

Provoz certifikační autority, Certifikační politika

Milan Sova
CESNET

Čipové technologie pro aplikace
vyžadující identifikaci a elektronický podpis

Praha 4.12.2003

Obsah

- Služby CA
- Provoz CA
- Dokumentace CA
- CESNET CA

Služby poskytované CA

- Identifikace vlastníka privátního klíče
 - Záruka jednoznačnosti vztahu subjekt – jméno
 - Přidělení jména
 - Identifikace subjektu
 - Odvolávání certifikátů
 - Ukončení platnosti identifikačních údajů
 - “Zveřejnění” či “ztráta” privátního klíče
- Časové razítko
 - Potvrzení existence datového objektu v daném čase

Registrační autorita

- Provádí identifikaci žadatele a autorizaci žádosti
- Obvykle více RA pro jednu CA
 - Organizační součást CA
 - nebo provozovaná jinou institucí ve smluvním vztahu s institucí provozující CA

Certifikační autorita

- Zpracovává žádosti o certifikáty ověřené registrační autoritou
- Vydává a publikuje certifikáty
- Odvolává certifikáty a publikuje seznamy odvolaných certifikátů
- Obvykle spravuje CPS

Policy Management Authority (PMA)

- Spravuje CP
- provozována
 - Přímo certifikační autoritou (CP pro jednu CA)
 - Nezávislým orgánem (CP pro více spolupracujících CA)

Identifikace subjektu

- Osoby
 - Ověření totožnosti
 - Ověření identifikačních údajů
 - Ověření vlastnictví privátního klíče
- Systémy & služby
 - Ověření identity žadatele
 - Ověření oprávnění provozovat službu

Základní dokumenty CA

- Certifikační politika (CP)
 - Pravidla pro vydávání, publikování a odvolávání certifikátů
- Certifikační prováděcí směrnice (CPS)
 - Popis procesů a opatření zaručujících dodržení CP
- RFC 3347
 - Obsah a struktura CP & CPS

RFC 3647

- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu. November 2003.
 - nahrazuje RFC 2527 z března 1999

CP/CPS podle RFC 3647

- Definice
 - Účastníci PKI
 - CA, RA, abonenti, uživatelé
 - Řádné a zakázané užití certifikátů
 - Proces správy CP/CPS
- Pravidla pro publikaci certifikátů

CP/CPS podle RFC 3647

- Identifikace a autentizace
 - Jména
 - Ověření totožnosti
 - Oprávnění

CP/CPS podle RFC 3647

- Životní cyklus certifikátu - provozní požadavky
 - Podání žádosti
 - Zpracování žádosti
 - Vydání certifikátu
 - Akceptování certifikátu
 - Použití certifikátu
 - Obnovení certifikátu
 - Odvolání certifikátu
 - Služby poskytující informace o stavu certifikátu

CP/CPS podle RFC 3647

- Provoz CA
 - Fyzické podmínky
 - Řízení procesů
 - Personální řízení
 - Audit
 - Archivace
 - Změna klíče CA
 - Zotavení po ztrátě privátního klíče a katastrofě
 - Ukončení provozu

CP/CPS podle RFC 3647

- Technické zabezpečení CA
 - Generování a instalace klíčů
 - Ochrana privátních klíčů
 - Archivace veřejných klíčů
 - Bezpečnost počítačů
 - Síťová bezpečnost
 - Časová razítka

CP/CPS podle RFC 3647

- Profily certifikátů, CRL a OCSP
- Audit
- Právní a další otázky
 - Poplatky
 - Odpovědnost
 - Důvěrnost informací
 - Záruky...

CESNET CA

- Historie

- 1. 6. 2001

- pilotní provoz pro podporu projektu DataGRID

- 2002:

- rutinní provoz pro DataGRID

- příprava rozšíření služeb

- Nová CP

- 1. 4. 2003

- Oficiální poskytování služeb pro VŠ a AV ČR

CESNET CA

- Poskytované služby
 - Osobní certifikáty
 - Autentizace
 - Elektronický podpis
 - Certifikáty pro servery a služby
 - Autentizace

CESNET CA

- Software pro provoz CA/RA
- Software pro využití PKI
 - mod_auth_ldap_x509
 - S/MIME pro PINE

CESNET CA

- Domovská stránka
 - <http://www.cesnet.cz/pki>
- Vydané certifikáty
 - <ldap://pki.cesnet.cz>
- CRL
 - <http://www.cesnet.cz/pki/crl/cca.crl>

CESNET CA

- Budoucnost
 - RA mimo CESNET
 - OCSP

Děkuji za pozornost...