <http://www.ikaros.cz/node/4722>. URN-NBN:cz-ik4722. ISSN 1212-5075.
- PAVLÍK, Jiří; NOVÁK, Petr Česká shibboletovská federace a vzdálený přístup k elektronickým zdrojům pomocí shibboleth. In *Knihovny současnosti 2008 : Sborník z 16. konference, konané ve dnech 16.-18. září 2008 v Seči u Chrudimi*. Brno : Sdružení knihoven ČR, 2008b. s. 373. Dostupné z WWW: <http://www.svkos.cz/data/xinha/sdruk/2008-1-078.pdf>. ISBN 978-80-86249-49-0.
- PAVLÍK, Jiří. Správa vzdáleného přístupu k elektronickým informačním zdrojům. Praha : Česká zemědělská univerzita, 2009. Dostupné z WWW: <http://www.slideshare.net/jpavlik88/shibboleth-1678818>.
- PETERKA, Jiří. *EArchiv.cz : archiv článků a přednášek Jiřího Peterky* [online]. 2000 [cit. 2010-07-24]. IP adresy. Dostupné z WWW: <http://www.earchiv.cz/anovinky/ai1646.php3>.
- PETRI, Daniel. Understanding VPN Remote Access Mechanism. *Petri IT Knowledgebase* [online]. 2009-01-08 [cit. 2010-07-08]. Dostupné z WWW: <http://www.petri.co.il/understanding-vpn-remote-access-mechanism.htm>.
- *PEZ - Portál elektronických informačních zdrojů UK* [online]. Praha : Univerzita Karlova, Ústav výpočetní techniky, 2007 [cit. 2010-08-11]. Dostupné z WWW: <http://pez.cuni.cz/ezdroje/>.
- PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z*. 2. aktualizované vyd. Brno : Computer Press, 2006. 430 s. ISBN 80-251-1278-0.

- Remote Desktop Services. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 22 March 2006, last modified on 12 July 2010 [cit. 2010-07-19]. Dostupné z WWW: <http://en.wikipedia.org/wiki/Remote_Desktop_Services>.
- SAML. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 22 January 2008, [cit. 2010-07-29]. Dostupné z WWW: <http://en.wikipedia.org/wiki/SAML>.
- SOVA, Milan. Federativní přístup k autentizaci. In TKAČÍKOVÁ, Daniela; RAMAJZLOVÁ, Barbora. *Automatizace knihovnických procesů – 10 : sborník z 10. ročníku semináře pořádaného ve dnech 3.–4. května 2005 v Liberci.* Praha : ČVUT, 2005. s. 9-15. Dostupné z WWW: <http://www.akvs.cz/akp-2005/03-sova.pdf>. ISBN 80-01-03228-0.
- SVRŠEK, Ladislav. Využívajte e-zdroje správne. In *ITlib*. Informačné technológie a knižnice [online]. 2004, č. 01 [cit. 2010-07-05]. Dostupné na WWW: <http://www.cvtisr.sk/itlib/itlib041/svrsek1.htm>. ISSN 1336-0779.
- TYSON, Jeff. In *HowStuffWorks?* [online]. c1998-2010 [cit. 2010-06-28]. How Virtual Private Networks Work. 2001. Dostupné z WWW: <http://computer.howstuffworks.com/vpn.htm>.
- SWITCH. *SWITCH : Serving Swiss Universities* [online]. c2010 [cit. 2010-08-11]. AAI Demo. Dostupné z WWW: <http://www.switch.ch/aai/demo/>.
- Uniform Resource Locator. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 22. 9. 2004, last modified on 12. 6. 2010 [cit. 2010-07-21]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Uniform_Resource_Locator>.
- *Univerzita Karlova v Praze* [online]. Praha : Univerzita Karlova, 2004, 29.říjen 2008 [cit. 2010-07-11]. O Ústřední knihovně UK . Dostupné z WWW: <http://www.cuni.cz/UK-2200.html>.
- VAŠEK, Jiří. VNC a Vzdálená plocha : kouzlo vzdáleného přístupu. In *Pc Tuning* [online]. S.l. : Mediacop, 11.2.2009 [cit. 2010-07-19]. Dostupné z WWW: <http://pctuning.tyden.cz/software/jak-zkrotit-internet/12639-vnc_a_vzdalena_plocha-kouzlo_vzdaleneho_pristupu>. ISSN 1214-0201
- VOCŮ, Michal. *SCWiki* [online]. 2007 [cit. 2010-07-16]. Politika CAS. Dostupné z WWW: <https://supercomp.cuni.cz/wiki/index.php/Politika_CAS>.

- WINDLEY, Phillip J. *Digital Identity*. 1st ed. Sebastopol (California) : O'Reilly Media, 2005. 234 s. ISBN 0-596-00878-3.
- ZACH, Michael. Kontextové linkování na Univerzitě Karlově [Context-sensitive linking at Charles University in Prague]. Praha, 2010. 88 s. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí diplomové práce Ing. Jiří Pavlík