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

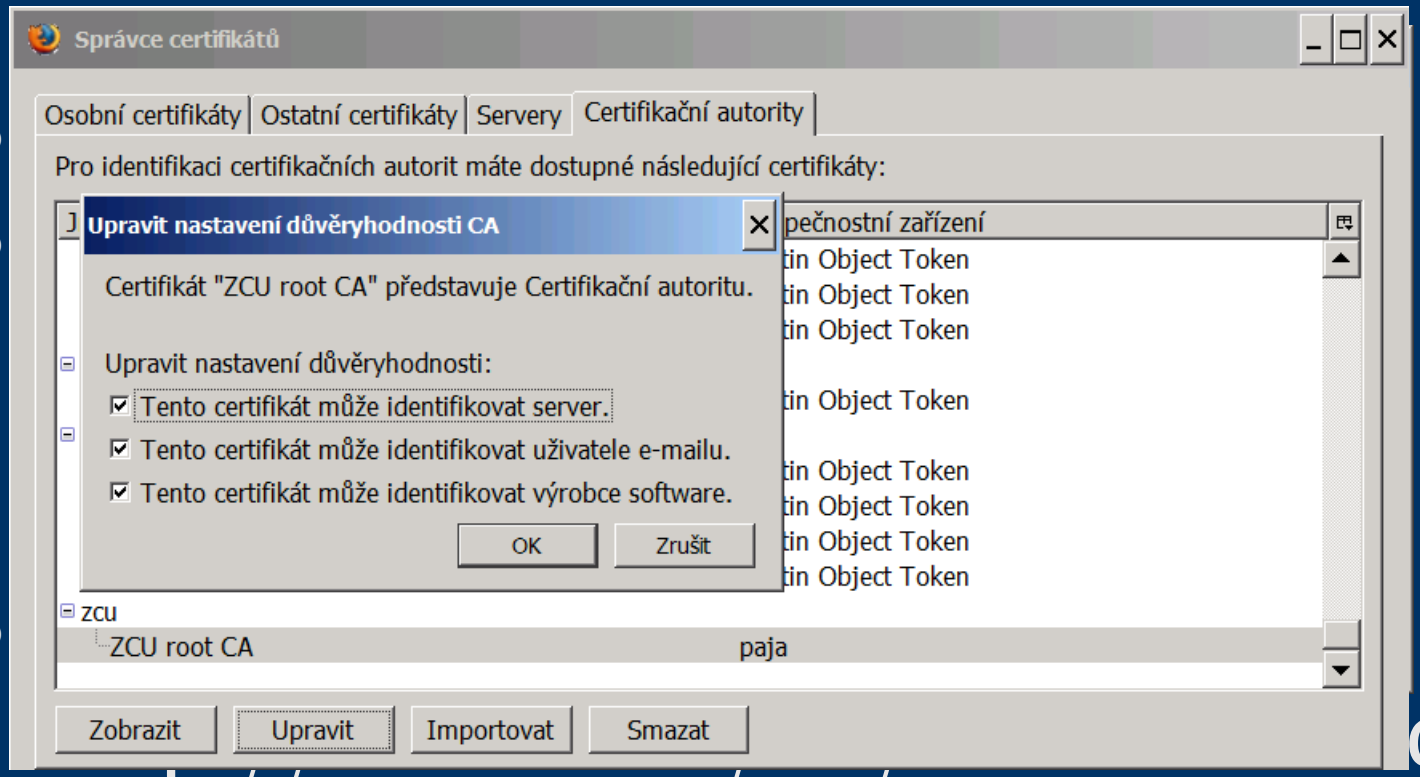
Uživatelské síťové certifikáty

- 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