WEBnet počítačová síť ZČU

Ing. Michal Petrovič

Seminář CIV 2006

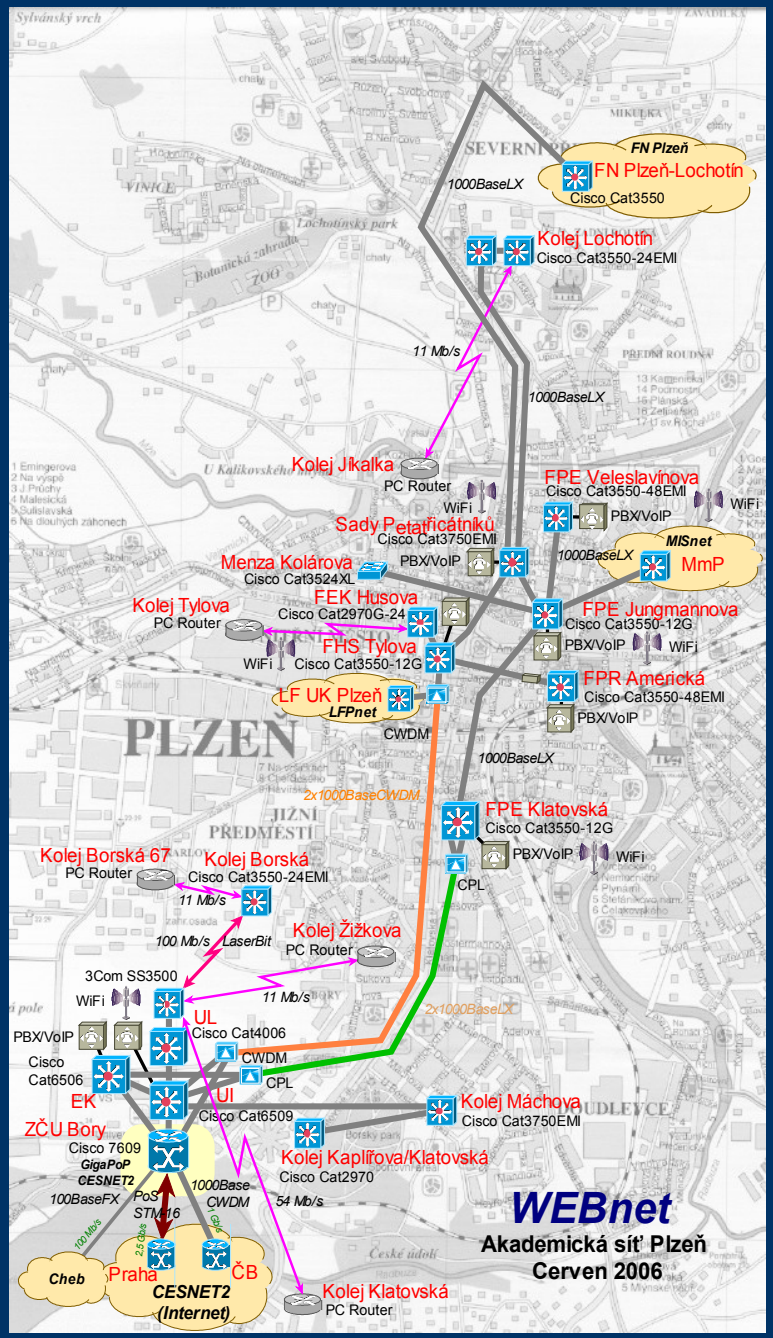
CIV-LPS

Obsah

- WEBnet – novinky
  - IP kamery v menze
  - VPN
  - IP telefonie
- CESNET
- Koleje
- Eduroam a Eduroam-simple
- Dotazy

WEBnet - novinky

- Počet PC cca 4200 + 2600
- Počet síťových prvků 154 + 71
- Změny:
  - Sady Pětatřicátníků
  - Kollárova
  - Nová budova Tylova 15
- Záložní připojení do Giga-PoP Plzeň
- Plán: 10Gb/s páteř WEBnetu



WEBnet - IP kamery v menze

- Pohled na výdej a prostor před výdejem
- Stojíte neradi fronty? Koukněte se na kamery.

WEBnet - VPN

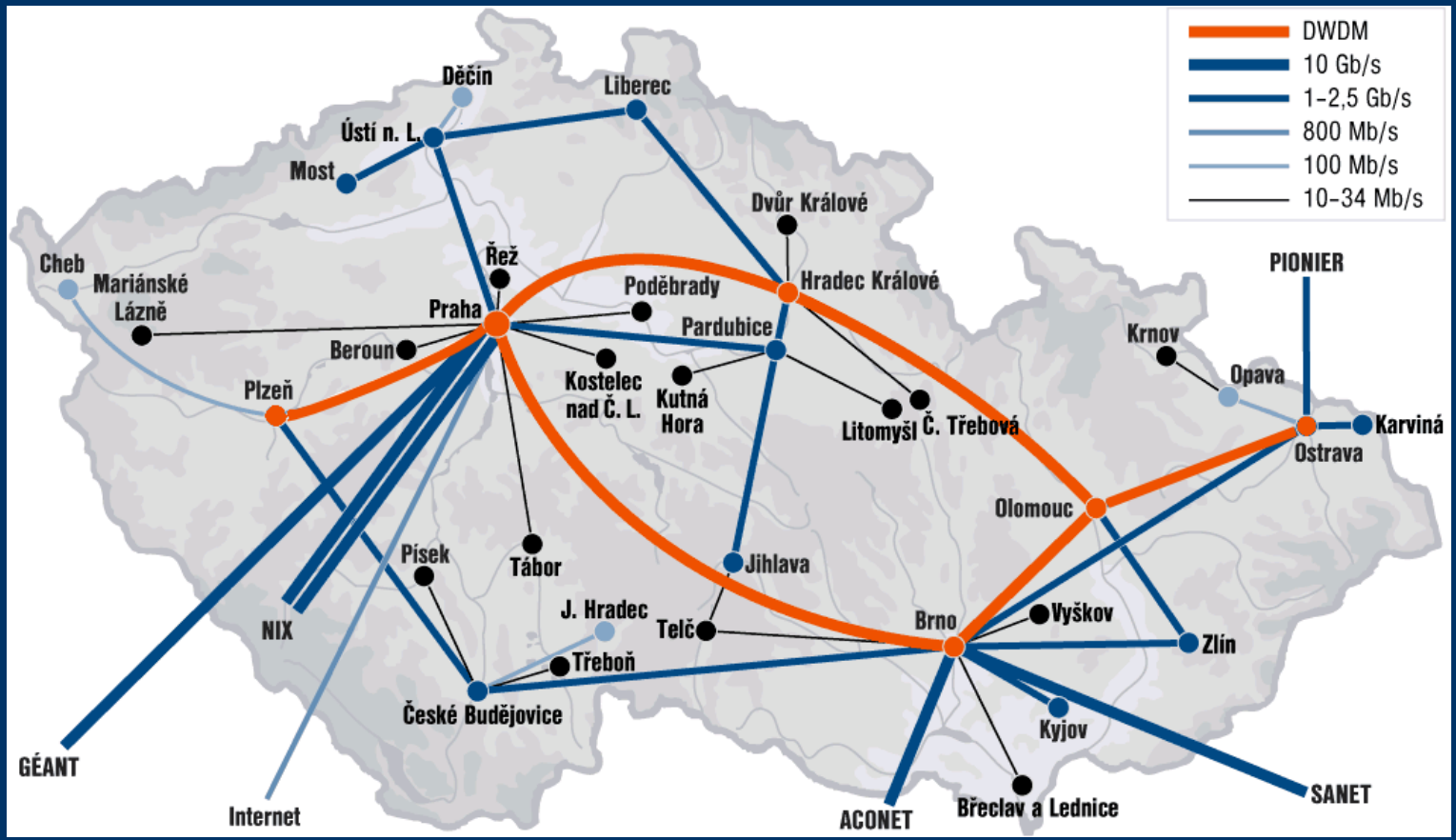
- Vzdálený přístup do sítě WEBnet
- Zabezpečené propojení do sítě
- Pouze ověření uživatelé
- Z bezpečnostních důvodů nefunguje z kolejí

WEBnet - IP telefonie

- Volání do ZČU a jiných partneských VŠ zdarma
- Nulové náklady na pořízení
  – softphone
- Veřejné telefoní číslo
  – každý se Vám dovolá
- Funguje odkudkoliv i z kolejí

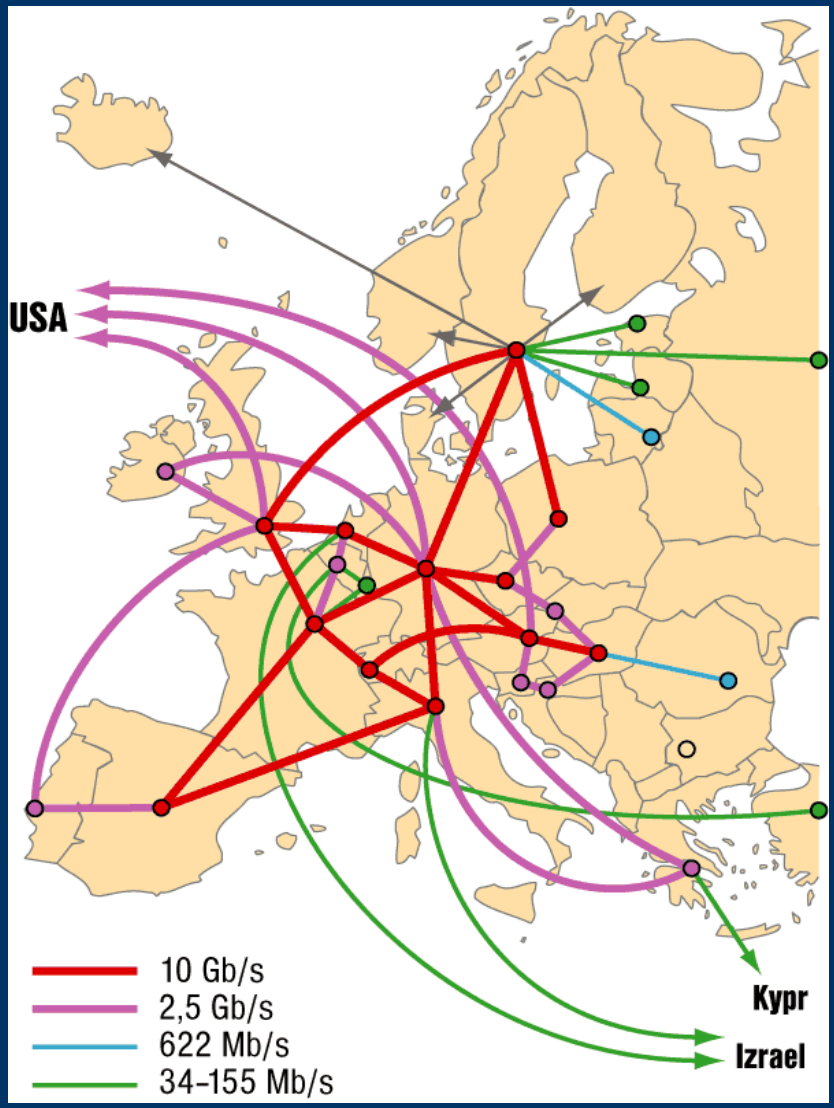
CESNET

- 10 Gb/s Praha, 1 Gb/s ČB, 100 Mb/s Cheb



CESNET

- Propojení sítě CESNET do evropské páteřní akademické sítě GÉANT

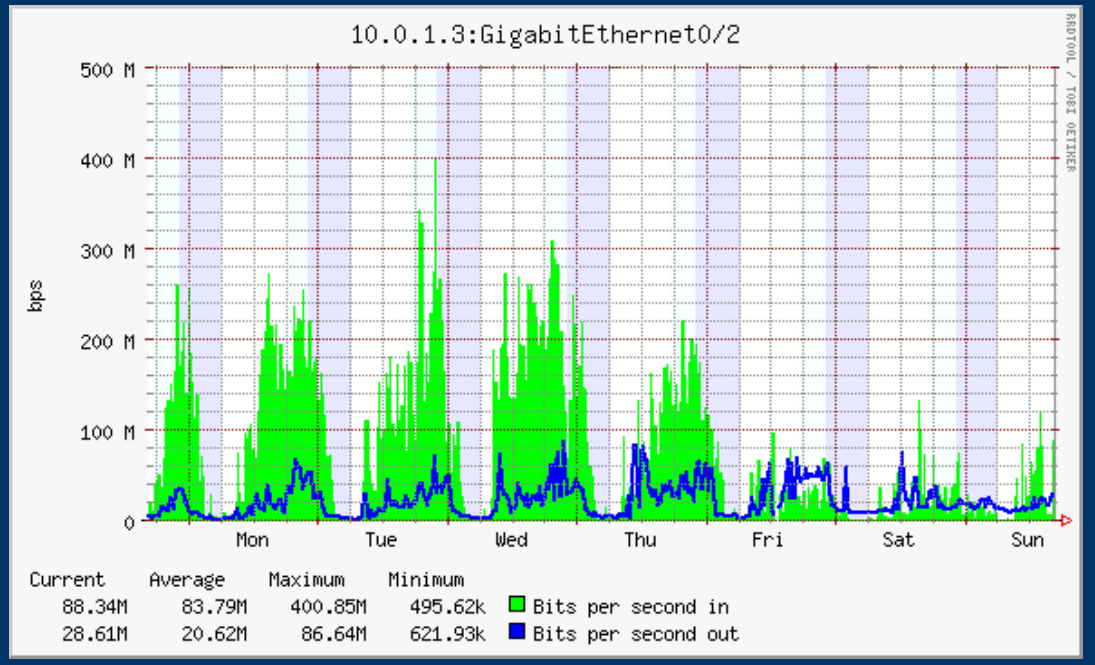


Koleje

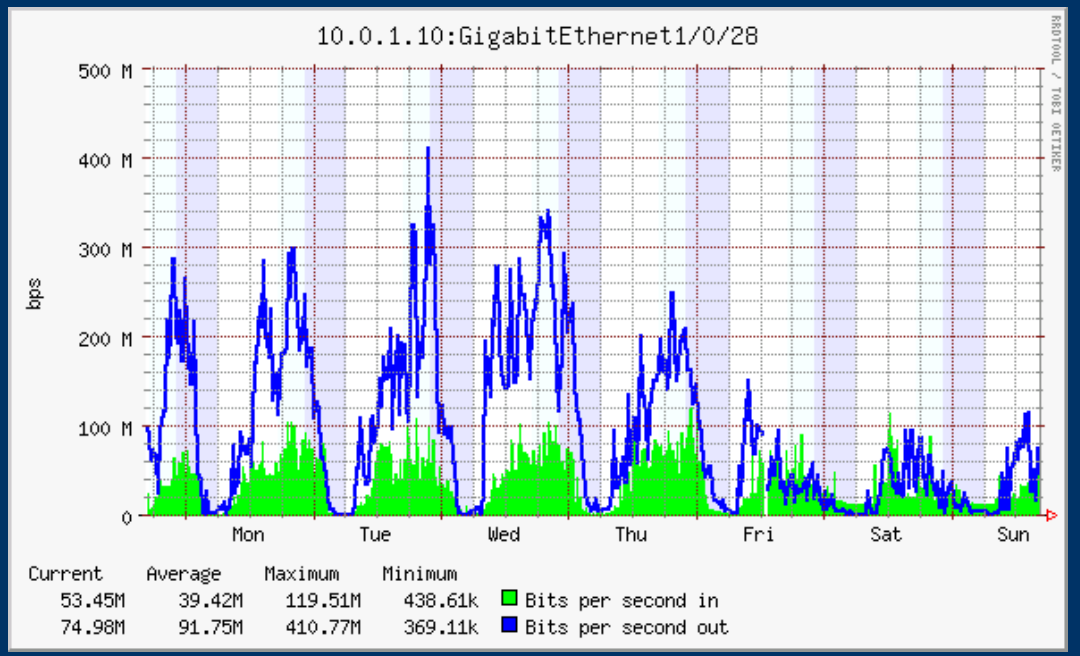
- Máchova, Borská, Bolevecká a Dylenská
- Novinky:
  - Nová profesionální kabeláž na M14
  - Dodělání profesionální kabeláže na M20
  - Plán: připojení Borské koleje 1Gb/s optickým kabelem
- Kvazikoleje připojené do ZČU:
  - Litice, Jíkalka, Borská 67 a Žižkova / Tylova
- Kvazikoleje bez přímého připojení do ZČU:
  - Internáty Vejprnická a Karlovarská

Koleje

- Bolevecká
  - Zaregistrovaných počítačů: 530

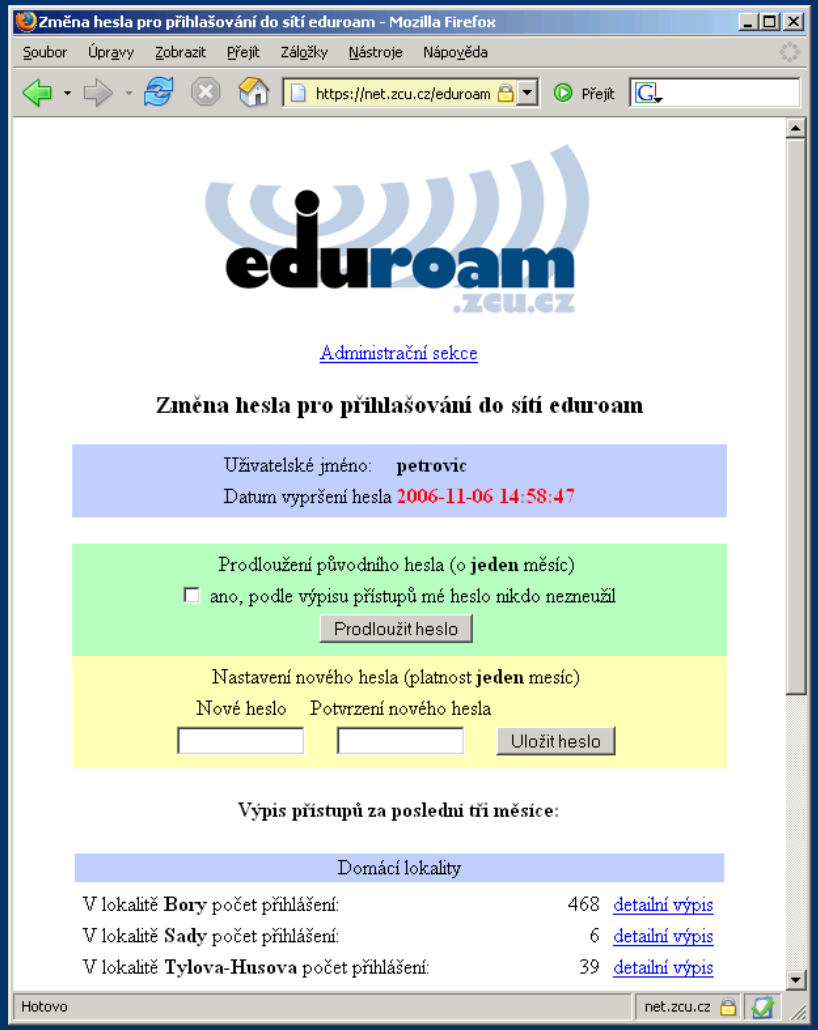


- Máchova
  - Zaregistrovaných počítačů: 1100



Eduroam – mobilní zařízení

- Bezdrátové i pevné připojení
- http://eduroam.zcu.cz
- Uživatelské jméno Orion
- Heslo je rozdílné
- Platnost hesla 3 měsíce
- 1980 registrovaných lidí
- 1100 aktivních lidí

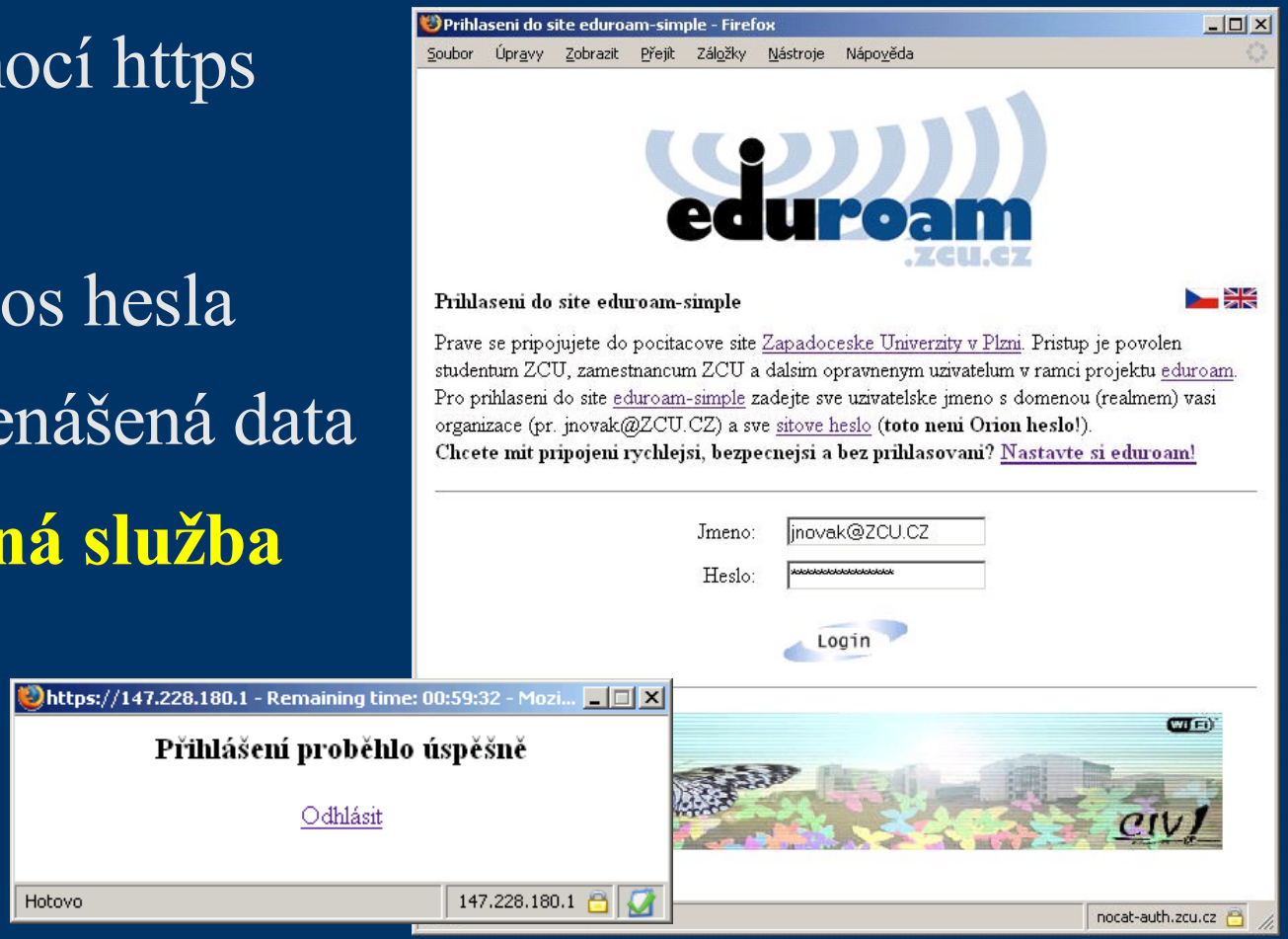


Eduroam – mobilní zařízení

- Eduroam - bezpečné připojení
  - Standard 802.1X
  - PEAP
  - WEP, WPA, WPA2
  - Šifrovaný přenos hesla
  - Šifrovaný přenos dat

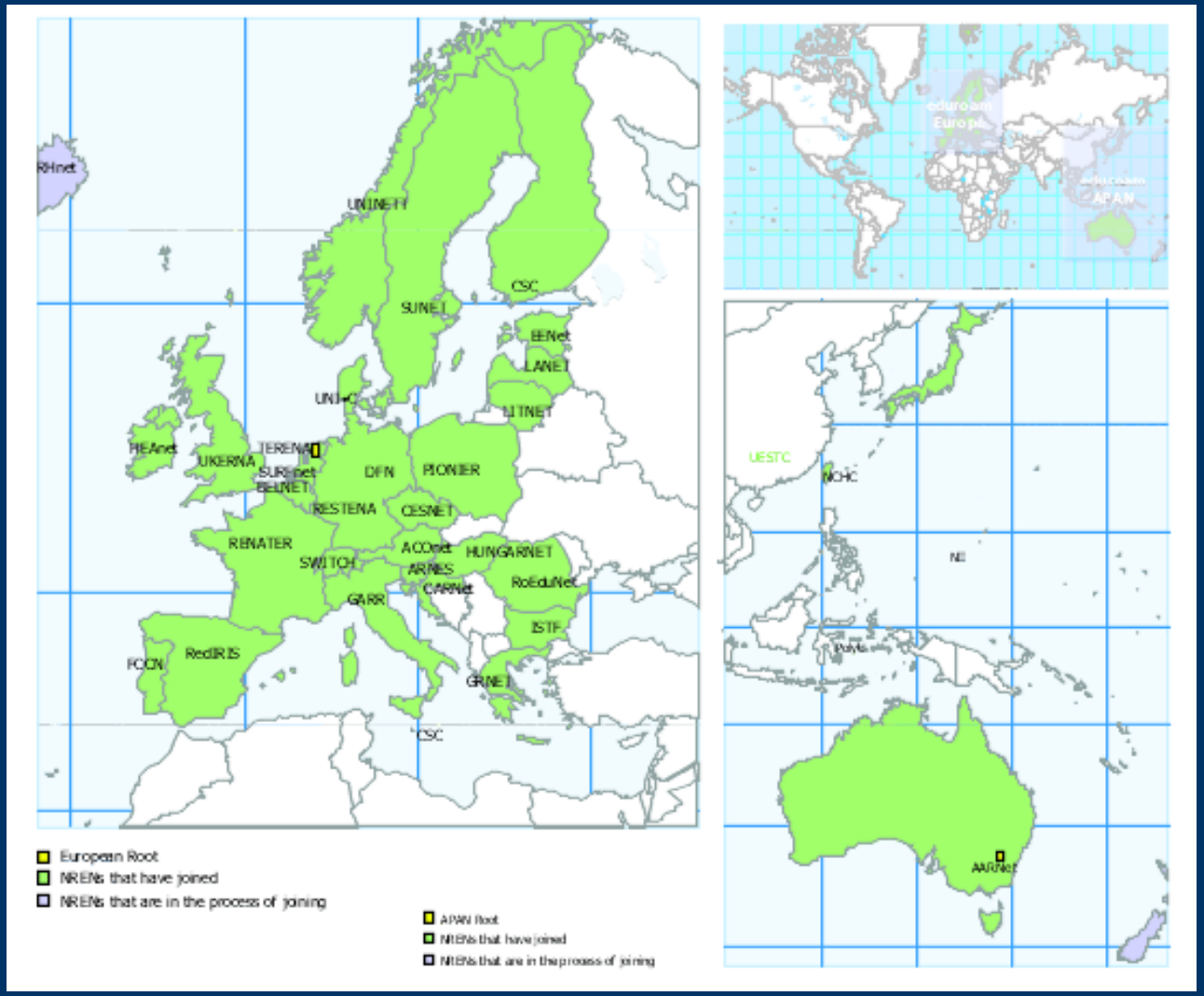
Eduroam – mobilní zařízení

- Eduroam-simple - poslední záchrana
  - Přihlášení pomocí https
  - Pop-up okno
  - Bezpečný přenos hesla
  - Nešifrují se přenášená data
  - **Nepodporovaná služba**



Eduroam – mobilní zařízení

- 30 zemí světa
- ČR:
  - AMU
  - CESNET
  - CUNI
  - ČVUT
  - MNUL
  - MUNI
  - OSU
  - SSŠVT
  - TUL
  - UHK
  - UJEP
  - UPa
  - VŠE
  - VŠCHT



Dotazy

Elektronická pošta

Miloš Wimmer

<wimmer@civ.zcu.cz>

Poštovní účet

- každý student a zaměstnanec ZČU získává e-mailovou adresu a schránku automaticky společně se svým uživatelským účtem v prostředí Orion


OUVENIR DU MAROC
PUBLIPUR
RALLYE du MAROC
Classic
SOUVEIR DU
Coca-Cola
WELCO

Elektronická adresa

- adresy mají tvar
  login@students.zcu.cz (studenti)
  login@útvar.zcu.cz (zaměstnanci)
  např. login@civ.zcu.cz
  login@service.zcu.cz (služební adresy)

- E-mailové adresy lze snadno vyhledat v LDAP serveru ldap.zcu.cz nebo na telefonním seznamu ZČU

  http://phone.zcu.cz

Velikost diskového prostoru

- zaměstnanci 50 MB --> 200 MB
- studenti 20 MB --> 100 MB
- uživatelé si mohou svojí kvótu sami jednorázově navýšit na extra limit na osobní stránce „Moje složky“

http://mail.zcu.cz/

- kvóta se vztahuje na všechny zprávy a složky dohromady
- zobrazení stavu zaplnění kvóty

Přístup k poště

- pomocí klientů pro vzdálený přístup přes protokoly IMAP nebo POP / SSL
- podporovanými poštovními klienty v prostředí Orion jsou pine, Mozilla Thunderbird, (((Outlook)))
- z WWW prohlížeče přes webovou bránu

  http://webmail.zcu.cz/

- všemi ostatními poštovními klienty, kteří podporují protokol IMAP nebo POP3 se zabezpečením SSL

Školní účet

- studenti i zaměstnanci mají povinnost číst svoji školní poštu, resp. el. pošta je postavena vyhláškou na rovinu úřední desky a po doručení zprávy je student/zaměstnanec považován za informovaného (viz Statut ZČU)
- elektronickou poštu doručovanou do školní schránky lze snadno třídit podle uživatelem zadaných pravidel nebo přesměrovat na jinou adresu

Školní účet

- je odpovědností uživatele, aby si udržoval ve své schránce přiměřené volné místo
- přeplnění schránky brání doručování dalších zpráv


ROYAL

Výhody školního účtu

- studenti i zaměstnanci by měli pro studijní resp. pracovní záležitosti používat školní poštovní účet
  - snadno zjistíte adresy
  - prokazatelnost
  - bezpečnost
  - důvěrnost
  - všechny protokoly zadarmo

Výhody školního účtu

- rychlost
- pomoc na dosah
- snadné zvýšení kvóty
- nikdo nerozhoduje za vás
- vaše zprávy neměníme
- obnova zpráv se zálohy

- řešení problémů – jen na zprávy posílané ze školního účtu

- žádná reklama


Coca-Cola

Limit

- Maximální velikost zprávy přenášené systémem elektronické pošty ZČU

10 MB


500
Jaouda
LAIT FRAIS

Dokumentace

- http://mail.zcu.cz/dokumentace/
- obrázky s nastavením klientů
- při přístupu z vnějších sítí nastavit zabezpečený přístup k serveru odchozí pošty (SSL) s použitím vašeho jména a hesla
  - anebo použít WebMail


دولي دول®

Systém antivirové/antispamové kontroly

- zprávy doručované na centrální poštovní server prochází předřazeným serverem antivirové/antispamové kontroly (fred)
- ze zpráv odstraňuje rozpoznané viry a zprávy obsahující virus nebo spam značkuje

- svobodný software (MailScanner, ClamAV, Spamassassin, ...)

Systém antivirové/antispamové kontroly

- Značky, jimiž jsou opatřeny zprávy obsahující virus nebo spam, lze následně využít při finálním doručení zpráv na centrálním poštovním serveru
- V závisloti na nastavení každého uživatele lze s nimi provádět automatické operace, např. smazání nebo přesun do určené složky

Antivirová kontrola

- Antivirová kontrola odstraňuje z procházejících zpráv rozpoznané viry a místo nich vkládá přílohu s informací o jejich vyjmutí. Zpráva obsahující virus je tedy odvirována, opatřena značkou o odhalení viru a doručena příjemci

- Značka se přidává do transportní obálky zprávy v podobě řádku
  X-ZCU-MailScanner: Found to be infected

Antispamová kontrola

- Antispamová kontrola značkuje zprávy, ve kterých byl rozpoznán nevyžádaný obsah/spam - to znamená, že do transportní obálky zprávy přidává řádku
  X-Spam-Flag: YES

- a dále pak řádky s informací o bodovém ohodnocení spamu typu:

  X-ZCU-MailScanner-SpamCheck: spam, SpamAssassin
  (score=9.236,required 5, EXTRA_MPART_TYPE 0.81,
  RCVD_IN_BL_SPAMCOP_NET 1.33, ...
  X-ZCU-MailScanner-SpamScore: *********


SINDIBAD

Nastavení chování

- Nastavení automatické operace pro zprávy označené jako virus (spam) je pro uživatele velmi jednoduché. Provádí se pomocí intuitivního WWW formuláře na adrese

  http://mail.zcu.cz/

- pod odkazem "Moje nastavení" v sekci "Nastavení antivirové (antispamové) kontroly"

Nastavení chování

- Kontrola nabízí následující režimy:
  - Bez automatické operace
  - Automatické zatřídění označených zpráv do složky X-Virus (X-Spam)
  - Automatické mazání označených zpráv
- Nápověda na formuláři
- Občas prohlédnout určenou složku a vyčistit, její obsah se započítává do kvóty

Moje posta - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://mail.zcu.cz/moje-nastaveni

Google

Moje pošta

Nastavení přesměrování a třídění pošty

Uživatelské jméno: wimmer

Nastavení přesměrování pošty (soubor .forward) *Nápověda*

Nastavení antivirové kontroly *Nápověda*

- ○ Bez automatické operace
- ◉ Automatické zatřídění označených zpráv do složky X-Virus
- ○ Automatické mazání označených zpráv

Nastavení antispamové kontroly *Nápověda*

- ○ Bez automatické operace
- ◉ Automatické zatřídění označených zpráv do složky X-Spam
- ○ Automatické mazání označených zpráv

Nastavení automatické odpovědi během nepřítomnosti *Nápověda*

- ◉ Není aktivní
- ○ Je aktivní

Dnes jsem mimo své pracoviště.
Vaši zprávu si přečtu po svém návratu

Nutné zvýšení obrany

- dříve poštovní systém představoval ryze transportní službu, doručoval veškeré zprávy, které přicházely, viry neodstraňoval (30 : 70 , 100.000)

- nyní jsme ve „válečném“ stavu
  - záplava spamu
  - virové bouře
  - DOS útoky
- musíme zajistit odolnost služby a její dostupnost

Statistika

- Poměr čistých zpráv ke spamu+virům

2 : 98

- Objem zpráv z Internetu za den

až 600.000

Nutné zvýšení obrany

- fred provádí vstupní kontroly a odmítá zprávy z
  - nekorektních serverů
  - nekorektních odesilatelů
  - serverů uvedených v RBL listech
- fred používá greylisting
  - interní databáze
  - prvotní odložení přijetí zprávy (zpoždění)
  - neuplatňuje se pro domény .cz


AFE
ESTAIJRA

Nutné zvýšení obrany

- žádná z kontrol zprávy tiše nezahazuje, v případě odmítnutí se vrací odesilateli
- kontroly – rozumný kompromis
- nechová se jako „černá díra“

Děkuji za pozornost

POČÍTAČOVÁ BEZPEČNOST
z pohledu uživatele

Aleš Padrta
apadrta@civ.zcu.cz

Obsah

- Motivace
- Úvod do bezpečnosti
- Doporučení
  - Technické prostředky
  - Bezpečné chování
  - Zobecněné rady
- Shrnutí

Motivace

Úvodní zamyšlení

- Bezpečnost
  - Ve “fyzickém” světě běžná
    - Už od dětství
      - Zamykání bytu
      - Přecházení silnice
      - ...
  - V prostředí výpočetní techniky
    - Není v povědomí
      - Nenápadný příchod sítí
      - Postupné rozšiřování služeb (čistě informační www → bankovnictví)
      - Syndrom technické magie (příliš složité “pro všechny”)
- Kriminálníci jsou všude
  - Také v oblasti výpočetní techniky → nutné se bránit

Motivace

Jaká jsou rizika?

- Důvody útoků
  - Nejčastěji peníze, hromady peněz
- Cíle útoků
  - Kontrola nad PC
    - Výpočetní výkon
    - Datové úložiště
    - Nástroj pro další útoky
  - Zajímavé údaje
    - Vědeckotechnická špionáž
    - Osobní informace
  - Krádež elektronické identity
    - Přesunutí odpovědnosti za své činy

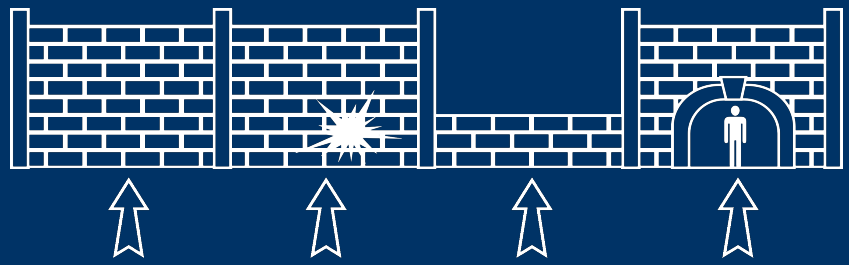
Motivace

Přístup k bezpečnosti

- Představa naivního uživatele
  - Bezpečnost nepotřebuji
  - Nechte mě pracovat
- Představa uvědomělého uživatele
  - Bezpečnost by se mi hodila
  - Investice minima času a zdrojů
- Představa CIV
  - Bezpečnost je nutná
  - Investice do bezpečnosti se vyplatí
- Řešení
  - CIV vám poradí :-)
    - Sborník o bezpečnosti, http://support.zcu.cz/bezpecnost, přednášky

Úvod do bezpečnosti

- Dosažení cíle
  - Více způsobů → více bráněných míst
    - Technické prostředky
    - Chování uživatele
  - Problém nejslabšího článku



- Vícestupňová obrana
  - Několik překážek
    - Antispam → uživatel → antivir
  - Chování uživatele
    - Někdy jediný prvek obrany
    - Zásadně ovlivňuje bezpečnost

Doporučení
Technické prostředky

- Aktualizace systému
  - Chyby v programech jsou a budou
  - Naprosto nezbytné
  - Standardní cestou
- Antivirový program
  - Blokování známých (!) virů
  - Heuristika (sofistikovaný odhad) ne vždy funguje
- Firewall
  - Snížení (!) počtu možných útočníků
  - Není zárukou 100% ochrany

Doporučení
Technické prostředky

- Uživatelské účty
  - Menší práva než administrátor → menší škody
- Bezpečná komunikace
  - Citlivé údaje vždy přenášet šifrovaně
  - SSH, HTTPS, IMAP-SSL, POP-SSL
- Ověření komunikujícího protějšku
  - Komu jsou data zasílána
  - Častý zdroj problému
  - Certifikáty

Doporučení

Bezpečné chování

- Instalace programů
  - Nejlépe neinstalovat :-)
  - Pouze oficiální verze
  - Žádné neověřené patche, cracky a pod.
    - Kdo je vytvořil?
    - Co asi tak provádí?

Doporučení

Bezpečné chování

- Zacházení s heslem
  - Zvolit vhodné heslo
    - Zapamatovatelné
    - Dostatečně složité
  - Pečlivě uschovat, nejlépe zapamatovat
  - Heslo zná pouze uživatel
    - Nikdo jiný nemá nárok

Doporučení

Bezpečné chování

- Zacházení s e-mailem
  - Odesílatele lze podvrhnout
    - Digitální podpis
  - Odesílatel není vždy Mirek Dušín
    - Sociální inženýrství
    - Přílohy mohou být nebezpečné
      - Virus
    - Odkazy na podvržené stránky
      - Phishing
    - Šíření poplašných zpráv (Hoax)
      - Další šíření spamu
      - Petice → zisk osobních údajů
      - Peněžní sbírky → přímé obohacení

Doporučení

Zobecněné rady

- Buďte podezřívaví - nejlépe paranoidní ;-)
  - Divný požadavek?
  - Jiný postup bež obvykle?
  - Nečekaná odezva?
- Ověřujte důležité údaje
  - Jiným způsobem (osobně, telefonicky)
- Buďte informovaní
  - Více informací = vyšší bezpečnost
    - Vhodný kompromis
  - Rizika se časem mění
    - Aktuality na http://support.zcu.cz (novinky)

Shrnutí

- Výpočetní technika
  - Zajímavý cíl pro kriminální živly
  - Potřeba zabezpečení
- Bezpečnost
  - Problém nejslabšího článku
  - Závisí na znalostech
- Zajištění bezpečnosti
  - Technické prostředky
  - Vhodné chování uživatelů (!!)

Certifikační autorita ZČU a PKI

Pavel Jindra

Seminář CIV, 18 a 19 října 2006

PKI - public key infrastructure

- infrastruktura veřejných klíčů
- soubor administrativně technických prostředků pro svázání el. identity s fyzickou
- identita je prokazována vlastnictvím privátního klíče
- hierarchicky delegovaná důvěryhodnost pomocí elektronických podpisů
- vše zaručuje Certifikační autorita (CA)

ZCU root CA - služby

- DN: CN = ZCU root CA, OU = zcu_pki, O = zcu, C = cz
- vydává a spravuje
  - uživatelské certifikáty
  - uživatelské síťové certifikáty
  - certifikáty serverů
- podepisuje SW komponenty
- pouze v rámci ZČU

Uživatelské certifikáty

- určené pro el. podpis e-mailových zpráv
- umožňuje šifrování e-mailové komunikace
- elektronický podpis pro webové formuláře (např. objednávky)
- autentizace pro webové služby (WebAuth)
- vydáván na HW kryptografický token
- pouze pro vybrané zaměstnance v rámci pilotního projektu

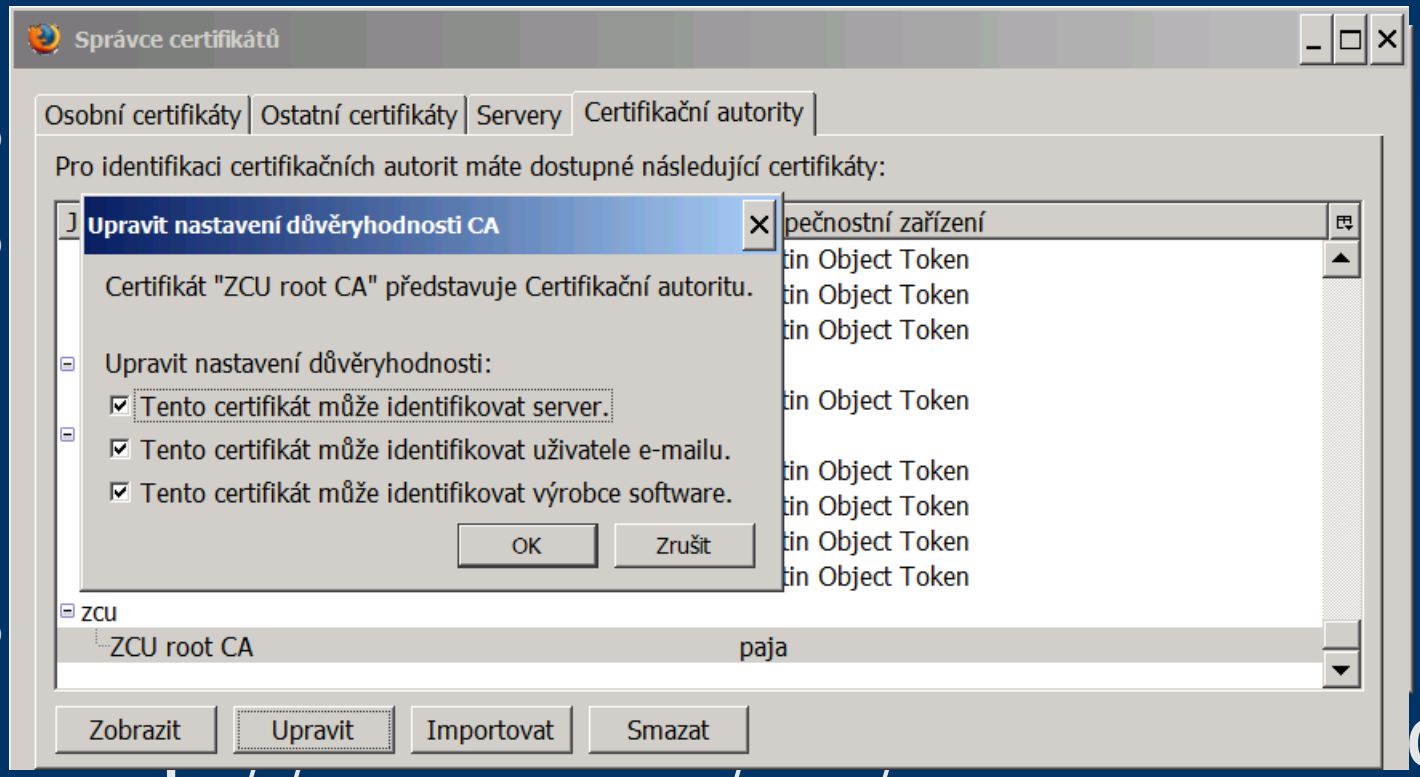
Uživatelské síťové certifikáty

- autentizace ke specializovaným síťovým službám
- eduroam, WiFi
- VPN
- mírnější politika vydávání
- vydávány pouze pro případy, kdy nelze použít jiné metody autentizace

Certifikáty pro servery

- identifikují komunikující server
- použití:
  - všechny servery zapojené do infrastruktury WebAuth
  - portál a další webové služby
  - IMAP, SMTP
  - Eduroam
- Nutné mít importován kořený certifikát

Import kořenového certifikátu

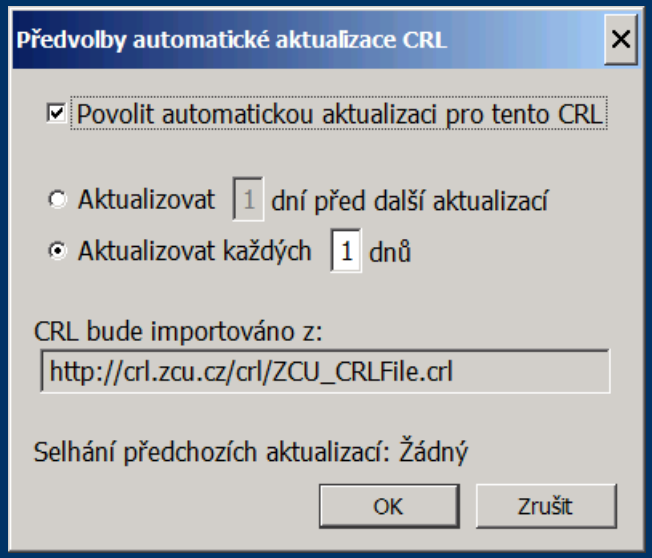


der

- Kontrola miniatury certifikátu:
  f3:7e:f0:15:a3:ac:47:6f:fb:c6:0d:b1:3e:e6:2c:33:a9:40:ed:49

CRL – Seznam odvolaných certifikátů

- tam kde se používají certifikáty by měl být pravidelně aktualizován seznam CRL
- http://crl.zcu.cz/crl/ZCU_CRLFile.crl
- nutno nastavit stahování CRL pro každé úložiště certifikátů zvlášť



Identity Management

ve výpočetním prostředí Západočeské univerzity v Plzni

Jiří Bořík

seminář CIV, říjen 2006

Co to je „Identity Management“

- komplexní systém pro správu zdrojů a identit ve výpočetním prostředí
- škálovatelné a přizpůsobitelné řešení pro automatizaci správy identit uživatelů za účelem řízení rizik, zajištění shody s předpisy a snižování administrativních nákladů. Optimalizuje a zjednodušuje správu identit interních a externích uživatelů a jejich oprávnění. Pomáhá tak zajistit kontrolu nad informačními systémy a dodržování podnikových zásad v rámci procesů.

Elektronické identity a zdroje

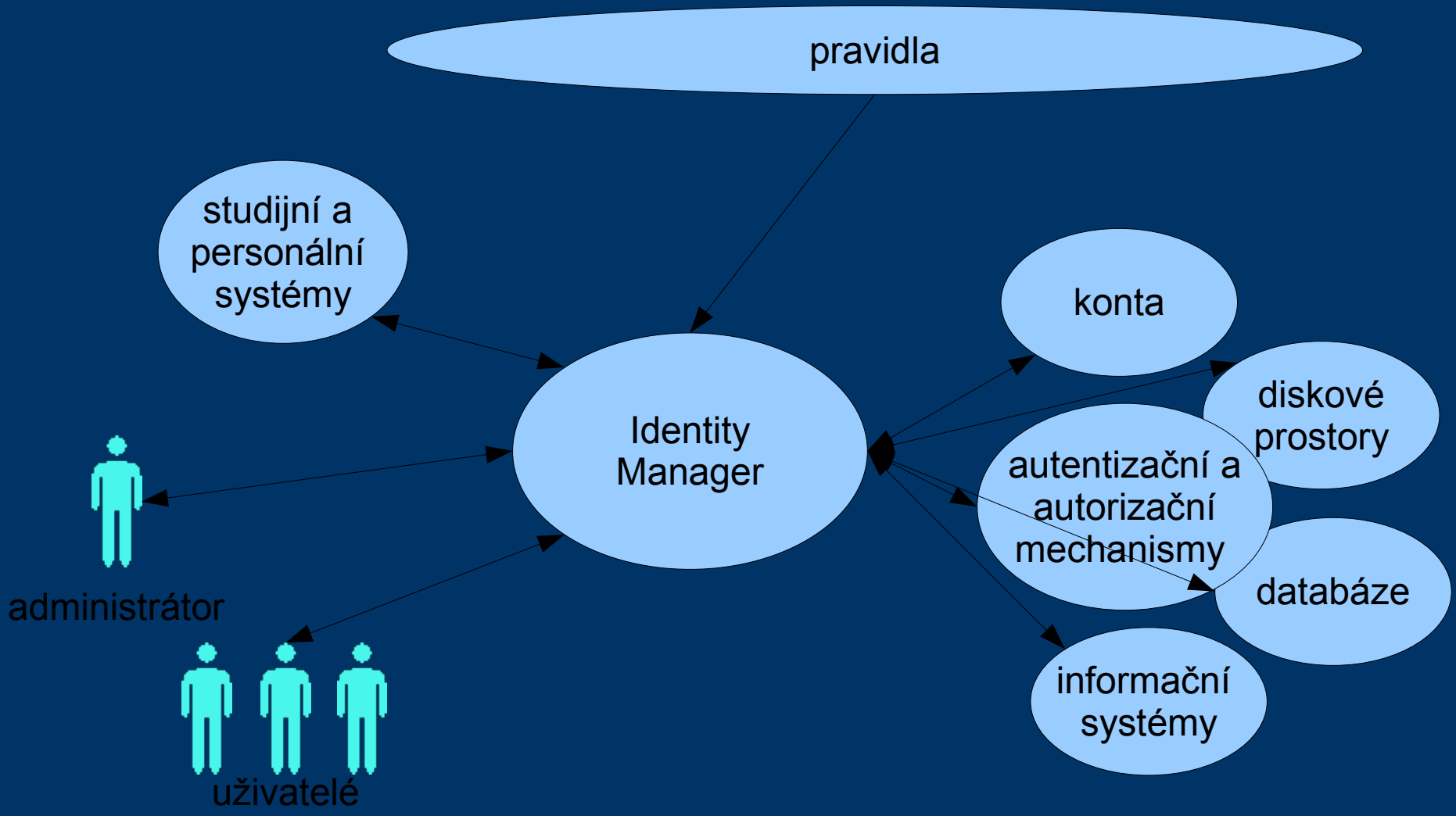
Identity

osoby
konta
emailové adresy
emailové aliasy
stroje
diskové prostory
...

Zdroje

diskové prostory
poštovní schránky
stroje
databáze
informační sytémy
síťové služby
...

Identity Management (IdM)



Implementace IdM

Předpoklady

- jasná pravidla přístupu k IT zdrojům
- centrální správa IT nebo jasně definované vztahy
- hodnověrná data

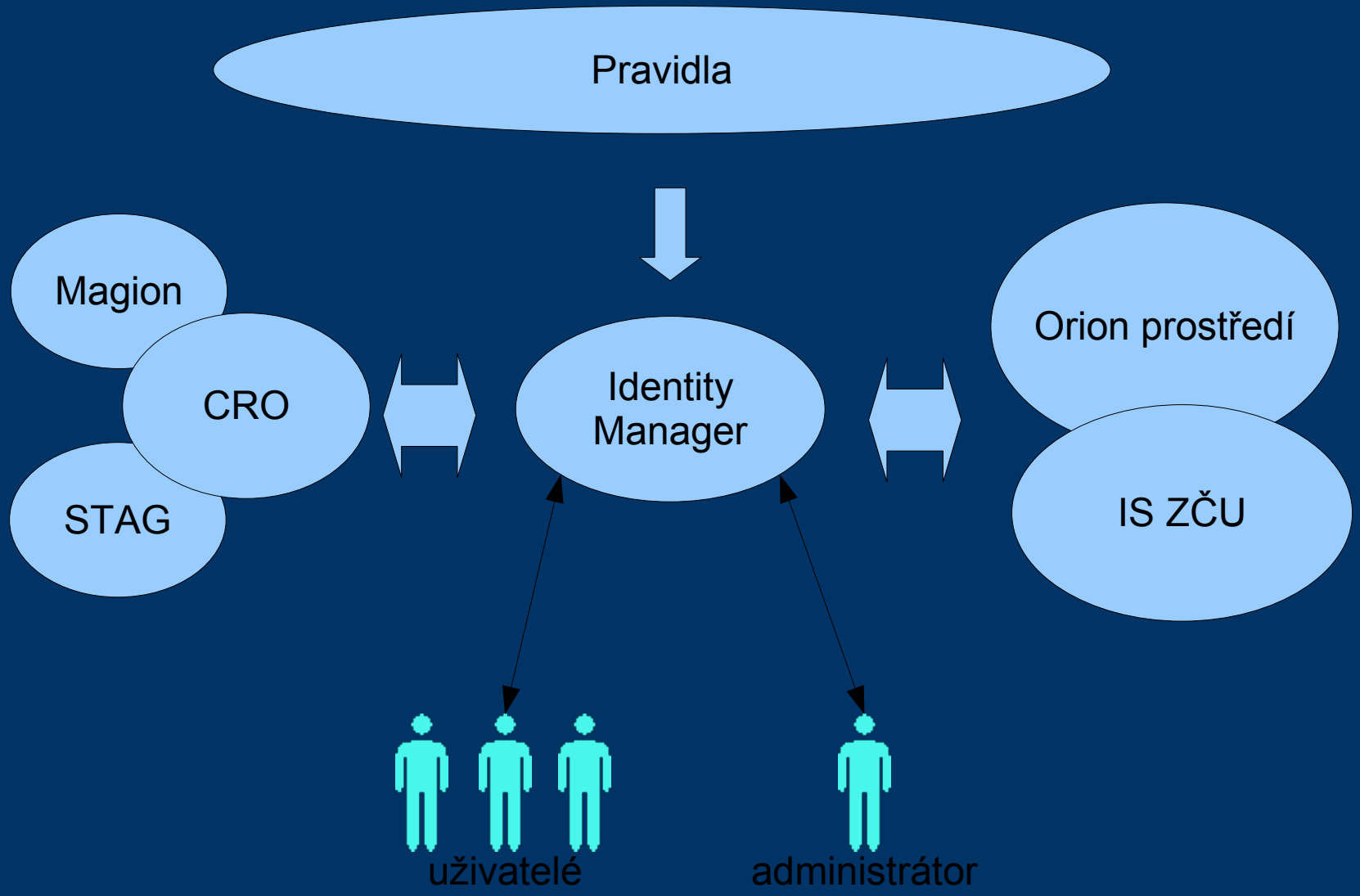
Požadavky

- vazby do mnoha typů cílových systémů
- efektivní nástroje pro administraci velkého počtu uživatelů
- schopnost delegace správy

Současná situace ZČU

- data máme v poměrně vysoké kvalitě (konsolidace dat CRO)
- životní cyklus uživatelské identity je definován pro běžné pozice studenta a zaměstnance
- vazby mezi systémy – postupně vzniklé, zaslouží si revizi, 24 hodinový cyklus dávkových přenosů mnohde už nevyhovuje
- nástroje pro správu – omezené, neumožňují efektivní delegaci administrátorských pravomocí
- dožívající HW a SW pro správu kont

Plánovaná struktura IdM v ZČU



Přínosy pro uživatele

- správa na jednom místě
- zjednodušení procesů zřizování přístupů ke zdrojům
- zrychlení odezvy požadavků
- lepší informovanost o stavu požadavku

Přínosy pro správce zdrojů

- jednoznačná identifikace uživatelů
- zjednodušení a zpřehlednění správy
- delegace správy a samoobslužná správa
- snadnější kontrola využití zdrojů
- rychlejší a spolehlivější propagace dat do cílových systémů
- zvýšení bezpečnosti systémů

Přínosy pro vlastníka zdrojů

- zajištění přístupu pouze oprávněným uživatelům
- lepší využití zdrojů
- snížení nákladů na správu
- zvýšení bezpečnosti IT systémů
- audit operací

Další kroky

- napojení na CRO
- správa Orion prostředí
- napojení vybraných IS ZČU

Výhled

- napojení většiny centrálních IS ZČU
- podpora vybraných lokálních služeb
- podpora federativních systémů

Prostor pro dotazy...

Děkuji za pozornost.